

Classical Cryptography

Summer 2008 course at b-it

Bonn-Aachen International Center
for Information Technology

© 2008 JOACHIM VON ZUR GATHEN

Version: July 14, 2008

Contents

1	Basic cryptosystems	1
1.1*	<i>Advanced Encryption Standard</i> (AES)	2
1.2*	The RSA cryptosystem	13
1.3	Visual cryptography	16
A	Substitution ciphers and frequency analysis	19
A.1	Cryptographic primitives	19
A.2*	Brief history of cryptography	26
A.3	Simple substitutions	36
A.4	Frequency analysis	38
A.5	Information theory	46
2	Security issues	53
2.1	Perfect security: the one-time pad	53
B	Key addition and modular arithmetic	57
B.1	Key addition systems	57
C	Breaking the unbreakable	61
C.1	Kasiski's attack on de Vigenère	61
D	Codebooks	73
D.1	Nomenclators	73
D.2	Commercial codebooks	82
D.3*	Unicity distance for codebooks	84
E	Transposition ciphers	87
E.1	The skytale tale	87
E.2	Columnar transpositions	88
E.3	Breaking a columnar transposition	91
F	The Zimmermann telegram	93
F.1	Capturing the <i>Magdeburg</i> 's codebooks	93
F.2	The telegram	96

F.3	Transmission and cryptanalysis	101
F.4	The drama unfolds	108
F.5	Wright or wrong, my country	112
G	ENIGMA, Turing, and COLOSSUS	117
G.1	ENIGMA	117
G.2*	Bletchley Park	122
G.3	Rotor cryptanalysis	125
	Acronyms	133
	Bibliography	135
	Players	143

Chapter 1

Basic cryptosystems

We start with a look at some of the most important cryptosystems. The description in this section focusses on the fundamental properties and leaves out some details, in particular proofs why certain things work the way they do. The complete underpinnings for these methods are provided in later chapters.

We learn to ask the fundamental questions: How easy is the system to use for its legitimate players? How hard is it to break for others? In other words: what can we say about its security? We begin with a short discussion of two fundamentally different types of cryptosystems that we will encounter: symmetric vs. asymmetric systems. In the first type, sender and receiver share the same secret key, while in the latter type, only the receiver needs a secret key. If you have not yet seen such systems, stop here for a moment! Does this not sound contradictory? How could it possibly work? The first system is the AES, chosen from 15 candidates in a competition launched in 1997 by the *National Institute of Standards and Technology* (NIST), a US government institution. This system is an example of a symmetric cryptosystem in which the two protagonists (sender and receiver) share the same key. AES is characterized by its simplicity, good structure, and efficiency.

We then describe the RSA system named after its inventors Rivest, Shamir & Adleman. The security of this *asymmetric* or *public key cryptosystem* is somewhat related to the difficulty of *factoring large integers* into their prime factors.

The third example is the Diffie & Hellman key exchange protocol. Here the goal is not to send a secret message, but somewhat more modest: the two players just want to agree on a common secret key (which they may then use in some other cryptographic setting). This example introduces the idea of doing cryptography in groups. The security of such system relies on the difficulty of computing *discrete logarithms* in these groups.

We then discuss Shamir's scheme for sharing a secret among many players so that together they know the secret but any coalition of fewer than all players has no knowledge about it. This is based on *polynomial interpolation*.

The final example is Naor & Shamir's *visual cryptography*. We have included

$\mathbb{F}_{2^8} \ni a = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7$,

where $a_i \in \mathbb{F}_2 = \{0, 1\}$.

Representation: 8 bits for an element = 1 byte.

Addition: XOR, $(a + b)_i = a_i + b_i$.

Multiplication: as for polynomials modulo $x^8 + x^4 + x^3 + x + 1$.

Example $57 \cdot 83 = \text{C1}$:

$$\begin{aligned} (x^6 + x^4 + x^2 + x + 1) \cdot (x^7 + x + 1) &= x^{13} + x^{11} + x^9 + x^8 + x^7 + \\ &\quad x^7 + x^5 + x^3 + x^2 + x + \\ &\quad x^6 + x^4 + x^2 + x + 1 \\ &= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\ &= x^7 + x^6 + 1 \pmod{x^8 + x^4 + x^3 + x + 1}. \end{aligned}$$

Field: You can divide by every non-zero element.

Figure 1.1: The field \mathbb{F}_{2^8}

it here because of its striking effects: you have two random pictures (here: one on paper and one on a transparency), and when you match them up, you can see a secret message.

1.1*. AES

In the early 1970's, a team at *International Business Machines* (IBM) developed a cryptosystem which became known as the *Data Encryption Standard* (DES). The US *National Bureau of Standards* (NBS) declared it in 1976 the standard for US government cryptography, for documents that are sensitive but not classified. (The *National Security Agency* (NSA) is responsible for higher levels of security.) As a consequence, any software or hardware systems with cryptographic capabilities tendered to the US government had to be based on DES. Sales to government agencies can be highly lucrative, and any company interested in them had to use DES. Thus it quickly found widespread use.

Over the years, many attacks on DES were developed, most notably differential cryptanalysis and linear cryptanalysis. In reply, DES was strengthened by tripling its number of “rounds”: triple-DES or 3-DES.

From the start, experts harbored suspicions—never substantiated—that the NSA might have built a “trapdoor” into DES that enabled it to decipher encrypted messages. Already in 1981, Deavours warned that *The agency [NSA] is currently capable of breaking DES using probable plaintext. The major cryptanalytic hardware involved is rumored to consist of 4 CRAY-1 computers. Analysis takes less than a day, on the average.* Finally, on 17 July 1998 the *Electronic Frontiers Foundation* (EFF) presented its US\$ 250,000 DES breaker. DES was dead, for

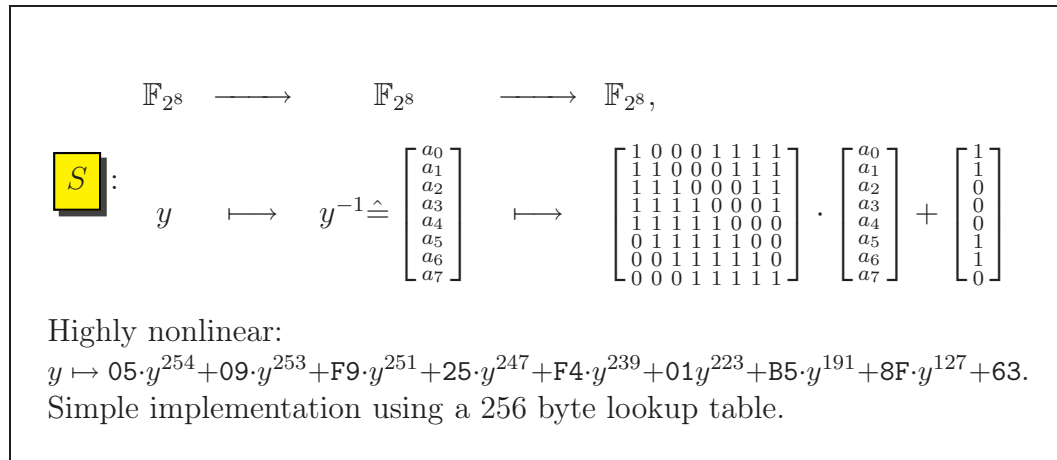


Figure 1.2: The S-Box

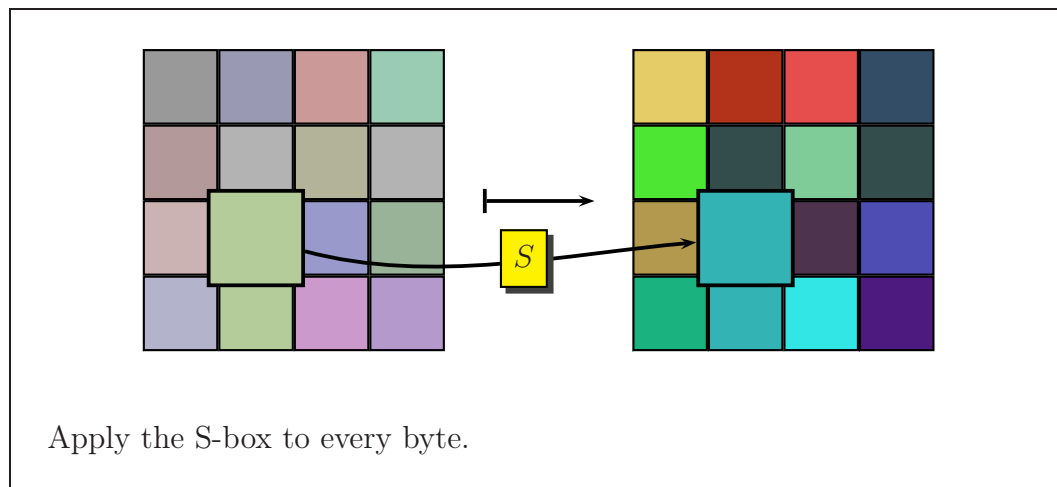


Figure 1.3: The SubBytes operation

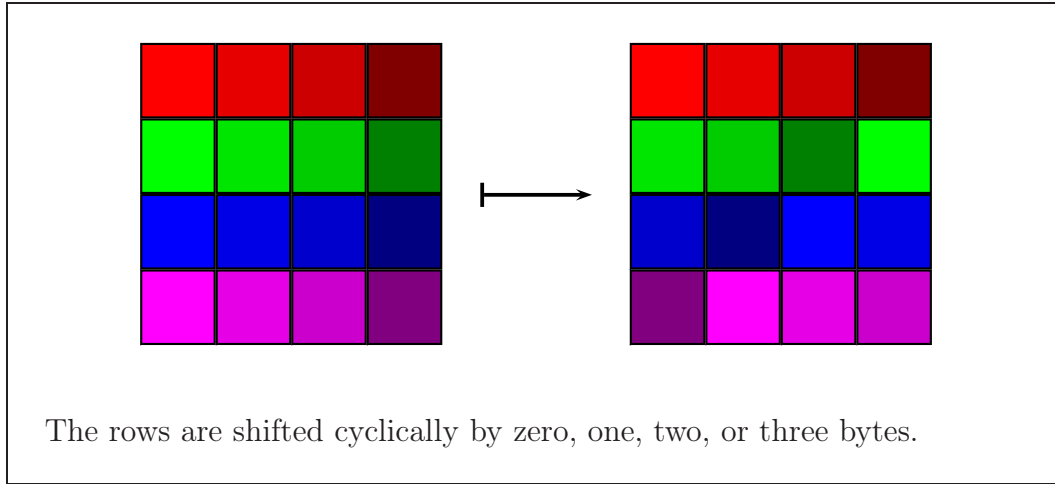


Figure 1.4: The ShiftRows operation

$R = \mathbb{F}_{2^8}[z]/(z^4 + 1) \ni a_0 + a_1z + a_2z^2 + a_3z^3$,

where $a_i \in \mathbb{F}_{2^8}$.

Addition: coefficient-wise $(a + b)_i = a_i + b_i$, XOR.

Multiplication: as for polynomials modulo $z^4 + 1$. Another way to express $d = a \cdot b$ is by the following matrix equation:

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Not a field: $(z + 1)^4 = 0$.

Figure 1.5: Polynomials over the field \mathbb{F}_{2^8}

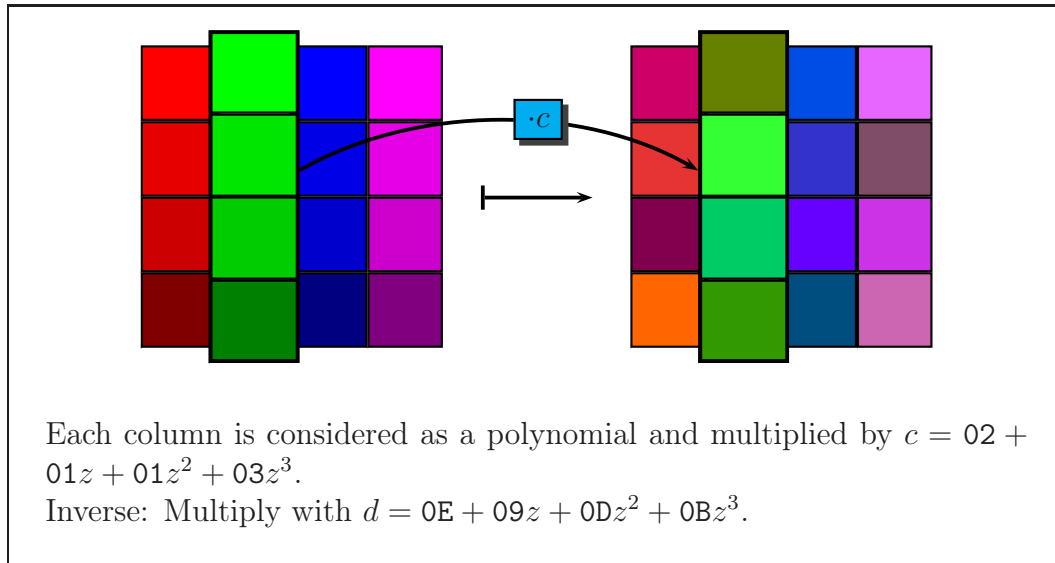


Figure 1.6: The MixColumns operation

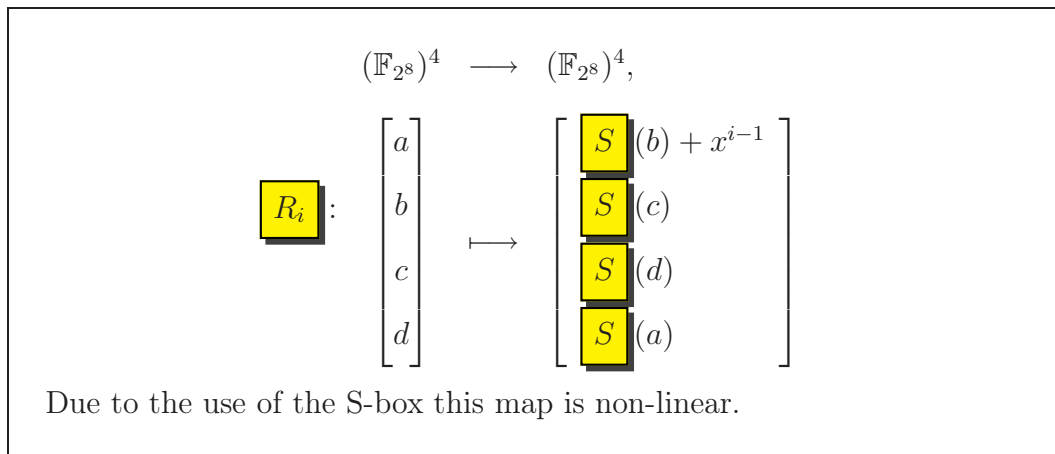


Figure 1.7: Nonlinear part of the key schedule

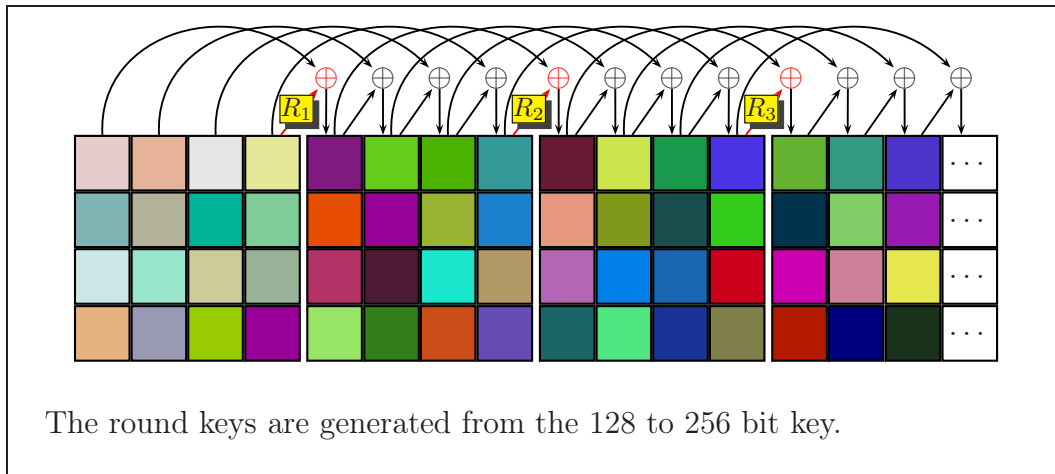


Figure 1.8: The Key Schedule

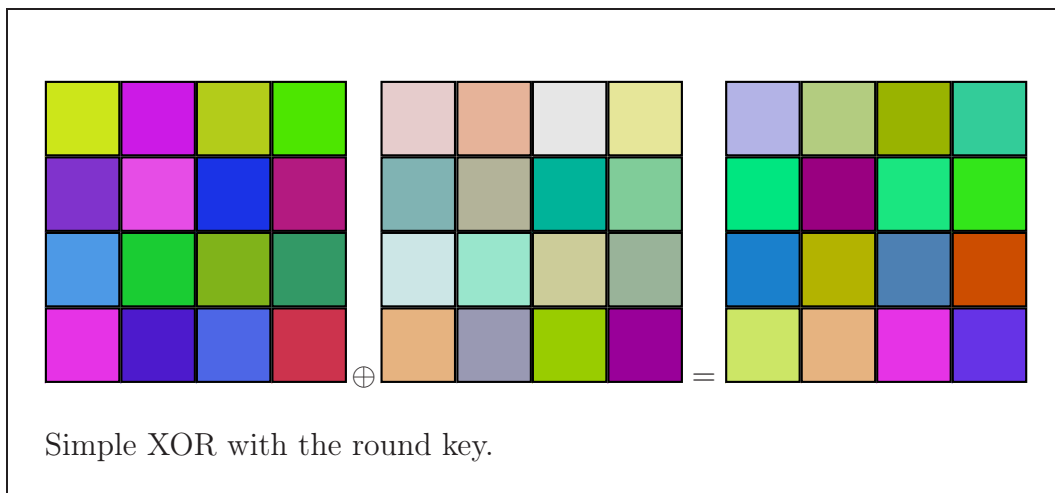


Figure 1.9: The AddRoundKey operation

most practical purposes. But it was still the standard and thus in heavy use ...

The US NIST, successor agency of the NBS, opened on 12 September 1997 a competition for the AES, to replace DES. The requirements were for a block cipher with blocks of 128 bits, and possible key lengths of 128, 192, and 256 bits. Not surprisingly, the specifications were rather more precise than in their 1973 competition which led to the adoption of DES. 15 candidates were submitted to NIST, and pared down to a short list of five systems by August 1999. These included *MARS* from IBM's Don Coppersmith, one of the chief designers of DES, *RC6* developed by Ron Rivest and three collaborators for RSA Laboratories, *Serpent* by Anderson, Biham, and Knudsen, and *Twofish* by Bruce Schneier's Counterpane Company. On 2 October 2000, the NIST announced the winner: AES, a system developed by the Belgian cryptographers Joan Daemen and Vincent Rijmen and originally called *Rijndael*. NIST expects this system to be secure for the next thirty years.

NIST was generally lauded for an open and well-documented procedure. One of its requirements was to make plausible that there are no hidden trapdoors, thus alleviating some of the concerns that had surrounded the DES standardization in 1976.

The features that secured Rijndael's first place in a tough competition are security—resistance against all currently known attacks—and efficiency—on a wide variety of platforms, from 8 bit smartcards to 32- or 64-bit processors.

AES encrypts a message of 128 bits using a key of 128, 192, or 256 bits. It is an *iterated cipher*, in which a sequence of four operations is applied a certain number of times. Thus it consists of 10 *rounds* at key length 128 (12 rounds at 196 and 14 rounds at 256 bits), and each round of these four operations, except that the first round only executes ADD ROUND KEY, and the last one leaves out MIX COLUMNS. Each operation turns a 128-bit word into another 128-bit word. To describe the operations, each 128-bit word is treated as a 4×4 matrix (or array, or block) of 8-bit bytes:

$$(1.1) \quad \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

The four operations have the following features:

- SUBBYTES substitutes each single byte by another value,
- SHIFTRROWS permutes the bytes in each row,
- MIXCOLUMNS performs a linear transformation on each column of the matrix,

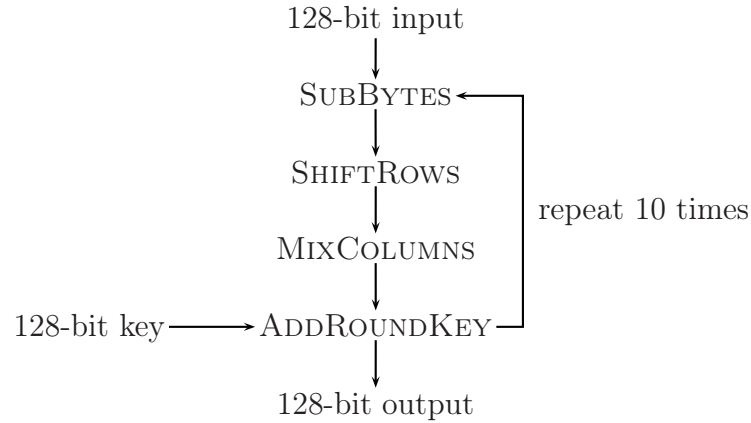


Figure 1.10: The overall structure of AES

- ADDROUNDKEY adds the key to the whole matrix.

Figure 1.10 illustrates the global view. The four operations in the middle constitute one round. For the first round, the key is explicitly provided as the secret key to the procedure. From this, the keys for the later rounds are calculated by the *key schedule*.

We now describe in more detail the four operations, assuming that the reader is familiar with the material in Sections ?? through ?. We see many cryptosystems in this book, including RSA and group-based cryptography, say with elliptic curves which by their nature require some algebra. But AES is the winner in a competition for bit-oriented (or Boolean) cryptography. The elegant algebraic description that follows is witness to the *unreasonable effectiveness of algebra* in cryptography. cite unreasonable

SUBBYTES. The basic unit processed is an 8-bit byte $a = (a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0) \in \{0, 1\}^8$. The fundamental operations on these bytes are addition and multiplication. The sum

$$c = a + b$$

of two bytes simply has the sum modulo 2 (or the exclusive-or) in each position:

$$c_i = a_i + b_i$$

for $0 \leq i \leq 7$. For example, if we take

$$(1.2) \quad a = (10011011), b = (11001101),$$

then

$$(1.3) \quad c = a + b = (01010110).$$

For multiplication, we might first consider the byte a to represent the polynomial

$$a_7x^7 + a_6x^6 + \cdots + a_1x + a_0,$$

so that a as in (1.2) now represents

$$x^7 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x].$$

The product $a \cdot b$ of two bytes a and b is calculated by multiplying the two polynomials, giving a polynomial of degree not more than 14. The product of the polynomials from (1.2) is

$$p = x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^3 + x^2 + x + 1.$$

Note that we work over \mathbb{F}_2 , so that all coefficients are reduced modulo 2. More details are given in ??.

We have an obvious problem: the result has up to 15 bits, but we should come up with just one byte. Algebra provides an elegant solution: reduce modulo a polynomial of degree 8. Indeed, in AES we work in the finite field \mathbb{F}_{256} defined by the irreducible polynomial

$$m = x^8 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x],$$

so that $a \bmod m \in \mathbb{F}_2[x]/\langle m \rangle = \mathbb{F}_{2^8} = \mathbb{F}_{256}$.

Now we divide p by m with remainder, obtaining

$$(1.4) \quad \begin{aligned} p &= (x^6 + x^5 + x^3) \cdot m + (x^4 + x^3 + x^2 + x + 1), \\ a \cdot b &= (00011111) \quad \text{in } \mathbb{F}_{256}. \end{aligned}$$

Thus we are back to degree at most 7, or 8 bits. Multiplication in \mathbb{F}_{256} maps two bytes to one byte. But in SUBBYTES, we have only one byte as input. How can we use the arithmetic in \mathbb{F}_{256} ? The answer is: inversion.

Since \mathbb{F}_{256} is a field, every nonzero element $a \in \mathbb{F}_{256}^\times$ has an inverse $a^{-1} \in \mathbb{F}_{256}^\times$. This can be calculated by the Extended Euclidean Algorithm (Section 16.14). We extend this mapping to all of \mathbb{F}_{256} by simply mapping zero to itself:

$$\text{inv}(a) = \begin{cases} a^{-1} & \text{if } a \neq \mathbf{0}, \\ \mathbf{0} & \text{if } a = \mathbf{0}, \end{cases}.$$

where $\mathbf{0} = (00000000)$. In our example (1.2), the Extended Euclidean Algorithm produces

$$(1.5) \quad (x^7 + x^3) \cdot a + (x^6 + x^3 + x^2 + x + 1) \cdot m = 1 \quad \text{in } \mathbb{F}_2[x],$$

so that indeed $\gcd(a, m) = 1$ in $\mathbb{Z}_2[x]$, and

$$\text{inv}(a) = (10001000) \quad \text{in } \mathbb{F}_{256}.$$

AES also uses a similar, yet different, algebraic structure on bytes, namely the ring $R = \mathbb{F}_2[x]/\langle x^8 + 1 \rangle$. This is not a field, since $x^8 + 1 = (x + 1)^8$ is not irreducible in $\mathbb{F}_2[x]$. Thus a byte $(a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0) \in \{0, 1\}^8$ now represents the element

$$a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \bmod (x^8 + 1) \in R.$$

Addition is, again, just the bit-wise addition (or exclusive-or). Thus (1.3) is also valid in R . Multiplication of two such polynomials gives a polynomial of degree at most 14, whose remainder modulo $x^8 + 1$ has again degree at most 7. Reduction modulo $x^8 + 1$ is particularly easy, since it corresponds to just adding the lower and the upper half of the polynomial, in the following sense. We split

$$c = c_1x^8 + c_0$$

into its upper and lower halves $c_1, c_0 \in \mathbb{F}_2[x]$ of degree at most 7, then

$$\begin{aligned} c &= c_1(x^8 + 1) + (c_1 + c_0) \equiv c_1 + c_0 \bmod (x^8 + 1), \\ c &= c_1 + c_0 \quad \text{in } R. \end{aligned}$$

To multiply the two bytes a and b in (1.2) in this new representation, we write their product as

$$p = (01101101) \cdot x^8 + (01100111),$$

and then their product in the ring R is the sum of these two bytes:

$$(10011011) \cdot (11001101) = (00001010).$$

In AES, actually only multiplication in R by the fixed polynomial

$$t_1 = (00011111) = x^4 + x^3 + x^2 + x + 1$$

is used, and only the polynomial

$$t_0 = (01100011) = x^6 + x^5 + x + 1$$

is added to others. Since t_1 is invertible modulo $x^8 + 1$, multiplication of bytes by t_1 corresponds to an invertible linear transformation over \mathbb{F}_2 . For a byte a , the bits in

$$b = t_1 \cdot a + t_0$$

can also be described by the affine linear transformation

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

To sum up, SUBBYTES consists of applying to each byte a in the block individually the following steps:

$$\begin{aligned} a &\longleftarrow \text{inv}(a) \quad (\text{in } \mathbb{F}_{256}), \\ a &\longleftarrow t_1 \cdot a \quad (\text{in } R), \\ a &\longleftarrow a + t_0. \end{aligned}$$

SHIFTRows. The operation SHIFTRows shifts each of the four rows cyclically to the left by 0, 1, 2 and 3 places, respectively. Thus SHIFTRows applied to the block (1.1) yields the array

$$(1.6) \quad \begin{array}{cccc} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{11} & a_{12} & a_{13} & a_{10} \\ a_{22} & a_{23} & a_{20} & a_{21} \\ a_{33} & a_{30} & a_{31} & a_{32} \end{array}.$$

MIXColumns. Here we consider an array $a = (a_3, a_2, a_1, a_0)$ of four bytes a_3, a_2, a_1 , and a_0 as a polynomial

$$a_3y^3 + a_2y^2 + a_1y + a_0 \in \mathbb{F}_{256}[y]$$

of degree at most 3. Addition of such polynomials again corresponds to a bit-wise exclusive-or. Multiplication gives a polynomial of degree at most 6 which is then decreased to degree at most 3 by reducing the result modulo

$$y^4 + 1 \in \mathbb{F}_{256}[y].$$

Thus in effect we are working in the ring

$$S = \mathbb{F}_{256}[y] / \langle y^4 + 1 \rangle$$

with 256^4 elements. As $x^8 + 1$ above, $y^4 + 1 = (y + 1)^4$ is not irreducible in $\mathbb{F}_{256}[y]$, hence S is not a field. Reduction modulo $y^4 + 1$ is again particularly easy:

$$a_1y^4 + a_0 = a_1 + a_0 \text{ in } S.$$

In fact, this multiplication is only applied when one factor is the fixed polynomial

$$(1.7) \quad c = (00000011) \cdot y^3 + (00000001) \cdot y^2 + (00000001) \cdot y + (00000010)$$

in $\mathbb{F}_{256}[y]$. Using the hexadecimal abbreviations 03, 01, 01, and 02 for the four coefficients, the product of c with $a = (a_3, a_2, a_1, a_0)$ can also be described as the 4-byte word $b = (b_3, b_2, b_1, b_0)$ given by the matrix-vector product

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}.$$

The operations on individual bytes are those in $\mathbb{F}_{256} = \mathbb{F}_2[x]/\langle m \rangle$, as above. We take the example

$$\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} 02 \\ 01 \\ 80 \\ A0 \end{pmatrix}.$$

Then

$$\begin{aligned} b_3 &= 03 \cdot 02 + 01 \cdot 01 + 01 \cdot 80 + 02 \cdot A0 \\ &= (x+1) \cdot x + 1 \cdot 1 + 1 \cdot x^7 + x \cdot (x^7 + x^5) \\ &= x^8 + x^7 + x^6 + x^5 + x^2 + x + 1. \end{aligned}$$

Since $x^8 = x^4 + x^3 + x + 1$ in \mathbb{F}_{256} , we have

$$b_3 = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 = (11111100) = FC.$$

It is interesting to note the three roles that the byte 11111100 plays here: first as an element of \mathbb{F}_{256} , represented by a polynomial in $\mathbb{F}_2[x]$ of degree 7, then as an 8-bit string, and finally a 2-letter hexadecimal word. Even more interesting is the fact that we consider the byte as elements of different domains, such as in the inversion in \mathbb{F}_{256} or in the second step in SUBBYTES, and then a multiplication on the same data may yield completely different results depending on the underlying domain. This versatility is one aspect of the *unreasonable effectiveness* of algebra in cryptography.

ADDRoundKey. The 128-bit block and a round key of the same size are added bitwise.

In an implementation, it is usually advantageous to replace calculations by table look-up as far as possible. With a table of 4 kB, a round of AES can be executed with 16 table look-ups and 16 32-bit XORs.

In DES the *S*-boxes provide the only nonlinear functions. Their seemingly arbitrary structure had led some cryptographers to fear that some “trapdoor” might have been built in that enables the NSA to break the system. This allegation has never been substantiated.

In Rijndael, the nonlinear *S*-box is the SUBBYTES function. Its design, and that of the other parts, involves a few fundamental decisions such as to work in rings like $\mathbb{F}_2[x]/\langle m \rangle$ or to arrange things in $4 \times \ell_b$ byte blocks and to use row shifts. Given this, there are only very few arbitrary items such as the polynomials m, t_0, t_1 , and the amount of row shifting. The authors say convincingly: *We believe that the cipher structure does not offer enough degrees of freedom to hide a trap door.*

The design of AES involved many decisions about its special structure. However, the specific values that had to be chosen are very few, and can actually be

	Cryptosystems	
	private-key	public-key
Examples	one-time pad, ?, DES, AES	RSA, ?-?, ?
speed	+	—
authentication	+	—
key exchange	—	+

Table 1.1: Aspects of private-key and public-key cryptosystems.

“explained” as natural choices: the irreducible polynomial m is $??$, t_0 and t_1 in SUBBYTES are $??$, and c is $??$ explain choices MDS property of Mix Columns; see Wiki AES Mix Columns. Cache attacks: see Wiki AES.

1.2*. The RSA cryptosystem

We follow the long-standing tradition of calling the two players ALICE and BOB. Our scenario is that BOB wants to send a message to ALICE that she should be able to read, but nobody else. To this end, ALICE generates a *private key* S and a *public key* K . Anybody can read K ; imagine it is posted on the internet or in some large database. But she guards S carefully as her secret. BOB uses K to encrypt his message for ALICE. ALICE uses S — which is for her eyes only — to decrypt it. In a symmetric cryptosystem like AES, the encryption and decryption keys are (essentially) the same, but here K and S are different, and in fact S cannot be computed easily from K (hopefully).

The messages to be sent may be text, digitized pictures or sound, data or program files, etc. But we assume here and always in the future that the messages have been converted into some standard form, say into a (possibly very long) string of bits 0 and 1. How to perform this conversion best depends very much on the type of data. For text, a common way is to use ASCII or extended ASCII encoding of letters into 7-bit or 8-bit strings, respectively.

BOB now wants to send this string of bits. There is a security parameter n to be explained in a minute. BOB splits his string into blocks of $n - 1$ bits each, and transmits each block separately. So we now explain how to transmit a single block (x_0, \dots, x_{n-2}) of $n - 1$ bits. We interpret this as the binary representation of the natural number $x = \sum_{i=0}^{n-2} x_i 2^i$. This number shall be transmitted.

The idea now is the following. ALICE chooses two prime numbers p and q at random with $n/2$ bits each, and computes their product $N = p \cdot q$, which has about n bits. She also chooses some random integer exponent e with $1 \leq e < N$. ALICE’s public key is $K = (N, e)$. BOB looks it up and sends the remainder $y = x^e \bmod N$ of x^e on division by N to ALICE. The magic now is that ALICE can recover x from BOB’s message with the help of her private information

derived from (p, q) . Here is the system described in full. The required algebraic terminology is explained in the *computer algebra toolbox* of ??.

CRYPTOSYSTEM 1.8. RSA.

Input: Security parameter n , an integer.

Before starting any communication, ALICE (and each other user) performs the following setup:

1. She chooses two distinct primes p and q at random with $2^{n/2-1} < p, q < 2^{n/2}$, and so that their product is an n -bit number.
2. She calculates $N = p \cdot q$ and $\varphi(N) = (p-1)(q-1)$. [This is Euler's phi function.]
3. She chooses $e \in \{2, \dots, \varphi(N) - 2\}$ at random, coprime to $\varphi(N)$.
4. She calculates the inverse d of e modulo $\varphi(N)$.
5. She publishes her public key $K = (N, e)$ and keeps $S = (N, d)$ as her private key.
6. After this setup, ALICE may forget p, q , and $\varphi(N)$, and may erase them in her computer.

Now BOB wants to transmit the plaintext x to ALICE. What do they do?

7. BOB knows ALICE's public key (N, e) and the plaintext x . He calculates $y = x^e \bmod N$ and sends this to ALICE.
8. ALICE knows her own secret key (N, d) and the ciphertext y . She now calculates $x^* = y^d \bmod N$.

This finishes the description of the system. We insist on N being an n -bit number, that is, $2^{n-1} \leq N < 2^n$. A simple way to achieve this is by choosing p and q in the interval $[2^{(n-1)/2}, \dots, 2^{n/2}]$. Here is a simple example.

EXAMPLE 1.9. We take $n = 6$. Literally, we would be looking for primes between 7 and 8, but at such small values we are a bit more liberal, and choose $p = 5$ and $q = 11$. Thus $N = 55$ is a 6-bit number, and $\varphi(N) = 40$. We choose $e = 13$. Using the EEA, we find in a single step that $-3 \cdot 13 + 40 = 1$, so that $d = e^{-1} = -3 = 37$ in \mathbb{Z}_{40} . Thus ALICE publishes her public key $K = (55, 13)$ and keeps her private key $S = (55, 37)$. This finishes the setup phase.

Now BOB wants to send a message to ALICE, say $x = 6$. Thus he has to calculate $y = x^e = 6^{13}$ in \mathbb{Z}_{55} . The obvious way to do this is to compute the integer 6^{13} and take its remainder modulo 55. This would be quite cumbersome here, and utterly infeasible at practical values of the security parameter n , where x^e would have more bits than there are elementary particles in the universe. But

there is an easy way out: we calculate x^e in small steps, reducing modulo 55 at each step.

The binary representation of $13 = 8 + 4 + 1 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$ is 1101, and BOB first calculates the powers with exponents 2^i :

i	0	1	2	3
2^i	1	2	4	8
6^{2^i}	6	36	31	26 in \mathbb{Z}_{55}

Now he multiplies those results together for which a 1 occurs in the binary representation: $y = 51 = 31 \cdot 51 \cdot 6 = 6^8 \cdot 6^4 \cdot 6^1 = 6^{8+4+1} = 6^{13}$ in \mathbb{Z}_{55} . This efficient way of calculating a large power is called *repeated squaring* and discussed in ??.

Now BOB has done his share of calculation and sends y to ALICE. She decrypts in the same way, using the binary representation 100101 of 37:

i	0	1	2	3	4	5
2^i	1	2	4	8	16	32
51^{2^i}	51	16	36	31	26	16 in \mathbb{Z}_{55}

and computing $x^* = 16 \cdot 36 \cdot 51 = 6 = 51^{32} \cdot 51^4 \cdot 51^1 = 51^{37}$ in \mathbb{Z}_{55} and indeed, $x^* = x = 6$ is the message that BOB wanted to send to ALICE. \diamond

We have to address several questions.

1. **Correctness:** is $x^* = x$?
2. **Easy handling:** How to calculate fast ...
 - ... large primes at random?
 - ... d from e ?
 - ... powers modulo N ? This has to be done for each message, and speed is even more a concern than for the previous two points.
3. **Security:** Suppose that an eavesdropper—traditionally called EVE—listens in to the communications between ALICE and BOB. Thus EVE knows y and, of course, (N, e) , and she would like to compute x . In fact, x is uniquely determined! But how long does it take to calculate this? Is this difficult enough?

Some of these questions are addressed in ??.

There are many facets to the security problem. We might be concerned about an EVE who has already seen some valid plaintext-ciphertext pairs (x, y) — the *known plaintext attack* — or even (x, y) where EVE has selected x to suit her purposes — the *chosen plaintext attack* (an example is mentioned on page ??).

Her goal is to compute x from y for another pair (x, y) . But even a weaker goal might be destructive to the cryptosystem: computing some information about x (say: is x even?) from y , and maybe not always correctly, but slightly better than guessing. These issues are discussed in ? .

There are two frameworks in which to discuss these questions. In the *asymptotic model*, we have a security parameter n for our system. Typically n is defined via the key length. In RSA, we have n -bit integers N, e and d , and so the public and secret keys both are $2n$ bits long. For easy handling, “fast” means computing time polynomial in n as a first approximation.

In the *concrete model*, we have a fixed system, say RSA with $n = 1024$, and will usually discuss practical attacks on that particular system. This is the only approach for AES that are fixed, and also for parameterized systems like like RSA it gives a basis for practical comparisons, as in ??.

1.3. Visual cryptography

The goal is to have a direct visual representation of a secure symmetric cryptosystem such as the one-time pad (which is described in Section 2.1). In its simplest variant, this scheme of Naor & Shamir (1995) transmits an image by first creating a random image as private key and then a second image depending on it and the message. By itself, this second image is again random.

For illustration, suppose a company manager stays at a hotel for negotiations with another company. If she requires information from home, maybe a blueprint or picture, her company sends her the second image by fax. Anyone seeing this fax alone obtains no information. But she can superimpose her secret key slide, which she took with her, on the fax and see the message.

Before we explain the workings, you should play with the toys provided here. Put the key transparency on either of the two printed images (Figures 1.11 and 1.12) and see if you recognize the cleartext.

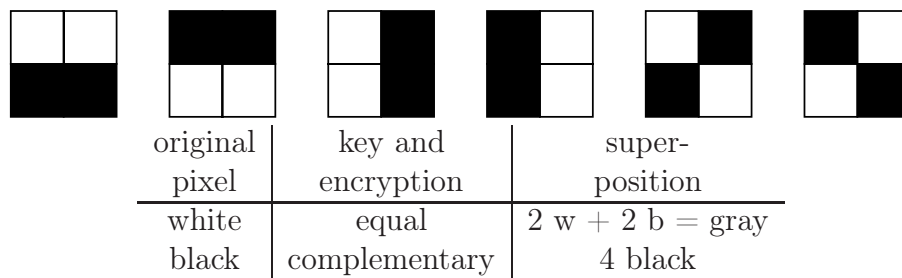


Figure 1.11:

How is this achieved? The cleartext image is split into square pixels, each of which is either black or white. Each pixel is further divided equally into four

square subpixels. Both in the random key and in the encrypted message, exactly two of the four subpixels are black, and two are white. There are six possible arrangements of two blacks in a 2×2 square. For the random key, one of the six is chosen uniformly at random, and independently for each of the many pixels. For the encryption, we choose the same arrangement as on the key if the cleartext pixel is white, and the complementary one if the cleartext pixel is black. If we then superimpose the key and the encryption, we have exactly two or four subpixels black if the cleartext pixel is white or black, respectively. This can be viewed as a visual variant of the one-time pad, discussed in Section 2.1.

In this system, we can even create *secret ink*. We take two images A and B whose superposition gives image C, according to the correspondence in Figure 1.12.

images A and B		white	\longleftrightarrow	2 white + 2 black
		black	\longleftrightarrow	1 white + 3 black
image C		white	\longleftrightarrow	1 white + 3 black
		black	\longleftrightarrow	4 black








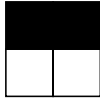




		A	B	A	B	A	B
		W	W	W	S	S	S
C	w						
C	s						

Figure 1.12: Sample pixels for secret ink



Chapter A

Substitution ciphers and frequency analysis

Most of this text is concerned with “modern” cryptography, which started in the 1970s.

But cryptography deals with such universal subjects—language and communication—that it has accumulated a rich history over the centuries of proud inventors and secretive cryptanalysts, famous people and amusing tales, redolent with fascinating characters and episodes, towering victories and abysmal failures. In this and some other chapters we present an eclectic selection of such stories. On these few pages, the goal is not a complete or balanced account. Rather we concentrate on a few systems, individuals, and happenings. If you find these glimpses to your liking, you might turn to the real thing: David Kahn’s monumental work *The Codebreakers* from 1967, still unsurpassed today.

A.1. Cryptographic primitives

Over the millenia, people have invented and used a bewildering array of cryptosystems for the secret transmission of messages. In this section, we establish a general framework into which these systems fit. This is a scientific approach and rather ahistorical. To assess the contributions of individuals over the centuries in a fair way, one has to look at them in the context of contemporary knowledge, not with modern 20/20 hindsight. However, our hindsight helps us to sort ideas and see when new things have emerged.

There are two fundamental cryptographic primitives:

- substitution,
- transposition.

In Claude Shannon's terminology, these are *confusion* and *diffusion*, and the goal is to create enough of one of them, or preferably of both, to provide secrecy in communication. There is also a modern notion of *cryptographic primitives* which includes one-way and trapdoor functions; however, in this chapter we are only concerned with historical cryptography.

In a substitution, we have some "alphabet" \mathbb{X} . This might be the 26-letter English alphabet $\mathbb{A} = \{a, b, c, \dots, x, y, z\}$, or pairs of letters (bigrams), so that $\mathbb{X} = \mathbb{A}^2$, or even longer polygrams, or bits $\mathbb{B} = \{0, 1\}$, or 128-bit words $\mathbb{X} = \mathbb{B}^{128}$ for AES. In general, \mathbb{X} is an arbitrary finite set. Furthermore, we have another alphabet \mathbb{Y} , which might equal \mathbb{X} or not.

Then a substitution is just a mapping $\sigma: \mathbb{X} \longrightarrow \mathbb{Y}$ which associates to any element x of \mathbb{X} an element $y = \sigma(x)$ of \mathbb{Y} . In the examples that follow, we try to be brief and make liberal use of forward references. The neophyte reader should first get familiar with the forward material, and then go back and look at it from this general point of view.

- EXAMPLE A.1. (i) AES (Section 1.1*) uses two substitutions. The first is the fixed substitution $\sigma = \text{SubByte}: \mathbb{F}_{256} \longrightarrow \mathbb{F}_{256}$ with $\sigma(x) = x^{-1}$ if $x \neq 0$, and $\sigma(0) = 0$. The second one is the key addition $\sigma = \text{AddRoundKey}: \mathbb{B}^{128} \longrightarrow \mathbb{B}^{128}$, where the 128-bit key (which we consider as fixed) and state are added bitwise.
- (ii) RSA (Section 1.2*) with public key (N, e) is the substitution $\sigma: \mathbb{Z}_N \longrightarrow \mathbb{Z}_N$ with $\sigma(x) = x^e$.
- (iii) The Caesar cipher (Section A.3) identifies \mathbb{A} with \mathbb{Z}_{26} and uses the substitution $\sigma: \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}$ with $\sigma(x) = x + 3$. More generally, we might have any key $k \in \mathbb{Z}_{26}$ and use $\sigma(x) = x + k$.
- (iv) A simple substitution (Section A.3) is a bijection $\sigma: \mathbb{A} \longrightarrow \mathbb{Y}$ from letters to some alphabet \mathbb{Y} .
- (v) The de Vigenère cipher (Section B.1) with an ℓ -letter keyword k uses ℓ Caesar substitutions $\sigma_0, \dots, \sigma_{\ell-1}$. Alternatively, it can be viewed as a simple substitution $\sigma: \mathbb{A}^\ell \longrightarrow \mathbb{A}^\ell$ with $\sigma(x) = x + k$, using letter-wise addition. For an example, we take the rather unimaginative keyword $k = \text{key}$ of length $\ell = 3$, and encrypt the cleartext $x = \text{confuse the enemies}$ as follows:

x	=	confuse the enemies
k'	=	keykeykeykeykeyke
y	=	mslpyqoxfoiloqgow

Thus $\sigma(x) = x + k'$, where k' is the 17-letter key obtained by the de Vigenère key scheduled from $k = \text{key}$, namely sufficiently long repetition (with the Procrustes rule to make things fit at the end).

The attentive reader has noticed that in this short example, we have no fewer than four single-letter additions $e + k = o$. This is a general phenomenon, although usually not this frequent, and will be used in Chapter D to break this cryptosystem.

The alphabet Table A.1 below may be useful for checking the letter addition.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Table A.1: Letter-number conversion in a 26-letter alphabet.

More generally a *multiple substitution* applies a fixed sequence of simple substitutions one after the other. When the sequence is exhausted, one starts again with the first one.

- (vi) As a generalization of simple substitutions, a relational substitution works in the same way, only for each letter we have not just a single possibility but several ones. We see an example in Tranchedini's codebook from 1463 in Figure D.1 below. Its first line (after the heading) gives the 21 letters A, b, . . . , z of the alphabet, plus the frequent words for and, with, and of. Five of the letters get three possible encryptions, the others two. In general, the goal of the multiple possibilities is to even out the disparate frequencies of the various letters. The corresponding σ is now only a relation, not necessarily a function. In the classical terminology, two ciphertext values corresponding to the same cleartext value are called *homophones*.
- (vii) Nomenclators and codebooks (Chapter D) have large alphabets \mathbb{X} and \mathbb{Y} , with several hundreds (in the 17th century) or thousands (19th century) of elements each. \mathbb{Y} has at least as many elements as \mathbb{X} does, and the codebook is a simple substitution $\sigma: \mathbb{X} \rightarrow \mathbb{Y}$. The alphabet \mathbb{X} usually comprises letters, plus certain frequently occurring items, such as syllables, or words and names that were likely to appear in the correspondence. Their use is recorded from 1377 to the Second World War, where in one German submarine cipher each square of a grid covering the North Atlantic was given its code. More examples are in Chapter D.

- (viii) The basic ingredient of the one-time pad (Section 2.1) is a substitution σ on single bits, where a (random) key bit k is chosen in \mathbb{B} , and a one-bit message $x \in \mathbb{B}$ is encrypted as $\sigma(x) = x + k$. Longer messages are encrypted by repeating this procedure, with keys chosen anew (independently) for each message bit.
- (ix) The Playfair cipher (??) is a simple substitution $\sigma: \mathbb{A}_0^2 \rightarrow \mathbb{A}_0^2$ on bigrams, where $\mathbb{A}_0 = \mathbb{A} \setminus \{j\}$ is the standard alphabet with j removed.
- (x) In the Enigma (Chapter G), the secret key determines (in a complicated fashion) a sequence of simple substitutions $\sigma_0, \sigma_1, \dots$, with $\sigma_i: \mathbb{A} \rightarrow \mathbb{A}$ for all i . \diamond

A further classical security measure was the introduction of dummies (or null values, or nulls). These are encrypting symbols that will be discarded by the legitimate decryptor, but whose presence is intended to confuse the cryptanalyst. Figure D.1 below shows a system from 1463 by Tranchedini, with twelve dummies in the fifth line of the text. The Spanish cipher from around 1590 in Figure D.3 contains the line: *Las nullas tendran una raya enzima, exemplo* $\overline{19}$.¹ This provides a systematic way of introducing a large number of dummies.

For the second cryptographic primitive, we have a length parameter ℓ . A **transposition** is simply a bijection (or permutation) on the first ℓ numbers:

$$\tau: \{0, \dots, \ell - 1\} \rightarrow \{0, \dots, \ell - 1\}.$$

When we have, in addition, an alphabet \mathbb{U} , this leads to a substitution $\tau_{\mathbb{U}}$ on words of ℓ letters from \mathbb{U} by taking the cleartext $x = (x_0, \dots, x_{\ell-1}) \in \mathbb{U}^{\ell}$ and rearranging it as the ciphertext $y = (y_0, \dots, y_{\ell-1}) \in \mathbb{U}^{\ell}$ by interchanging positions according to τ . That is, the letter x_i in cleartext position i is moved to ciphertext position $\tau(i)$: $y_{\tau(i)} = x_i$. If $\alpha = \tau^{-1}$ is the inverse of τ , then we can write

$$y = (x_{\alpha(0)}, x_{\alpha(1)}, \dots, x_{\alpha(\ell-1)}).$$

EXAMPLE A.2. (i) AES uses two transpositions: ShiftRow and MixColumns. The first performs certain cyclic shifts on the rows of the state matrix, and the second produces a more complicated mixing of the columns of that matrix. Both are explained in ??.

- (ii) In a single columnar transposition (Section E.2) we write the cleartext in r rows of length c and read it off in columns as the ciphertext. Thus $x =$ column becomes $y = \text{c1moun} = x_0x_2x_4x_1x_3x_5$ in an $r \times c = 3 \times 2$ array:

¹The nulls will have a bar above, for example $\overline{19}$.

$$x = \begin{array}{cc} \text{c} & \text{o} \\ \text{l} & \text{u} \\ \text{m} & \text{n} \end{array}$$

The transposition τ and its inverse α are given by

i	0	1	2	3	4	5
$\tau(i)$	0	3	1	4	2	5
$\alpha(i)$	0	2	4	1	3	5

and one checks that $\tau(i) = 3i - 5\lfloor i/2 \rfloor$.

(iii) The grille (??) is a transposition on a square array.

(iv) The skytale (Section E.1) can be viewed as a columnar transposition. \diamond

From a transposition τ on ℓ numbers we obtain, for any alphabet \mathbb{U} , a substitution $\tau_{\mathbb{U}}: \mathbb{U}^{\ell} \rightarrow \mathbb{U}^{\ell}$ by setting $\tau_{\mathbb{U}}(x) = x_{\alpha(0)}x_{\alpha(1)} \cdots x_{\alpha(\ell-1)}$ for $x \in \mathbb{U}^{\ell}$, where α is the inverse of τ . This is illustrated in Example A.2(ii). Thus a transposition of length ℓ yields a simple substitution on ℓ -grams. However, it is profitable to keep the two primitives apart. For one, τ as above is much less “powerful” than a general substitution on \mathbb{U}^{ℓ} , and furthermore, τ works for any \mathbb{U} and might be called a “scheme” for such substitutions. From a higher point of view, substitutions are semantic objects and transpositions of a syntactical (or combinatorial) nature.

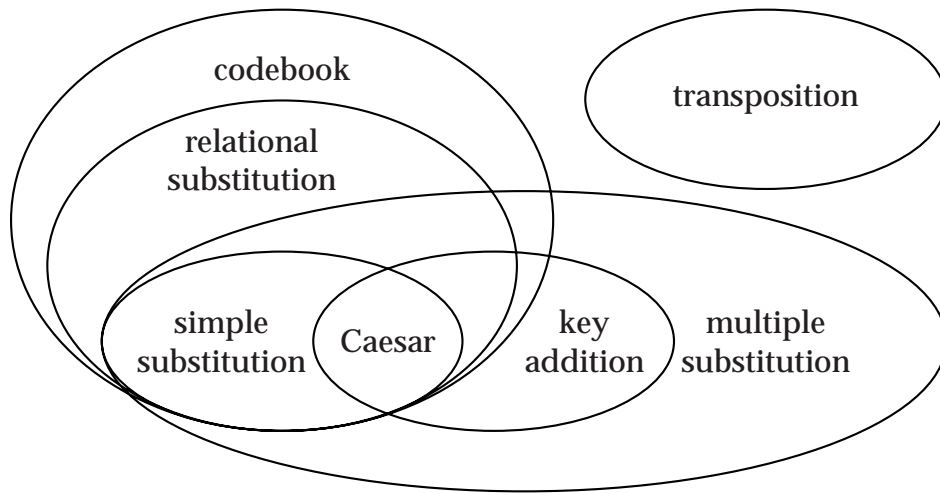


Figure A.1: A taxonomy of cryptosystems.

Once we have the primitives, we need two operations to work with them:

- chaining,
- composition (classically called superencipherment).

The primitives work on messages of a fixed length, maybe single letters, or bigrams, or 128-bit words. In order to transmit messages of arbitrary length, one has to “chain” such fixed-length primitives together. The most common mode is to just repeat the primitive as often as necessary. When the primitive is key-driven, there are other ways of chaining them together. For example, in the cipher-block chaining (or autokey) mode one uses the output of the previous application as key for the next one; see ???. A characteristic of modern cryptosystems is that they operate on uniform data formats for input, output, and key, so that the basic operations can be composed and iterated in many rounds.

In particular, when we have a substitution $\sigma: \mathbb{X} \longrightarrow \mathbb{Y}$ and some number ℓ , we can apply σ independently to each of ℓ elements from \mathbb{X} and thus obtain $\sigma^\ell: \mathbb{X}^\ell \longrightarrow \mathbb{Y}^\ell$ with

$$\sigma^\ell(x_0, \dots, x_{\ell-1}) = (\sigma(x_0), \dots, \sigma(x_{\ell-1}))$$

for any $x_0, \dots, x_{\ell-1} \in \mathbb{X}$ is their composition. Then σ^ℓ is called the ℓ -fold product substitution derived from σ .

The second operation is the composition of two substitutions ρ and σ . For this to work, we have $\rho: \mathbb{X} \longrightarrow \mathbb{Y}$ and $\sigma: \mathbb{Y} \longrightarrow \mathbb{Z}$, and then $\sigma \circ \rho: \mathbb{X} \longrightarrow \mathbb{Z}$ with

$$(\sigma \circ \rho)(x) = \sigma(\rho(x))$$

for any $x \in \mathbb{X}$ is their composition. When $\sigma: \mathbb{A} \longrightarrow \mathbb{A}$ is the Caesar cipher, shifting by three positions, then $\sigma^2 = \sigma \circ \sigma: \mathbb{A} \longrightarrow \mathbb{A}$ is the shift by six positions.

The most profitable application is when we start with a substitution $\sigma: \mathbb{X} \longrightarrow \mathbb{X}$ and a transposition τ on ℓ numbers. Then we have the product substitution $\sigma^\ell: \mathbb{X}^\ell \longrightarrow \mathbb{X}^\ell$, and can compose it with the substitution $\tau_{\mathbb{X}}: \mathbb{X}^\ell \longrightarrow \mathbb{X}^\ell$ to obtain

$$\tau_{\mathbb{X}} \circ \sigma^\ell: \mathbb{X}^\ell \longrightarrow \mathbb{X}^\ell.$$

EXAMPLE A.3. (i) AES uses the four primitives SubByte, MixColumn, ShiftRow, and AddRoundKey. The basic substitution $\sigma: \mathbb{B}^8 = \mathbb{F}_{256} \longrightarrow \mathbb{B}^8 = \mathbb{F}_{256}$ has been discussed, and SubByte = $\sigma^{16}: \mathbb{B}^{128} \longrightarrow \mathbb{B}^{128}$ is the 16-fold product of σ . The other three primitives work on 128 bits, and their composition gives one round of AES. Finally, AES is the composition of 12 such rounds (with minor modifications in the first and last rounds).

(ii) A German code from the First World War (see Section F.2) involved a codebook $\sigma: \mathbb{X} \longrightarrow \mathbb{Y} \subseteq \mathbb{A}^3$, with \mathbb{X} and \mathbb{Y} consisting of several thousand

words, the latter being encoded by trigrams in a 29-letter alphabet \mathbb{A} , which includes ä, ö and ü. Furthermore, there was a simple substitution $\tau: \mathbb{A} \rightarrow \mathbb{A}$, and the complete cipher was $\tau^3 \circ \sigma$, that is, the codebook superenciphered by the simple substitution.

- (iii) We take the de Vigenère cipher σ with key length 3 from Example A.1(v), so that $\sigma: \mathbb{A}^3 \rightarrow \mathbb{A}^3$ is a substitution, and we take the columnar transposition τ from Example A.2(ii). Following the general recipe, we would consider

$$\rho = \tau_{\mathbb{A}^3} \circ \sigma^6: \mathbb{A}^{18} \rightarrow \mathbb{A}^{18},$$

which first performs the de Vigenère on six blocks of three letters each, and then interchanges the six blocks according to τ . Thus τ is applied to the matrix

msl	pyg
oxf	oil
oqg	owv

to yield the ciphertext

$$z_1 = \text{msloxfoqgpyqoilowv}.$$

However, we may also perform first the de Vigenère and then the transposition separately on each sixpack of consecutive letters:

$$(\tau_{\mathbb{A}})^3 \circ \sigma^6: \mathbb{A}^{18} \rightarrow \mathbb{A}^{18}.$$

That is, τ is applied to each of the following three 3×2 matrices individually

ms	ox	oq
lp	fo	go
yq	il	wv

to yield the ciphertext

$$z_2 = \text{mlyspqofixologwqov}.$$

See ?? for another example ?.

◇

We have appended a dummy letter x to the cleartext in order to make its length divisible by 6. It encrypts as $x + y = v$. The two options are not cryptographically equivalent: under the Kasiski attack of Section C.1, z_1 reveals the de Vigenère key length 3, but z_2 does not.

There is one further general ingredient: the many tools for efficient encryption and decryption, and for remembering keys. The de Vigenère table reduces the three steps

$$\text{letter} \longrightarrow \text{number} \xrightarrow{\text{key add}} \text{number} \longrightarrow \text{letter}$$

to a simple table look-up. The Alberti system helps to memorize a simple substitution, and an example is shown in Section A.4; the Playfair cipher (??) has a mnemonic component for its bigram substitution. And today, couldn't we do with a little help to remember all our pass phrases?

A generally useful mnemonic aid is given by the key addition systems. Here we think of the letters a, \dots, z as the numbers $0, \dots, 25$ and add a secret key to each number. As explained in Section A.3 and Chapters B and C, this includes the ? cipher, where 3 is added to each number, the de Vigenère cipher, where a longer keyword is added letter-by-letter, and the one-time pad (Section 2.1), where the key is random and as long as the message.

An even more amazing example is the RSA cryptosystem (Section 1.2*), which is just a simple substitution but, with a common key size of 1024 bits, the alphabet of 2^{1024} letters is so huge that frequency analysis is hopeless. The winning point here is to encode a substitution on such a huge alphabet in an extremely concise fashion, namely by its modulus and two exponents. We might even call this a *key exponentiation system*: the cleartext has to be multiplied with itself as many times as the key indicates.

A.2*. Brief history of cryptography

Over the centuries, several cryptographic systems have played the major role in professional use, mainly by the relevant government institutions: diplomatic, military, and secret services. The timeline in Figure A.4 tries to give an overview of the dominating systems throughout history. Of course, this has to leave out many of the finer points. In particular, it was not uncommon to mix two types of systems. A fundamental distinction is between the transposition systems, where individual letters are moved to other positions without being changed, and various types of substitution, where the units (letters, words, ...) are altered individually, but the flow of the message is not changed.

Historical completeness cannot be achieved in such a concise presentation, and some injustice to systems, attacks, and their inventors is inherent.

In the history of cryptography, we can distinguish several periods and indicate, very roughly, the corresponding time frames.

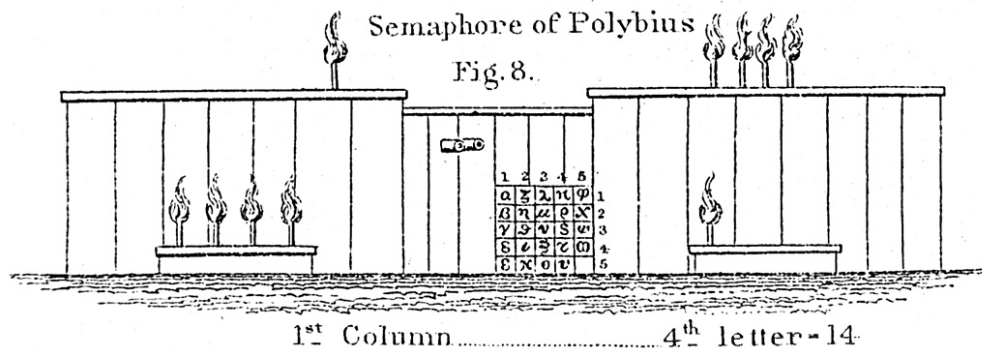


Figure A.2: Polybios' signalling system as interpreted by Myer (1879).

antiquity	1000 BC – 100 AD
Arab civilization	800 – 1200
European Middle Ages	1000 – 1500
Renaissance	1450 – 1600
Baroque, salon cryptography	1600 – 1850
mechanical devices	1580 – 1950
electromechanical devices	1920 – 1950
computers	1950 – present
public key systems	1977 - present

From antiquity, a few cryptographic tidbits have survived. In the beginning, the knowledge of writing was so exclusive that it did not require further protection.

There are some examples of Egyptian hieroglyphic cryptography from the Middle Kingdom time?. The usual writing system employed symbols at three levels: sound, word, and meaning. As an example, *ra* means *mouth*, and ?? can stand either for the letter *r* or the notion *mouth*. ?? is the letter *h*, and ?? is transliterated as *hr* and pronounced *khore*, rhyming with *more*. Its third letter ? is not pronounced but determines that the preceding word denotes a divine being. The known Egyptian cryptographic examples employ symbols that are not or very rarely used, but clearly denote some object, and then stand for the first letter of its name. They are usually inscriptions hewn into large stone slabs (*stelae*). Their purpose was not secret communication, but rather to create an aura of mystery, accessible only to the initiated. example

Like codebooks, also *Egyptian hieroglyphs* can denote either a single letter or a whole word. There is a third usage as *determinatives* where a symbol denotes the category into which the object falls.

In the Hebrew bible, a simple substitution occurs in a few places. The first letter is interchanged with the last, the second with the last but one, and so on.

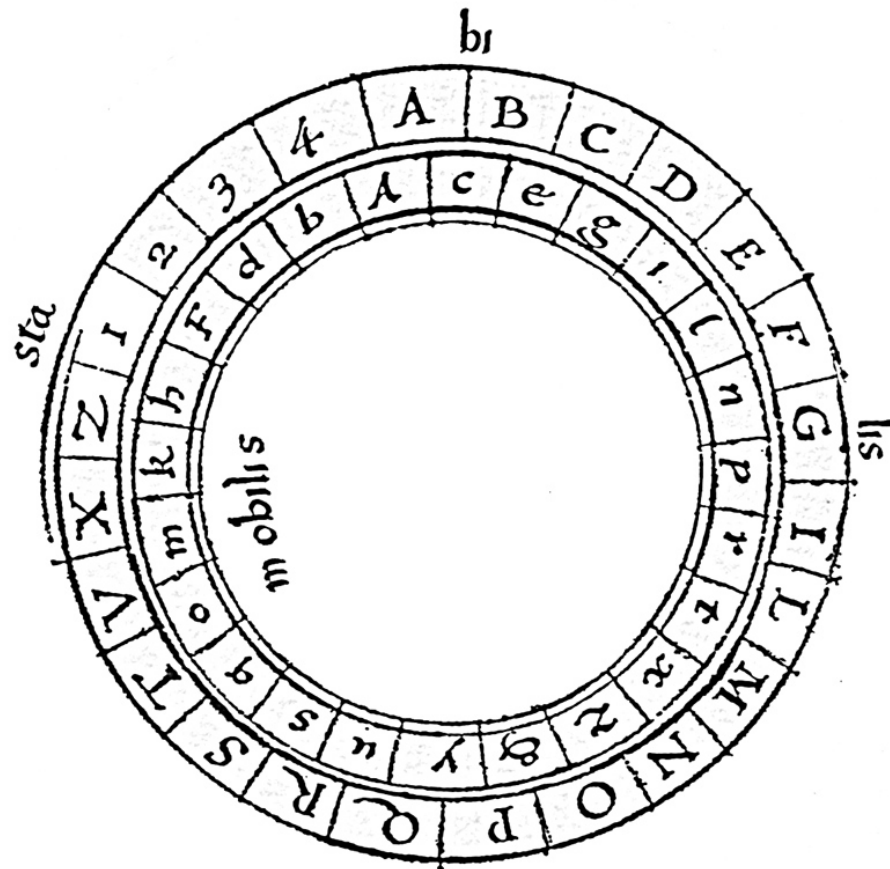


Figure A.3: Alberti's cipher disc.

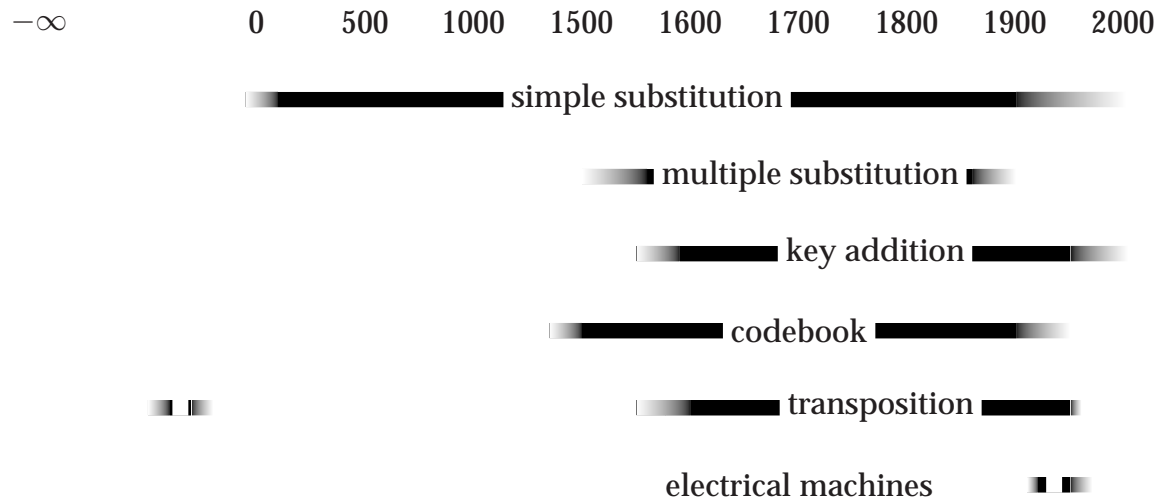


Figure A.4: Timeline of cryptography before computers

In our alphabet this would be: $a \leftrightarrow z$, $b \leftrightarrow y$, $c \leftrightarrow x$, \dots , $m \leftrightarrow n$. The Hebrew version reads:

a	b
th	sh

It is called the athbash system, corresponding to the first two replacements, and an example is babel encrypted as sheshakh. where? (Only the consonants and long vowels are written.)

Our knowledge of Greek cryptography consists of a few isolated incidents, the Polybios square, and the skytale, of Spartan origin. The latter is a transposition cipher with a hardware implementation. Later authors describe it, but it is not clear whether it was really used as claimed; see Section E.1 for details.

The famous historian Polybios (ca. 200–ca. 120 BC) described in his important work *Histories* the conquest of the Mediterranean world by the Romans, covering the period from 220 to 144 BC. King Philip V. of Macedonia (238–179 BC) had defended his territories in the First Macedonian War from 215 to 210, but lost everything except his home state in the Second Macedonian War, 200 to 197. Polybios describes his war preparations against Attalos I. Soter, King of Pergamon (269–197 BC), who had become an ally of the Romans in 211 BC.

They used a signalling system with lighted torches on hilltops. One example is the communication from the top of Mount Tisaion, 644 m high, across the Strait of Trikeri to Demetrios, a distance of about 7 km. On the tortuous mountain roads around the Bay of Pegasis, the land distance is over 160 km.

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Figure A.5: The Polybios Square

Polybios writes that before his invention, only the few terms of a prearranged tiny “codebook” could be transmitted by fire signals. Of his own method, he says that Kleoxenus is the inventor, but that others think that Democrit proposed it; in any case, Polybios perfected it. He uses an alphabet of 25 letters, and writes them in a 5×5 square. With our letters, leaving out j , this would look as in Figure A.5.

The person signalling a message has an arrangement of ten torches hidden behind a screen, five to the left and five to the right. For each letter, he raises as many left torches as are required to indicate the row, and then right torches for the column. Thus to transmit d , in row 1 and column 4, he raises one left torch and then four right torches. Formally, this is a simple substitution with elements from $\{1, 2, 3, 4, 5\}^2$. Both the system and the key are public. Polybios does not mention the possibility of arranging the letters in his square in a different sequence. The security depends on the enemy being unable to observe the light signal - an unexpected similarity to photon-based quantum cryptography.

Albert C. Myer, United States signals officer, adapted Polybios’ system and replaced torches by flags. This was used on both sides in the US Civil War, and the energetic up-and-down waving of flags earned the procedure the name *wigwag system*. Many other variations have been used, for example a prisoners’ system where the torches are replaced by knocks on the jail walls.

The Romans perfected military technology in many respects, but apparently not in the area of cryptography. Caesar invented his famous cipher, consisting of a shift by three positions in the alphabet, and Augustus simplified it to a shift by one only; see Section A.3. This seems to have been used in private correspondence only.

The Arabs mastered already around 800 the major aspects of simple substitutions, including cryptanalysis based on frequency counts, and had a basic knowledge of transpositions; see ??.

No example of secret communication using medieval cryptography has survived. Its purpose was different. Secret writing often occurs in signatures and a scribe’s request to pray for him. It does not make much sense for the

latter, but may be related to an atavistic aversion against naming names. In signatures on legal documents, one may have thought that they add some security. And finally, bashfulness may be responsible for the scribes' use of cryptography in superstitious and pornographic writing.

In the Middle Ages, two systems of simple substitutions for the vowels only were popular: by one to five dots, and by the consonant following the vowel. Here are one plaintext and its two encryptions:

```
medievalcriptohadnokei
medievalcriptohadnokei
mfdjfvblcrjptphbdnpkfj
```

There is no secret key between correspondents involved. Anyone who knows the system can decrypt any message. Figure A.6 shows leaf 126r of the beautifully illustrated *codex aureus* of St. Emmeran, written in 870. It was restored under the direction of abbot Ramwold (975–1001). The names Aripo and Adalpertus of the renovators are given in a cryptogram in the center of the right-hand column and enlarged in Figure A.7:

Figure A.8 shows a unique example of a different type. It comes from a biography of the English missionary Saint Willibald (ca. 700–787), who tried hard—with his brother, Saint Wynnebald (701–761)—and ultimately successfully to proselytize the heathens of Southern Germany. Willibald had spent about a decade of adventure travel in Italy, Asia Minor and the Holy Land. His *Vita* is the first travel book written by an English person. It was penned around 800 by an Anglo-Saxon nun of *Heidenheim*, whose name remained cryptographically hidden for a long time. Namely, after the last words *Amen. Finit* of the biography, the scribe inserted the text in Figure A.8 which reads literally as follows:

```
Sēcdgquār. quīn. npri. sprix quār. ntēr.
cpri. nquār. mtēr. nsecun. hquīn. gsecd
bquinrc. qārr. dinando hsecdc. scrter
bsecd. bprim.
```

The consonants are written in plaintext, and the five vowels are encrypted in order:

a	=	primum	=	first,
e	=	secundum	=	second,
i	=	tertium	=	third,
o	=	quartum	=	fourth,
u	=	quintum	=	fifth.

The ciphertext is abbreviated in a standard medieval fashion, and indicated by a tilde. For example, the first word *Sēcdgquār* means *secundum g quartum*, which decrypts as *ego*. Thus the Latin decryption is



Figure A.6: Leaf 126r of the *Codex Aureus* from the Bayrische Staatsbibliothek, München

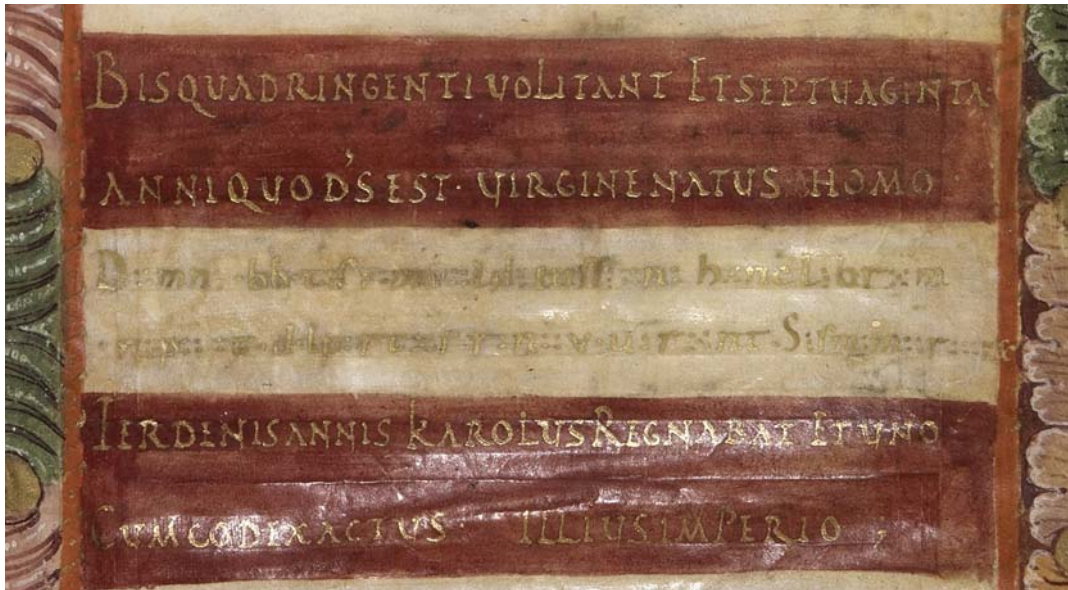


Figure A.7: The cryptogram below the center of the right column in Figure A.6.

D:mn: .bb:ts r:m:wld: .ss:un: h:nc librum .r:p: :t
 .d:lp: r:ts r:n:v:v:rent. S:s m:mr :ir

Decryption: Dom[i]ni abbatis Ramuoldi iussione hunc librum Aripo et Adalper-
 tus renovaverunt. Sis memor eor[um].

At the order of abbot Ramwold, Aripo and Adalpertus repaired this book.
 Remember them.

Sēcd 3 quār. quīn. nprī. sp̄h̄x quār. mēr.
 cpri. n quār. mēr. n secūn. h quīn. 3 secū
 b quīn re. qarr. dimando h secūc. ser tēr.
 b secū. b prīm.

Figure A.8: Hugeburc's encrypted subscription to her *Life of Willibald*.

Ego una Saxonica nomine Hugeburc ordinando hec scribebam

I am a Saxon lady by name of Hugeburc. I arranged and wrote this.

The last sentence presumably means that she did not just copy the text, but restructured the material available to her.

Systematic, professional, and well-documented use of cryptography in Western Europe starts only in the early Renaissance, in Italy. The city states established permanent diplomatic missions in other states. These had to communicate regularly with their governments at home. Travel was insecure, and messengers were often attacked and had their letters (and lives) taken away. To protect the secrets, cipher bureaus were established which produced codebooks for the various embassies. Tranchedini's nomenclator in Section D.1 is a sample output of such a code factory. Frequency cryptanalysis of a simple substitution was well understood, and protective measures such as dummies, several encryptions of a single letter, and long codebooks were commonly used.

The principles developed by these early Italian code builders formed the backbone of professional cryptography until the First World War, almost half a millenium later.

A later Renaissance invention is the encryption by several simple substitutions. This was proposed by the abbot Trithemius., and published as the first printed book on cryptography in 1516; see ???. He included a table which reduced encryption to a table look-up and was later named after de Vigenère, who used it in 1586. Its arithmetic nature—the encryption is the modular sum of plaintext and key—was recognized around 1690 and the system was completely broken by Kasiski in 1863, but continued as the “chiffre indéchiffrable” well into the 20th century. We discuss it at length in Chapters B and C. There is not much evidence of its use under practical conditions; one such application was on the Confederate side in the US Civil War. On the other hand, we typically only learn about cryptography gone wrong and much less about successful uses.

Codebooks—small and large—continued to be the method of choice, but while the Renaissance had freed spirits from dogmatic confines, the flowering imagination of baroque and later mindsets brought about an exuberant multitude of cryptographic proposals, often beautifully illustrated and explained, and in general quite useless. This “salon cryptography” includes the elaborate image in ??, musical ciphers in ??, knots on threads (but much simpler than Inca quipus), trumpets sounding (Notes ??), flower arrangements, or arithmetic puzzles (Buck (1772); see von zur Gathen (2004)). These systems were often esthetically or intellectually pleasing, difficult to execute and easy to break (being simple substitutions), and showed off the imagination of their authors, who rarely failed to assert their absolute security.

The earliest mechanical devices for cryptography are—apart from the skytale—the cipher disks of Alberti and Porta (see Porta disk) and the movable de Vi-

genère substitutions in Collange's 1561 edition of Trithemius.' *Polygraphia*, one of which is shown in ???. Later inventions had wheels that rotated about a common axis; as handy and robust field ciphers they were in military use until the Second World War. when?

Porta disk image

In the early 1920s, the time was ripe for electromechanical devices, and four people independently invented rotor-based machines. The most famous of these became the *Enigma*, to which Chapter G is devoted.

Also in the 1920s, Vernam proposed his *one-time pad*. Here the message is represented as a string of bits, each either 0 or 1, a random bit string of equal length is generated, and the two are added, bit by bit. This provides perfect security; see Section 2.1. Alas, it is not easy to generate and distribute the required huge keys, but the system was employed extensively by Soviet and East Bloc secret services during the Cold War. Variants of it were put to practical use, where the key is not really random but pseudorandom; see ??? on pseudorandom generation. Actually, Vernam's invention was of this type, and there were later electromagnetical implementations such as the German Siemens Geheimschreiber ??? in World War II. The hope presumably was that the minor change from random to pseudorandom would leave the security intact—but the British cryptanalysts broke the system, incidentally building the first computer, called *Colossus*, for this purpose; see Section G.2*.

From the 1950s on, computers took over much of the cryptographic work. Shannon had developed a theory and identified confusion and diffusion as fundamental goals. The Data Encryption Standard (DES), established in 1977, is a typical product of that era: a fairly complicated set of bit operations performed in 16 rounds on the 64 bits of a message, and which can be run by standard digital computer hardware at great speed.

In 1976, a 12-page paper by Diffie and ? brought about a revolution in cryptography. They proposed to consider systems where one part of the key is kept secret and another part is made public. This sounds rather strange, but it soon sparked the interest of a large community. Much of the present text is about various aspects of this new *public-key cryptography*. On the technical side, it solved the problem of key distribution. More importantly, the new methods used a wide variety of tools from computer science and mathematics, in particular from computational complexity and from number theory. The latter's influence is pervasive throughout this book, from RSA and discrete logarithms to elliptic curves. Typical questions in complexity theory are: What does it mean for a problem to be hard to solve? Can we prove problems to be hard? The ultimate answer to the last question is still lacking, but the methodologies developed are essential for the modern theory of cryptography; we can look at pseudorandom generation, formal notions of security, and zero knowledge protocols as examples (Chapters ???, ???, ???).

The word *cryptography* comes from the Greek $\kappa\rho\upsilon\pi\tau\acute{o}\sigma$ (kryptos) meaning *hidden* or *secret*, and $\gamma\rho\alpha\varphi\epsilon\iota\nu$ (graphein) *to write*. The $\kappa\rho\upsilon\pi\tau\epsilon\acute{\iota}\alpha$ (krypteia) was a Secret Service in Sparta. *Cryptanalysis* is the art of breaking cryptosystems, a subdiscipline of cryptography.

In the traditional terminology of historical cryptography, a simple substitution is called an *alphabet*. Unfortunately, this clashes with the use of *alphabet* as the finite set of letters (or symbols) in which everything is written; this is its standard meaning in computer science, mathematics and natural language. Thus we cannot use the traditional term or its derivatives, but have arrived at the following dictionary:

simple substitution = alphabet or monoalphabetic substitution,
relational substitution = monoalphabetic substitution with homophones,
multiple substitution = polyalphabetic substitution.

A.3. Simple substitutions

In its simplest form, a *simple substitution* cipher is a permutation $\text{enc}: \mathbb{A} \longrightarrow \mathbb{A}$ of an alphabet \mathbb{A} , that is, to each letter $x \in \mathbb{A}$ is associated a unique encrypting letter $\text{enc}(x) \in \mathbb{A}$, and different letters have different encryptions. Gaius Iulius **Caesar** (100–44 BC) used such a cryptosystem, where $\text{enc}_{\text{Caesar}}$ just moves each letter three positions ahead. Thus $\text{enc}_{\text{Caesar}}(\text{caesar}) = \text{fdhvd u}$ in our 26-letter alphabet. The letters at the end of the alphabet wrap around, so that $\text{enc}_{\text{Caesar}}(\text{wxyz}) = \text{zabc}$.

In this and the following examples, the alphabet table Table A.1 on page 21 may be helpful.

If instead of letters we take the corresponding numbers, as in Table A.1, then $\text{enc}_{\text{Caesar}}(x) = x + 3$, and decryption is just as easy: $\text{dec}_{\text{Caesar}}(y) = y - 3$. In both operations, wrap-around applies. We can replace the shift 3 by any number k , and consider $\text{enc}_k(x) = x + k$, with decryption $\text{dec}_k(y) = y - k$, applying wrap-around. These 26 ciphers are called the *Caesar ciphers*.

The historian Gaius Suetonius Tranquillus (c. 70–c. 140) writes about Caesar's cryptography: *Extant & ad Ciceronem, item ad familiares domesticis de rebus: in quibus si qua occultiùs perferenda erāt, per notas scripsit, id est, sic structo litterarum ordine, vt nullum verbum effici posset: quæ si quis inuestigare & persequi vellet, quartam elementorum litteram, id est, d pro a, & perinde reliquas commutet.*² Tranquillus also relates how Caesar's successor Augustus (63 BC–14 AD) used an even simpler version: shift by one, and no wrap around:

²There exist also [letters of Caesar] to Cicero, and to his family about domestic matters, in which he wrote in cipher if something was to be hidden. That is, in an arrangement of letters where no word was recognizable even to someone who wants to find out and read it. Namely, he turned a letter into the fourth element [following it], that is, *a* into *d*, and the others in the same way.

*quotiens autem per notas scribit, B pro A, C pro B ac deinceps eadem ratione sequentis litteras ponit; pro X autem duplex A.*³

As an example, Caesar would send the plaintext $x = \text{gallia omnia divisa est}$ as $\text{enc}_{\text{Caesar}}(x) = \text{jdooldrqpqlldglylvdhvw}$, and Augustus as $\text{enc}_{\text{Aug}}(x) = \text{hbmmjbpnojb ejwjt bftu}$. For simplicity, we are using the 26-letter alphabet (which the Romans did not), and arrive at the encryption as follows:

plaintext	g	a	l	l	i	a	o	m	n	i	a	d	i	v	i	s	a	e	s	t
numerical	6	0	11	11	8	0	14	12	13	8	0	3	8	21	8	18	0	4	18	19
Caesar num.	9	3	14	14	11	3	17	15	16	11	3	6	11	24	11	21	3	7	21	22
ciphertext	j	d	o	o	l	d	r	p	q	l	d	g	l	y	l	v	d	h	v	w
Augustus num.	7	1	12	12	9	1	15	13	14	9	1	4	9	22	9	19	1	5	19	20
ciphertext	h	b	m	m	j	b	p	n	o	j	b	e	j	w	j	t	b	f	t	u

In his collection *Noctes Atticae*, written in the second century AD, Aulus Gellius has preserved excerpts from Greek and Roman writings several of which are known to us only through this work. He mentions that *Libri sunt epistolarum C. Cæsaris ad C. Oppium, & Baltum Cornelium, qui res eius absentis curabant. In his epistolis quibusdam in locis inveniuntur literæ singulariæ, sine coagmentis syllabarum, quas tu putes positas inconditè. Nam uerba ex his literis confici nulla possunt. Erat autẽ conuenium inter eos clandestinum, de commutando situ litterarum, ut inscriptio quidem alia aliæ locũ & nomen teneret: sed in legẽdo locus cuiq, suus & potestas restitueretur. Id est, hãc latentẽ & occultã significationem litterarum.*⁴

The meaning is not quite clear, but it may well be that Caesar also used either a codebook (“strange letters”) or a transposition cipher. Roman cryptography seems to have been more imaginative than what we learn from Tranquillus.

There are only 26 “Caesar ciphers” as above (in our alphabet), but if we consider arbitrary permutations on 26 letters, then there are $26! \approx 4.03 \cdot 10^{26}$ such permutations enc. If a cryptographer chooses enc at random among those $26!$ possibilities, and a cryptanalyst wants to decrypt a message, it seems that he has to try out all of them—a hopeless task, at least by hand. Even if it were feasible on a computer, one would still have to choose one of the $26!$ outputs, most of which are nonsense, of course. In the unlikely event that there are two or more that make sense, you would not even know which one is right. A precise analysis of this problem is in Section A.5. bale=able

While the cryptanalyst has to find out the permutation, the legitimate users only have to agree on it, and then remember it. One of the most popular ways

³Often he writes in cipher and puts B for A, C for B, and the following letters in the same way; for X, he writes a double A. [X is the last letter of the Latin alphabet.]

⁴There are also collections of letters from Gaius Caesar to Gaius Oppius and Baltus Cornelius, who took care of his affairs in his absence. In these letters you find in some places strange letters, not connected into syllables, which you would think were placed at random. For no words can be formed from these letters. They also had arranged a secret key among them of changing the position of letters. Then although in the writing one letter has the position and meaning of another one, by reading it in its proper position, the real meaning is restored. That is, the hidden and secret meaning of the letters.

of facilitating this was invented by an Italian family of cryptographers, the Argentis. Giovanni Batista Argenti was cipher secretary to the popes Sixtus V and Gregorius XIV, at the end of the 16th century. His two nephews Matteo and Marcello Batista succeeded him in this post. After being sacked in 1605, Matteo Argenti wrote his famous *manuale argenti*.

The Argentis proposed the following way of memorizing a substitution $\text{enc}: \mathbb{A} \rightarrow \mathbb{A}$, where \mathbb{A} is an alphabet. You choose a key word K , map its letters in sequence to the first letters of \mathbb{A} (removing duplicates in K), and then the rest of the alphabet in sequence. With the English alphabet for \mathbb{A} and $K = \text{giovanni}$, this gives the following permutation:

$$(A.4) \quad \begin{array}{cccccccccccccccccccccccc} \text{g} & \text{i} & \text{o} & \text{v} & \text{n} & \text{a} & \text{b} & \text{c} & \text{d} & \text{e} & \text{f} & \text{h} & \text{j} & \text{k} & \text{l} & \text{m} & \text{p} & \text{q} & \text{r} & \text{s} & \text{t} & \text{u} & \text{w} & \text{x} & \text{y} & \text{z} \\ \text{a} & \text{b} & \text{c} & \text{d} & \text{e} & \text{f} & \text{g} & \text{h} & \text{i} & \text{j} & \text{k} & \text{l} & \text{m} & \text{n} & \text{o} & \text{p} & \text{q} & \text{r} & \text{s} & \text{t} & \text{u} & \text{v} & \text{w} & \text{x} & \text{y} & \text{z} \end{array}$$

and $\text{enc}_K(\text{batista}) = \text{geubtue}$. As is visible in the example, most keywords provide only little change in the latter part of the alphabet.

Throughout the historical chapters, we distinguish typographically between the cleartext, key, and ciphertext.

A.4. Frequency analysis

Any simple substitution is easy prey to a **frequency analysis**, if only the message is long enough.

This cryptanalysis requires as its main tools frequency tables for individual letters, but also for bigrams (pairs of letters), trigrams (triples), and short words. Table A.2 gives eight lists of letter frequencies in percent, four for English in the first columns, and one each for German (D), French (F), Spanish (S), and Italian (I).

The first English column “HP” is from Joanne Rowling’s (1998) *Harry Potter and the Philosopher’s Stone*, the second from Chapter 5 of this book, the third from Meyer & Matyas (1982), and the fourth from Gaines (1956). The last row is 100 times the sum of the squares of the frequencies; thus e contributes $100 \cdot 0.1191^2 \approx 1.42$ to the first entry 6.36. More details are in the Notes. When we refer in the following to the English frequency of this table, this will always be the *Harry Potter* column—cryptanalysis has its own magic.

We can observe material differences between the various tables for English, notably k varying from 0.42% to 1.2%. The message of the four English columns is that there is some consistency across various types of texts, but certainly not after the decimal point. We can sort the letters into seven categories, according to a rough approximation of their frequencies:

%	12	9	8	6	4	2	0
	e	t	ao	nirsh	dl	bcfgkmpuwy	jvxxz

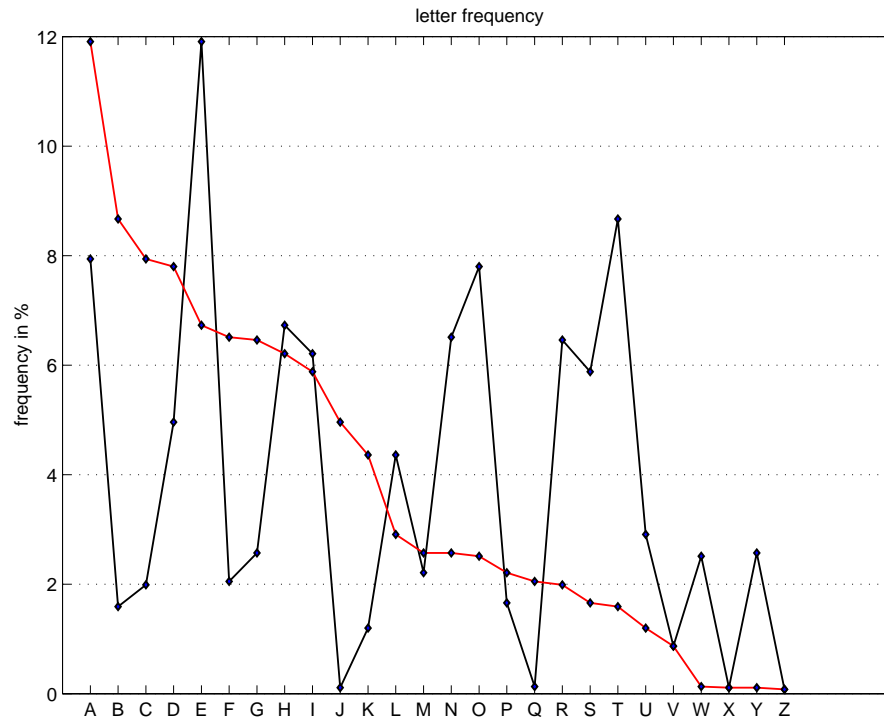


Figure A.9: English frequencies (Harry Potter), ordered by alphabet (black) and by frequency (red).

letter	HP	Ch. 5	MM	G	D	F	S	I
a	7.94	7.13	8.04	7.81	5.26	7.75	12.25	10.71
b	1.59	1.70	1.54	1.28	1.85	0.99	1.48	0.74
c	1.99	3.72	3.06	2.93	3.62	2.67	3.63	5.14
d	4.96	3.29	3.99	4.11	5.05	3.35	5.33	3.73
e	11.91	11.75	12.51	13.05	17.41	16.61	14.01	12.04
f	2.05	2.20	2.30	2.88	1.50	1.08	0.46	1.29
g	2.57	2.83	1.96	1.39	2.94	1.29	1.05	1.82
h	6.73	4.55	5.49	5.85	5.90	0.93	1.22	1.81
i	6.21	8.16	7.26	6.77	8.85	7.33	5.50	10.26
j	0.11	0.29	0.16	0.23	0.15	0.71	0.64	
k	1.20	0.59	0.67	0.42	1.13			0.01
l	4.36	3.99	4.14	3.60	3.75	4.90	5.45	5.78
m	2.21	2.87	2.53	2.62	3.19	3.28	2.73	2.98
n	6.51	6.53	7.09	7.28	10.71	7.61	6.63	6.60
o	7.80	7.58	7.60	8.21	1.93	6.92	9.93	9.55
p	1.66	3.09	2.00	2.15	0.37	2.53	2.17	2.79
q	0.13	0.47	0.11	0.14	0.02	1.47	1.99	0.82
r	6.46	5.82	6.12	6.64	6.65	6.57	6.17	6.44
s	5.88	6.00	6.54	6.46	6.14	7.56	7.68	5.61
t	8.67	8.87	9.25	9.02	5.79	6.54	3.77	5.74
u	2.91	2.64	2.71	2.77	3.86	6.62	4.86	3.60
v	0.87	0.93	0.99	1.00	0.76	2.22	1.09	2.01
w	2.51	1.90	1.92	1.49	2.01			0.02
x	0.11	1.08	0.19	0.30	0.01	0.37	0.02	0.04
y	2.57	1.75	1.73	1.51	0.01	0.22	1.53	0.02
z	0.08	0.26	0.09	0.09	1.15	0.48	0.40	0.45
$\sum f_i^2$	6.36	6.15	6.58	6.74	7.77	7.55	7.51	7.22

Table A.2: Four frequency tables for English, and one each for German, French, Spanish, and Italian, all in percent.

Thus *etaonirsh* is a useful mnemonic for English frequencies if you ever have to break a simple substitution.

If we want to analyse some encrypted message that we suspect to be in a classical system, we set up the frequency table of the ciphertext, preferably in the frequency ordered way of the red graph in Figure A.9. If it matches roughly the English table, then this is a strong indication that we deal indeed with a simple substitution and that the plaintext could be in English. The context will usually tell us the language, or leave a choice between two or three. Then we assume the language that matches best. If no language matches at all, as in

the “flat” distribution of Figure C.1 below, then we conclude that this is not a simple substitution.

Then we substitute matching entries in the two frequency tables, starting with the ones that occur most often. Of course, we cannot expect the two tables to match exactly. For example, in Figure A.9, the rates for n, i, r, s , and h (near the 6% line) are so close to each other that we can, at best, expect them to match as a group. Thus one makes conjectures about individual letters. Some sections of the ciphertext will then have a substantial portion of cleartext guesses, and one tries to find actual words that fit. The search for individual words, such as one-letter words like *a* or *I* (if the word divisions are visible), or frequent words like *the*, helps along. The whole is a process of trial and error. Some experts have observed that as important as the technical tools are a certain degree of ingenuity and perseverance—virtues that are generally useful in life.

The great American poet Edgar Allan Poe (1809–1849) became interested in cryptography in late 1839, and had a forum as the editor of the weekly *Graham’s Magazine*, where readers would send him ciphertexts and he would publish his solutions. The only systems he solved were simple substitutions. He soon achieved a reputation as a master cryptographer, but modern-day experts judge differently; see below.

Rather than quibble about his boastful self-aggrandization as master cryptographer, we follow the master story-teller in the frequency analysis in his story *The Gold-Bug*, written in 1843. It deals with the hunt for the treasure of the pirate Captain Kidd, hidden on Sullivan’s Island, near Charleston SC. The hero, William Legrand, has discovered a parchment with hidden characters on it. This is an example of superencipherment: the secret message was first encrypted (by a simple substitution, as it turns out), and this then superenciphered by steganographic use of sympathetic ink (see ??). The superencipherment was stripped by accident: on a cold autumn evening, the narrator warmed himself by the fire-place, holding the parchment close to it and thus revealing the secret writing. The ciphertext is as follows:

```
53†††305))6*;4826)4†.)4†);806*;48†8¶60))
85;]8*:†*8†83(88)5*†;46(;88*96*?;8)*†;(485);
5*†2*:†;(4956*2(5*—4)8¶8*;4069285);)6†8)
4††;1(†9;48081;8:8†1;48†85;4)485†528806*81(
†9;48;(88;4(†?34;48)4†;161;:188;†?;
```

Legrand shows off: *the solution is by no means so difficult as you might be led to imagine from the first hasty inspection of the characters. These characters, as any one might readily guess, form a cipher—that is to say, they convey a meaning; but then, from what is known of Kidd, I could not suppose him*



"This is a strange scarabeus, I must confess"

Figure A.10: The narrator (seated), Legrand, and Jupiter examine the parchment with the Gold-Bug cryptogram.

capable of constructing any of the more abstruse cryptographs. [...] Circumstances, and a certain bias of mind, have led me to take interest in such riddles, and it may well be doubted whether human ingenuity can construct an enigma of the kind which human ingenuity may not, by proper application, resolve.

Circumstantial evidence points to English as the language. He sets up the ciphertext's frequency table:

Of the character 8	there are	33.
;	“	26.
4	“	19.
†)	“	16.
*	“	13.
5	“	12.
6	“	11.
†1	“	8.
0	“	6.
9 2	“	5.
: 3	“	4.
?	“	3.
¶	“	2.
] —	“	1.

In Figure A.11, we have overlain the graphs of this and the English frequency tables; the match is quite reasonable. Legrand goes on: “Now, in English, the letter which most frequently occurs is e. Afterwards, the succession runs thus: a o i d h n r s t u y c f g l m w b k p q x z. E however predominates so remarkably that an individual sentence of any length is rarely seen, in which it is not the prevailing character.” His positions of t and n are somewhat different from Table A.2. “Let us assume 8, then, as e. Now, of all words in the language, ‘the’ is most usual; let us see, therefore, whether there are not repetitions of any three characters, in the same order of collocation, the last of them being 8. If we discover repetitions of such letters, so arranged, they will most probably represent the word ‘the.’ On inspection, we find no less than seven such arrangements, the characters being ;48. We may, therefore, assume that the semicolon represents t, that 4 represents h, and that 8 represents e—the last being now well confirmed. Thus a great step has been taken.

“But, having established a single word, we are enabled to establish a vastly important point; that is to say, several commencements and terminations of other words. Let us refer, for example, to the last instance but one, in which the combination ;48 occurs—not far from the end of the cipher. We know that the semicolon immediately ensuing is the commencement of a word, and, of the six characters succeeding this ‘the,’ we are cognizant of no less than five. Let us set these characters down, thus, by the letters we know them to represent, leaving a space for the unknown—

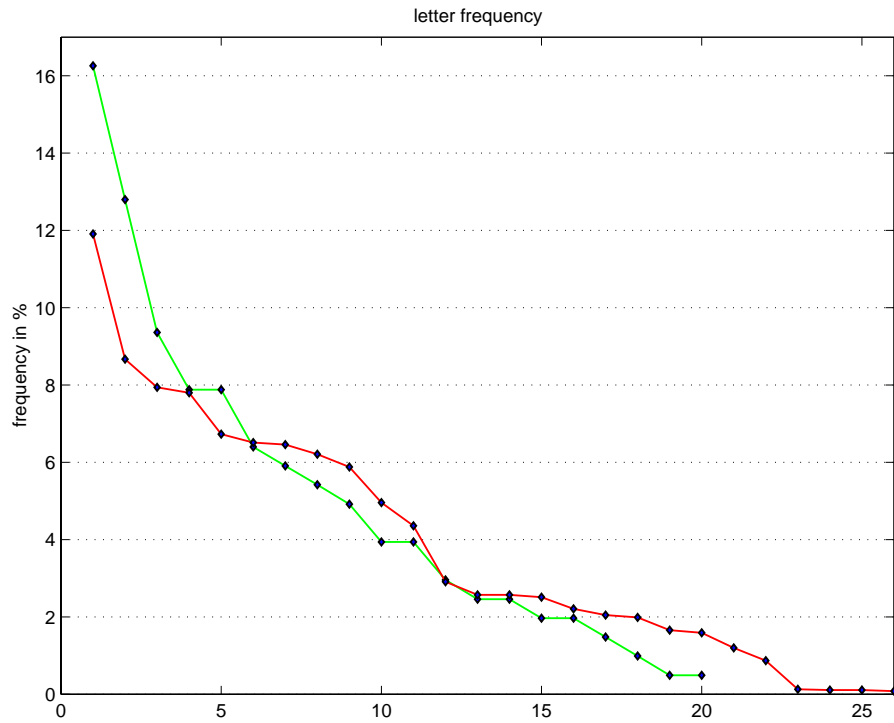


Figure A.11: English frequencies (red) and Gold Bug (green).

t eeth.

“Here we are enabled, at once, to discard the ‘th,’ as forming no portion of the word commencing with the first t; since, by experiment of the entire alphabet for a letter adapted to the vacancy we perceive that no word can be formed of which this th can be a part. We are thus narrowed into

t ee,

and, going through the alphabet, if necessary, as before, we arrive at the word ‘tree’, as the sole possible reading.” Then he notes the arrangement

the tree thr†?3h the.

and “the word ‘through’ makes itself evident at once.” He then finds †83(88 or †egree, which gives † = *d*, and ;46(;88* or th6rtee*, “an arrangement immediately suggestive of the word ‘thirteen’, and again furnishing us with two new characters, *i* and *n*, represented by 6 and *. The first characters 5good yield 5 = *a*, and to avoid confusion, it is now time that we arrange our key, as far as discovered, in a tabular form. It will stand thus:

5	represents	<i>a</i>
†	“	<i>d</i>
8	“	<i>e</i>
3	“	<i>g</i>
4	“	<i>h</i>
6	“	<i>i</i>
*	“	<i>n</i>
†	“	<i>o</i>
(“	<i>r</i>
;	“	<i>t</i>

“We have, therefore, no less than ten of the most important letters represented, and it will be unnecessary to proceed with the details of the solution. I have said enough to convince you that ciphers of this nature are readily soluble, and to give you some insight into the rationale of their development. But be assured that the specimen before us appertains to the very simplest species of cryptograph. It now only remains to give you the full translation of the characters upon the parchment, as unriddled. Here it is: ‘A good glass in the Bishop’s hostel in the Devil’s seat—twenty-one degrees and thirteen minutes—northeast and by north—main branch seventh limb east side—shoot from the left eye of the death’s-head—a bee-line from the tree through the shot fifty feet out.’”

The secret message is deciphered, but Legrand still has a lot of figuring to do. Will he find Captain Kidd’s treasure?

William F. Friedman, the leading US cryptographer of his days, says about Poe: *The serious student of cryptography can, if he takes the trouble, see in*

Poe's essay and in his other writing on this subject many things which are not apparent to the layman. Against his will he is driven to the conclusion that Poe was only a dabbler in cryptography. At the same time it is only fair to say that as compared with the vast majority of other persons of his time in this or in foreign countries, his knowledge of the subject, as an amateur, was sufficient to warrant notice. Had he had opportunity to make cryptography a vocation, there is no doubt that he would have gone far in the profession.

Wimsatt (1943) writes: *Legrand's explanation of how he solved the cipher is a fine feat of exposition—as anybody will realize who undertakes to write a few paragraphs about ciphers. As we follow the steps of the argument, we have the impression of intricacy and precision, of Legrand's shrewdness and patience—each detail receives attention—and yet we are never lost, the main outlines remain clear, the reasoning turns where it should, the momentum, or rhythm, of the whole is sustained. The writing of this kind of prose was, as I see it, one of Poe's most impressive gifts.*

Many writers have commented on the intellectual capabilities that are useful for cryptanalysis. quotes van s'Gravesande (1748) goes one step further: he considers cryptanalysis (of a simple substitution) as part of logic, which in turn is a branch of philosophy. Indeed, he develops on twelve pages the decipherment of a 109-letter text, first using letter frequencies and repetitions, then the word structure of Latin. Particularly instructive are his wrong turns and explanations on how to backtrack from them.

Professionals (then) and amateurs (still today) have burnt a lot of midnight oil figuring out messages encrypted in this kind of system, which must be considered perfectly insecure.

A.5. Information theory

Claude Elwood Shannon worked at the Bell Laboratories and published in 1948 and 1949 two treatises on a *mathematical theory of communication* and on a *communication theory of secrecy systems*. The first one became the foundation for the theory of error-correcting codes. The second one “transformed cryptography from an art to a science”. He identified the two principal actions that provide security: *confusion* and *diffusion*. The first action is to scramble the alphabet thoroughly, as in Rijndael's SubByte operation, and the second one is to diffuse information throughout the message, as Rijndael's Mix Column and ShiftRow do. Furthermore, Shannon quantified the notion of “information content” and derived a result saying that an encrypted message has to have at least a certain length for a cryptanalytic attack to be successful. An example is the one-time pad of Section 2.1, which is proven to be absolutely secure.

We now explain some of Shannon's theory. It only gives a lower bound

on the required length of ciphertext, but no method for actually decrypting. However, for the simplest systems, like simple substitutions or de Vigenère ciphers, the cryptanalytic methods described in Sections C.1 through ?? almost attain that bound in practice.

We have an alphabet \mathbb{A} of s letters. The letter $x \in \mathbb{A}$ occurs with probability p_x , so that $p_x \geq 0$ and $\sum_{x \in \mathbb{A}} p_x = 1$. This can be abbreviated by the probability distribution $p = (p_x)_{x \in \mathbb{A}}$. In the Harry Potter example of Table A.2, we have $s = 26$, $\mathbb{A} = \{a, b, c, \dots, z\}$, and $p = (7.94, 1.59, \dots, 2.57, 0.08)$.

How much “information” do we provide by writing down one letter, or a long message? One of Shannon’s contributions is to make this notion precise, in a useful way. Intuitively, his idea is to insist on writing everything in binary—using only 0 and 1—and to say that the shortest general way of specifying a message in binary is the information provided by the message. That is, we count the number of “bits”—a word coined by Shannon.

But to have a meaningful notion, we cannot allow any old way of presenting letters in binary, but must look at the cleverest one.

EXAMPLE A.5. (i) In Extended ASCII code, each letter is coded by 8 bits, and an n -letter message requires $8n$ bits.

(ii) The following is the International Morse code:

letter	a	b	c	d	e	f	g	h	i	j	k	l	m
Morse code	.--.	...--	------	..-	--
length	2	4	4	3	1	4	3	4	2	4	3	4	2
letter	n	o	p	q	r	s	t	u	v	w	x	y	z
Morse code	-. -	---	..-.	---.	..-	...	-	..-	...-	.-.	...--
length	2	3	4	4	3	3	1	3	4	3	4	4	4

Besides $-$ and $.$, there is actually a third invisible symbol present: the space between adjacent letters. Without it, one could not distinguish between the encodings of ee and i . Thus Morse coding is not a binary encoding. The property violated is called “prefix-freeness”, meaning that no letter code may be a prefix (an initial segment) of another code. But for the sake of illustration, suppose that we had a binary prefix-free encoding with the same lengths as above. Then the expected length of the code for a message of n letters would be

$$2np_a + 4np_b + 4np_c + \dots = n \cdot \sum_{x \in \mathbb{A}} \text{length}(x)p_x,$$

where \mathbb{A} is the English alphabet, and p_x the frequency of some letter x . Thus we expect $np_a \approx 0.0794n$ many a ’s in the message, which take $2 \cdot np_a$ bits, the first term in the sum.

Thus the expected length is a constant times n , with the constant depending on the alphabet and its letter frequencies.

- (iii) Suppose that we have a 3-letter alphabet $\mathbb{A} = \{a, b, c\}$ with frequency distribution $p = (5/12, 1/3, 1/4)$. If we use a two-bit code like $(00, 01, 10)$, then this is prefix-free, and the expected length of an n -letter encoding is

$$n \cdot \left(2 \cdot \frac{5}{12} + 2 \cdot \frac{1}{3} + 2 \cdot \frac{1}{4} \right) = 2n.$$

In the prefix-free code $(1, 01, 00)$, the expected length is

$$n \cdot \left(1 \cdot \frac{5}{12} + 2 \cdot \frac{1}{3} + 2 \cdot \frac{1}{4} \right) = \frac{19}{12}n \approx 1.583n < 2n.$$

This is quite a bit better. To go even further, one of Shannon's ideas is that we might also encode bigrams, that is $\mathbb{A}^2 = \{aa, ab, ac, ba, bb, bc, ca, cb, cc\}$, which occur with probabilities

$$p = \left(\frac{25}{144}, \frac{20}{144}, \frac{15}{144}, \frac{20}{144}, \frac{16}{144}, \frac{12}{144}, \frac{15}{144}, \frac{12}{144}, \frac{9}{144} \right),$$

where we have not simplified the fractions. When we use the prefix-free code

$$(000, 001, 010, 011, 100, 101, 110, 1110, 1111),$$

then a message of n letters will consist of $n/2$ codewords (for even n) and have expected length

$$\begin{aligned} \frac{n}{2} \cdot \left(\frac{3}{144} \cdot (25 + 20 + 15 + 20 + 16 + 12 + 15) + \frac{4}{144} \cdot (12 + 9) \right) \\ = \frac{151}{96}n \approx 1.573n < \frac{19}{12}n. \end{aligned}$$

When we code trigrams and longer polygrams, it turns out we can get smaller and smaller constant factors of n , but there is a limit, 1.555 in this case. \diamond

We now define the limit alluded to at the end of the example.

DEFINITION A.6. Let $p = (p_1, p_2, \dots, p_s)$ be a probability distribution. Then its **entropy** $H(p)$ is

$$H(p) = \sum_{1 \leq i \leq s} p_i \log_2(p_i^{-1}).$$

(We write p_i^{-1} to make the logarithm nonnegative, and interpret the summand as 0 when $p_i = 0$.) The entropy has the following property:

$$(A.7) \quad 0 \leq H(p) \leq H\left(\frac{1}{s}, \frac{1}{s}, \dots, \frac{1}{s}\right) = \log_2 s.$$

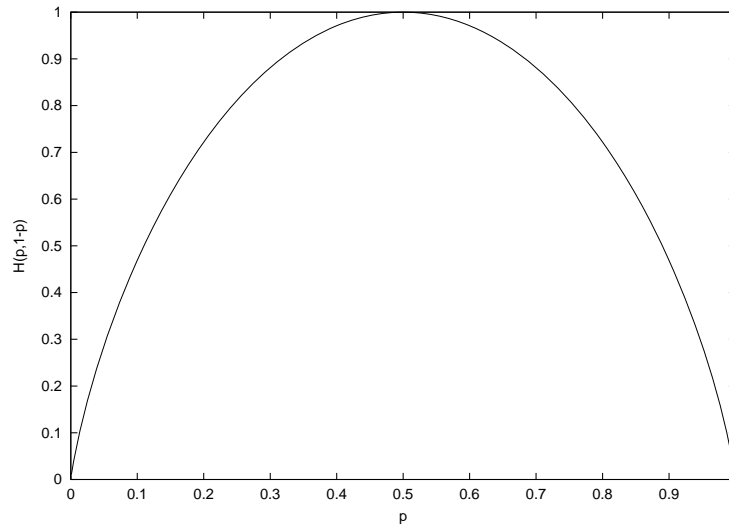


Figure A.12: The entropy $H(p, 1 - p)$ for $0 \leq p \leq 1$.

For $s = 2$, we have $p_2 = 1 - p_1$; $H(p_1, 1 - p_1)$ is shown in Figure A.12.

A prefix-free code $c: \mathbb{A} \longrightarrow \{0, 1\}^*$, or $c: \mathbb{A}^2 \longrightarrow \{0, 1\}^*$, or $c: \mathbb{A}^k \longrightarrow \{0, 1\}^*$ for some $k \geq 1$, gives an encoding $c: \mathbb{A}^* \longrightarrow \{0, 1\}^*$ of messages over \mathbb{A} of arbitrary length (padding the messages if necessary). Here,

$$\mathbb{A}^* = \{x_1 \cdots x_n : n \geq 0, x_1, \dots, x_n \in \mathbb{A}\}$$

consists of the finite strings over \mathbb{A} , and similarly for $\{0, 1\}^*$. We denote by $\lambda_c(x)$ the length of $c(x) \in \{0, 1\}^*$ for any message $x \in \mathbb{A}^*$. The expected length $\lambda_c(n)$ for n -letter messages is

$$\lambda_c(n) = \sum_{x \in \mathbb{A}^n} \lambda_c(x) \text{prob}(x),$$

where $\text{prob}(x) = p_{x_1} \cdot p_{x_2} \cdots p_{x_n}$ is the probability of $x = x_1 x_2 \cdots x_n$. Shannon proved the following fundamental theorem.

THEOREM A.8. *Let \mathbb{A} be an alphabet with probability distribution p .*

- (i) *For any $\epsilon > 0$ there exists a code c so that $\lambda_c(n) \leq n \cdot (H(p) + \epsilon)$ for all sufficiently large n .*
- (ii) *For any code c , we have $\lambda_c(n) \geq n \cdot H(p)$.*

We interpret Shannon's Theorem as saying that an n -letter message contains $nH(p)$ bits of information, and thus one letter conveys $H(p)$ bits on average. Huffman I, MV, have added the name-key pair for David A. Huffman in names.bib,

but I ain't sure whether I should replace it here or not. If not required the name-key pair can be deleted from names.bib. trees provide a reasonable approximation to the upper bound in (i), namely with $\epsilon = 1$. The more general question is data compression, where one tries to get close to Shannon's bound under practical constraints; in the form of JPEG, MPEG or MP3 coded files this theory is now part of daily life.

EXAMPLE A.5 CONTINUED. (ii) The entropy of English is, according to Table A.2,

$$H(p_{\text{Eng}}) = 4.198.$$

Thus one letter of an English text contains 4.198 bits of information. However, this figure is based only on single-letter frequencies and rather misleading. The bigrams *th* and *ht* are assumed to be equally likely, and *qqqq* occurs with positive probability. Taking better account of the properties of the language, Shannon arrives at an estimate of

$$(A.9) \quad H_{\text{Eng}} \approx ?$$

for the entropy of English. value, source

Note that we ignore spaces, punctuation, foreign words with funny letters, numerals, etc. The maximal entropy of any distribution on 26 letters is $\log_2 26 \approx 4.7$, according to (A.7). The **redundancy** of English is the difference $\log_2 26 - 4.198 \approx 0.5$. This can be interpreted as saying that we “lose” half a bit of information per letter when we write English rather than some artificial 26-letter language with the uniform distribution of its letters.

(iii) The entropy of this 3-letter alphabet is

$$H(p) = \frac{5}{12} \log \frac{12}{5} + \frac{1}{3} \log 3 + \frac{1}{4} \log 4 \approx 1.555 < 1.585 \approx \log 3 = H\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right).$$

One letter of this alphabet contains about 1.555 bits of information, and the redundancy is about 0.03 bits per letter. \diamond

Now Shannon applied his theory also to cryptanalysis. We have, as usual, an alphabet \mathbb{A} of size s and with probability distribution $p = (p_x)_{x \in \mathbb{A}}$, and a cryptosystem (enc, dec) with keys K in the total key space \mathbb{K} . We assume that $\text{enc}_K: \mathbb{A}^n \rightarrow \mathbb{A}^n$ maps n -letter cleartexts to n -letter ciphertexts, for any $K \in \mathbb{K}$. The ciphertext is supposed to look random and to have

$$H\left(\frac{1}{s}, \dots, \frac{1}{s}\right) = \log_2 s$$

bits of information per letter. An n -letter message contains $nH(p)$ bits of information. We denote by $I(\mathbb{K})$ the average information in one random key. If

keys are k -bit strings chosen at random (as they should be), then $\mathbb{K} = \{0, 1\}^k$ and $I(\mathbb{K}) = k$. If \mathbb{K} consists of k -letter English words, then $I(\mathbb{K}) = k \cdot H(p_{\text{Eng}}) \approx 4.198k$.

DEFINITION A.10. *The **unicity distance** of the above cryptosystem is*

$$d = \left\lceil \frac{I(\mathbb{K})}{\log_2 s - H(p)} \right\rceil.$$

THEOREM A.11. *Consider a ciphertext of length n .*

- (i) *If $n \geq d$, then an exhaustive key search is likely to reveal the plaintext.*
- (ii) *If $n < d$, then the plaintext cannot be derived.*

The idea of the proof is simple. The ciphertext contains $n \log_2 s$ bits of information, the plaintext $nH(p)$, and the key $I(\mathbb{K})$. In order to derive the plaintext and key from the ciphertext, we need

$$n \log_2 s \geq nH(p) + I(\mathbb{K}),$$

which is the claim.

Exhaustive key search is usually not feasible, but we happily ignore this fact.

EXAMPLE A.12. (i) We consider arbitrary simple substitutions $\pi: \mathbb{A} \rightarrow \mathbb{A}$, where \mathbb{A} is the English alphabet with probability distribution p_{Eng} . The key space $\mathbb{K} = S_{26}$ is the set of all $26! \approx 2^{88.382}$ permutations. Thus $I(\mathbb{K}) \approx 88.382$. The unicity distance is

$$d = \left\lceil \frac{88.382}{\log_2 26 - H(p_{\text{Eng}})} \right\rceil \approx 28.$$

Thus messages of length at least 28 can usually be deciphered, but not when the length is less. When we have such a short length, then exhaustive key search will sometimes discover two or more pairs (plaintext x , key K) so that $\text{enc}_K(x)$ equals the given plaintext. Thus the decipherment is not unique below the unicity distance.

- (ii) We take our toy example with $\mathbb{A} = \{a, b, c\}$ from Example A.5 (iii), and the same encryption method as in (i), namely by a random permutation on three letters. Then $I(\mathbb{K}) = \log_2(3!) = \log_2 6 \approx 2.585$, and the unicity distance is

$$d = \left\lceil \frac{\log_2 6}{\log_2 3 - H(p)} \right\rceil = 86.$$

Thus ciphertexts of length at least 86 will usually have a unique solution (cleartext, key), and shorter ones may have several solutions.

- (iii) In the one-time pad (Section 2.1), we have an n -bit message (in English, coded in 8-bit Extended ASCII, say) of length n , so that $H(p) = H(p_{\text{Eng}})/8 \approx 0.525$, an n -bit random key, with $I(\mathbb{K}) = n$, and the ciphertext of n bits. The alphabet is $\{0, 1\}^n$, so that $s = 2^n$, and the unicity distance is

$$d = \left\lceil \frac{n}{n - 0.525} \right\rceil = 2.$$

Thus the “two-time pad” would be unsafe, and that is why the rules say you may transmit only a single message with the same key.

- (iv) What about a modern system like AES? Suppose we encrypt English plaintext (small letters only, no spaces, punctuation etc.) by coding it in 8-bit Extended ASCII and then applying 128-bit AES with a 128-bit random key. Each letter contains 4.198 bits of information, so that the ASCII message has $4.198 \cdot 128/8 \approx 67.17$ bits of information per 128-bit word of the alphabet $\{0, 1\}^{128}$. The key has $I(\mathbb{K}) = 128$ bits, so that the unicity distance is

$$d = \left\lceil \frac{128}{\log_2 2^{128} - 67.17} \right\rceil = 3.$$

Thus three transmitted messages would be enough to determine the key, if only we could perform an exhaustive key search . . .

- (v) Enigma

◇

In summary, Shannon’s theory tells us that for ciphertexts with a certain minimum length, namely his unicity distance, we can expect a single “solution” (plaintext, key), and below this minimum, we will usually have several solutions. It does not tell us how to find these solutions.

It does not say much about modern cryptosystems with huge alphabets, say of size 2^{128} in the smallest version of AES. It does say that very short messages are not uniquely decipherable even in easy-to-break systems like short-keyword-driven alternations between random permutations. But this does not inspire much confidence.

We will come across two occasions where a decipherment of a codebook had to be proven correct to a skeptical audience: the English King’s cryptanalysts confirming Layer’s guilt in 1722 (??), and *Room 40* and US President Wilson convincing American public opinion (and the rest of the world) of the authenticity of the Zimmermann telegram (Section F.4).

The attentive reader has already realized how to help these cryptanalysts: simply show that the message is longer than the unicity distance. Then Theorem A.11 says that the decipherment is unique.

Chapter 2

Security issues

2.1. Perfect security: the one-time pad

Consider the bit string $x = 100110$ of length six. BOB and ALICE have previously established the secret key $K = 010011$ which was randomly chosen among the strings of six bits. Then BOB forms the bitwise *exclusive or* (*XOR*) \oplus , so that $y = x \oplus K = 100110 \oplus 010011 = 110101$. We have $(a \oplus b) \oplus b = a \oplus (b \oplus b) = a \oplus 0 = a$ for any bits a, b , and so $y \oplus K = (x \oplus K) \oplus K = x \oplus (K \oplus K) = x \oplus (0 \cdots 0) = x$. We define $\text{enc}_K(x) = x \oplus K$, $\text{dec}_K(y) = y \oplus K$. Then $\text{dec}_K(\text{enc}_K(x)) = x$.

THEESIS 2.1. *This system is perfectly secure.*

What does this mean? Can we make this precise?

First attempt: We have a fixed number $n \in \mathbb{N}$. The message space is $\{0, 1\}^n$, so that each message x is a string of n bits. The key K is chosen *uniformly at random* among the 2^n possibilities in $\{0, 1\}^n$. For each string $z \in \{0, 1\}^n$, we have

$$\text{prob}(K = z) = 2^{-n}.$$

Now x and K are chosen. Then $y = x \oplus K$ is determined, and $x = y \oplus K$. Furthermore, EVE sees y but does not know K .

For how many pairs (x', K') is $\text{enc}_{K'}(x') = \text{enc}_K(x) = y$? For each $x' \in \{0, 1\}^n$, there is precisely one K' with this property, namely $K' = x' \oplus y$. (Check: $x' \oplus K' = x' \oplus (x' \oplus y) = (x' \oplus x') \oplus y = y$.) Therefore, just given y , each x' is equally likely to have been the message. EVE has learnt nothing from y about x .

Second attempt: Each message $x \in \{0, 1\}^n$ occurs with some probability p_x : So we have $p_x \geq 0$, $\sum_{x \in \{0, 1\}^n} p_x = 1$.

THEOREM 2.2. *Using conditional probabilities, we have for all x, y :*

$$\text{prob}(\text{message} = x | \text{encryption} = y) = p_x.$$

PROOF. Let M be the message, C its encryption. Then

$$\text{prob}(M = x | C = y) = \frac{\text{prob}(M = x \wedge C = y)}{\text{prob}(C = y)},$$

Consider the numerator first:

$$\begin{aligned} \text{prob}(M = x \wedge C = y) &= \text{prob}(M = x \wedge K = x \oplus y) \\ &\stackrel{*}{=} \text{prob}(M = x) \cdot \text{prob}(K = x \oplus y) \\ &= p_x \cdot 2^{-n}, \end{aligned}$$

where $*$ holds since K is independent of M , and the last equation since K is chosen uniformly. Now we calculate the denominator:

$$\begin{aligned} \text{prob}(C = y) &= \sum_{z \in \{0,1\}^n} \text{prob}(M = z \wedge C = y) \\ &= \sum_{z \in \{0,1\}^n} \text{prob}(K \oplus M = y \wedge M = z) \\ &= \sum_{z \in \{0,1\}^n} \text{prob}(K = z \oplus y) \text{prob}(M = z) \\ &= 2^{-n} \cdot \sum_{z \in \{0,1\}^n} \text{prob}(M = z) \\ &= 2^{-n} \sum_x p_x = 2^{-n}, \end{aligned}$$

where we use again, that K is chosen independently of M .

Thus each encryption is equally likely, independent of the message. We find

$$\text{prob}(M = x | C = y) = \frac{p_x \cdot 2^{-n}}{2^{-n}} = p_x. \quad \square$$

The claim depends critically on the uniform random choice of the keys K . Otherwise, it is false.

REMARK 2.3. *Should there be also two-time pads? Suppose that two messages x, x' are encrypted with the same key K :*

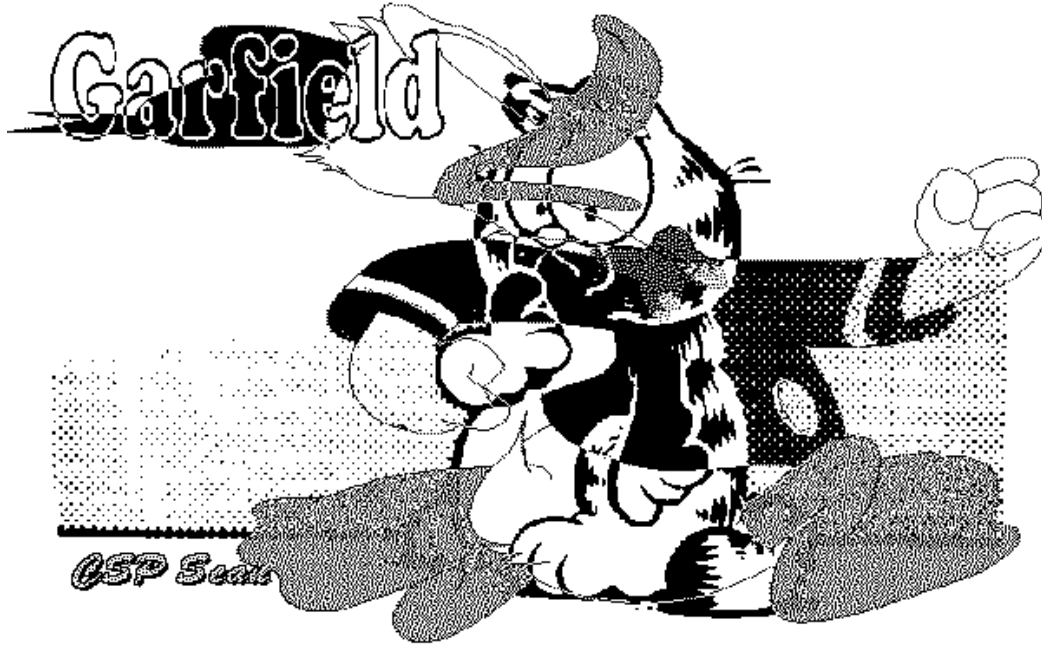
$$y = x \oplus K, y' = x' \oplus K.$$

Then

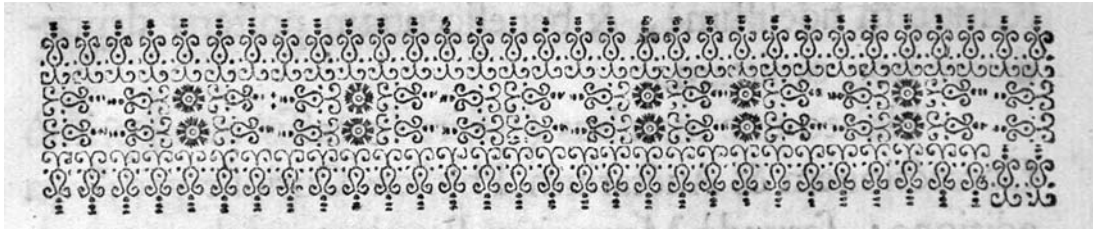
$$\begin{aligned} y \oplus y' &= (x \oplus K) \oplus (x' \oplus K) \\ &= x \oplus x' \oplus K \oplus K = x \oplus x'. \end{aligned}$$

Hence, ...

You are not convinced? So consider images, coded as strings of bits. The exclusive or of two images x , x' clearly contains still a lot of information:



Now the conclusion is clear ...



Chapter B

Key addition and modular arithmetic



his chapter presents some historical examples of key-addition systems. These are easy to describe with our modern notion of modular arithmetic. Already in 1690, a rather obscure French author, Claude Comiers, had the right intuition about the arithmetic nature of such systems. But without the proper notions and notations, it is very strenuous to express these things. Remove repetitions Sections 1+2

B.1. Key addition systems

In a key addition system, given a message, one produces a key of the same length and adds the two together, letter by letter, to obtain the encryption. This is then transmitted, and the legitimate receiver only has to subtract the key, again letter by letter, to find the original message. This can be described as

$$(B.1) \quad \begin{aligned} \text{ciphertext} &= \text{plaintext} + \text{key}, \\ \text{plaintext} &= \text{ciphertext} - \text{key}. \end{aligned}$$

More formally, we have letters from a fixed alphabet of some size m (in modern English, $m = 26$), and then the plaintext $x = (x_0, x_1, \dots)$, the key $k = (k_0, k_1, \dots)$, and the ciphertext $y = (y_0, y_1, \dots)$ are related as

$$y_i = x_i + k_i, \quad x_i = y_i - k_i$$

for all i . Here addition and subtraction take place in the additive group $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$, that is, by doing arithmetic modulo m . The relation between the alphabet and \mathbb{Z}_m is taken in the natural way: $a \longleftrightarrow 0, b \longleftrightarrow 1, \dots$

A simple example is to encrypt vigenere cipher with the key caesar, using Table A.1 for the letter-to-number conversion.

Table B.1: A de Vigenère encryption

clear	v	i	g	e	n	e	r	e	c	i	p	h	e	r
	21	8	6	4	13	4	17	4	2	8	15	7	4	17
key	c	a	e	s	a	r	c	a	e	s	a	r	c	a
	2	0	4	18	0	17	2	0	4	18	0	17	2	0
cipher	23	8	10	22	13	21	19	4	6	0	15	24	6	17
	x	i	k	w	n	v	t	e	g	a	p	y	g	r

Thus the ciphertext xikwn vtega pygr would be transmitted. Many ways of producing the required key have been employed. We have seen the Caesar cipher, where one uses a single letter and repeats it as often as necessary: $k_i = k_0$ for all i . Caesar used $k_0 = 3$, and Augustus $k_0 = 1$ (with $z + k_0 = aa$). The abbot Iohannes Trithemius . published in 1518 his *Polygraphia*, the first printed book about cryptography; ?? describes some details. It contains, among other things, his *Recta transpositionis tabula*¹ (??) consisting of the 24 Caesar substitutions on his 24-letter alphabet $\{a, b, c, d, e, f, g, h, i, k, \ell, m, n, o, p, q, r, s, t, u, x, y, z, w\}$. Trithemius . suggested to use these substitutions one after the other. But together with the idea from Blaise de de Vigenère's 1586 *Traicté des Chiffres* of using a keyword-driven alternation between the various Caesar ciphers, this gives the *de Vigenère cipher*, which was famous as the *chiffre indéchiffrable* or *unbreakable cipher* for centuries. Formally, one has a keyword $k_0, \dots, k_{\ell-1}$ of some length ℓ , and repeats this as necessary: $k_i = k_{i \bmod \ell}$ for all i . This is illustrated in Table B.1 with the keyword $k_0 k_1 k_2 k_3 k_4 k_5 = \text{Caesar}$ of $\ell = 6$ letters, and the encryption is $y_i = x_i + k_i$.

The *autokey systems* proposed by de Vigenère are discussed in ??.

Modern variants, usually over the binary alphabet, are the *one-time pad* (Section 2.1) where the key k is a random sequence of the same length as the message, and variations where one has an initial segment of the key (possibly random) and generates the remaining key letters in a pseudorandom fashion. Modern pseudorandom generation is discussed in ??. There were electromechanical machines implementing this principle already during World War II: the Siemens Geheimschreiber in Germany, and the British Typex.

¹square table of substitutions

A systematic method for breaking the de Vigenère system was published by Kasiski (1863) and is explained in Chapter C. Charles Babbage had found a solution method earlier, in February or March of 1846, but never published it. His notes were discovered in the early 1980s in the British Library; Franksen (1984) narrates the story. The central part of Babbage's success is his discovery of (B.1), which he writes as

$$\begin{aligned}\text{Cypher} &= \text{Key} + \text{Translation} - 1, \\ \text{Translation} &= \text{Cypher} - \text{Key} + 1.\end{aligned}$$

The ± 1 comes from the fact that he starts his alphabet with $a = 1$ instead of $a = 0$, as we do.

Was Babbage the first to discover the key equation (B.1)?



Chapter C

Breaking the unbreakable

Resteemed as “le chiffre indéchiffrable”, the de Vigenère system was considered unbreakable for over three centuries. Its workings and arithmetic nature have been explained in Chapter B. We now present an attack from 1863 which brings the system to its knees. However, it did not really diminish the system’s popularity, and it was reinvented again and again by people unaware of this attack. first popular acct of Kasiski? Combine Figures C.3, C.4, C.5 into one? Bugeaud & Mignotte has appeared? End of C.3: calculate mc’s! C.4: color Playfair! Porta table

In fact, the British scientist Charles Babbage (1792-1870), inventor of the mechanical computer, seems to have broken the de Vigenère system (see Franksen 1993), but his work was kept secret. The first published attack on the de Vigenère was a 95-page booklet written by the Prussian officer Wilhelm Kasiski (1805-1881). We present his cryptanalysis, and also a tool later developed by the US cryptographer William Friedman (1891-1969): the index of coincidence.

C.1. Kasiski’s attack on de Vigenère

In this section, we discuss the attack by Kasiski (1863) on the de Vigenère cryptosystem, and in fact on a generalization of it with arbitrary simple substitutions instead of just Caesar ciphers.

We have an alphabet \mathbb{A} of s letters and a secret key $k = (\pi_0, \dots, \pi_{m-1})$ consisting of m permutations π_0, \dots, π_{m-1} of \mathbb{A} . The encryption is by applying $\pi_0, \dots, \pi_{m-1}, \pi_0, \dots, \pi_{m-1}, \pi_0, \dots$ to the consecutive letters of the plaintext

$x = (x_0, x_1, \dots)$, so that the ciphertext is

$$y = (y_0, y_1, \dots) = (\pi_0(x_0), \dots, \pi_{m-1}(x_{m-1}), \pi_0(x_m), \dots, \pi_{m-1}(x_{2m-1}), \pi_0(x_{2m}), \dots).$$

In other words, we have $y_i = \pi_{i \bmod m}(x_i)$ for each i . The de Vigenère system is the special case where an alphabetical key $(k_0, \dots, k_{m-1}) \in \mathbb{A}^m$ is given and

$$\pi_i(x) = x + k_i,$$

where addition in \mathbb{A} is addition modulo s . Thus each π_i is the Caesar cipher with shift by k_i . An example is given in Table B.1.

Kasiski's cryptanalysis, that is, finding the message x and key k from y , proceeds in two stages:

- find the key length m ,
- determine each permutation π_0, \dots, π_{m-1} .

As our running example, we take the following ciphertext of 348 letters, generated by a de Vigenère system:

	0	5	10	15	20	25
0	KODGD	UCXEM	XGMFQ	PUEUX	DDOVA	ZXLOE
30	HSMVY	YEJRV	YPAMC	LWGAQ	YXYSK	CFOKI
60	VKYIN	CSLAC	BLJGW	HDQXN	GMMGA	NJRVN
90	FQRNC	GNYDE	CSTXF	MNPIV	UWFHN	RWVIN
120	UCRGM	RULUC	GNYDE	MISWZ	GTHSM	TPQTX
150	FWVSF	DXAFT	JUVNE	FWWAU	AFGPC	XSCST
180	XRMKN	RGNRM	NMFMK	LFBNJ	GKCKO	DVXTA
210	QYXYJ	ACMDR	WLHZQ	SNZWK	CPFAS	ERMGR
240	KSVRY	ZDHSM	KZADH	XGUCP	IEMVX	BUNCS
270	XHSDQ	DEJMC	DSJRV	MFMTN	SMKFQ	AMEFW
300	OGAAX	WKQNE	MMKIM	EEMSX	PFQRN	LALKM
330	JNWLR	QTAUP	LAGZK	OML		

M	N	X	S	A	G	F	C	R	K	D	E	W
8.62	5.46	5.17	5.17	5.17	4.89	4.89	4.89	4.6	4.6	4.31	4.02	3.74
V	U	Q	L	Y	T	P	J	H	Z	O	I	B
3.74	3.45	3.45	3.45	3.16	2.59	2.59	2.59	2.59	2.01	2.01	2.01	0.86

Table C.1: Frequency table for cryptogram

In any classical cryptanalysis, the first thing is to count how often each encrypting symbol occurs, as was done in Figure A.9 for the Gold-Bug cryptogram. Figure C.1 shows the frequency-ordered frequency tables for English

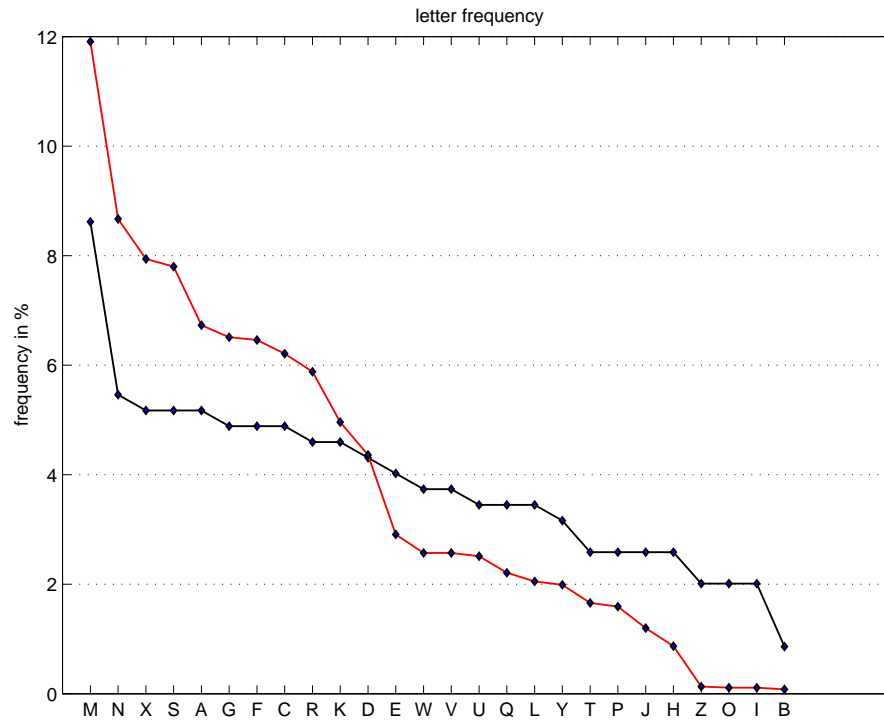


Figure C.1: English frequencies (Harry Potter, in red) and ciphertext (in blue), both ordered by frequency.

and for our cryptogram. The two curves differ sufficiently for us to conclude that we are not dealing with a simple substitution. No wonder—we set it up as a de Vigenère encryption.

For the first step in his cryptanalysis, Kasiski looks at all polygrams (= sequences of two or more letters) that occur repeatedly in the ciphertext, then factors the differences of their initial positions, and determines m as the most frequently occurring factor. He says: *Jetzt sucht man zuerst zu ermitteln, aus wieviel Buchstaben der Schlüssel besteht. Zu diesem Zweck sucht man in der aufgeschriebenen Chiffre=Schrift alle Wiederholungen von zwei und mehreren Chiffren auf, zählt dann die Entfernung der gleichen Wiederholungen von einander, schreibt diese mit der Zahl ihrer Entfernung von einander unter die Chiffre=Schrift und sucht diese Zahl in ihre Faktoren zu zerlegen.*¹

The idea is that, with sufficiently long plaintext and short key, there will a repeated polygram like ...you ...you ... in the plaintext which happens to be encrypted by the same piece of the key:

...y	o	u	...	y	o	u	...
...m	a	j	...	m	a	j	...
...K	O	D	...	K	O	D	...

In fact, this is precisely what takes place at positions 0 and 203 of our example. Of course, it may also occur that unrelated pieces of plaintext and key happen to add up to the same ciphertext. In the example, the repeated TXF at positions 102 and 148 is of this nature. But we will see that these accidents are not a serious obstacle.

We now turn to Kasiski's suggestion: Look at repeated polygrams! The polygrams of length at least three that occur repeatedly are given in the following list, together with the factorization of the difference in positions of occurrences. The column "rep" gives the number of repetitions; a polygram repeated four times gives rise to six pairwise differences. The column "first" is the first occurrence.

Furthermore, there are 73 repeated bigrams, three of them five times, five of them four times, fifteen thrice and fifty twice. Their statistics are in the following table which shows for each prime power how many positional differences it divides. Thus the factor 4 for the pentagram JRVMF gives a contribution of one for the prime powers 2 and 2^2 .

Furthermore, the prime powers 2^5 , 2^6 , 2^7 , 13^2 , 17, 41, 62, 71, 73, 89, 113, 137, 179, 197, 229, and 241 divide exactly one bigram difference. This table strongly

¹Now one first tries to determine of how many letters the key consists. To this end, one finds all repetitions in the ciphertext of two or more letters, counts the relative distances of repetitions of the same polygram, writes these with their distance below the ciphertext, and tries to factor these distances.

polygram	rep	first	distance	polygram	rep	first	distance
CGNYDE	2	94	$5 \cdot 7$	JRV	3	37	$7^2, 5 \cdot 7^2, 2^2 \cdot 7^2$
AQYXY	2	48	$7 \cdot 23$	AQY	2	48	$7 \cdot 23$
JRVMF	2	86	$2^2 \cdot 7^2$	QYX	2	49	$7 \cdot 23$
CGNYD	2	94	$5 \cdot 7$	YXY	2	50	$7 \cdot 23$
GNYDE	2	95	$5 \cdot 7$	NCS	2	64	$7 \cdot 29$
AQYX	2	48	$7 \cdot 23$	RVM	2	87	$2^2 \cdot 7^2$
QYXY	2	49	$7 \cdot 23$	VMF	2	88	$2^2 \cdot 7^2$
JRVM	2	86	$2^2 \cdot 7^2$	FQR	2	90	$3 \cdot 7 \cdot 11$
RVMF	2	87	$2^2 \cdot 7^2$	QRN	2	91	$3 \cdot 7 \cdot 11$
FQRN	2	90	$3 \cdot 7 \cdot 11$	CGN	2	94	$5 \cdot 7$
CGNY	2	94	$5 \cdot 7$	GNV	2	95	$5 \cdot 7$
GNYD	2	95	$5 \cdot 7$	NYD	2	96	$5 \cdot 7$
NYDE	2	96	$5 \cdot 7$	YDE	2	97	$5 \cdot 7$
CSTX	2	100	$7 \cdot 11$	CST	2	100	$7 \cdot 11$
THSM	2	141	$3 \cdot 7^2$	STX	2	101	$7 \cdot 11$
HSMK	2	247	$2 \cdot 3 \cdot 7$	TXF	2	102	$2 \cdot 23$
KOD	2	0	$7 \cdot 29$	THS	2	141	$3 \cdot 7^2$
MFQ	2	12	$7 \cdot 11$	EFW	2	164	$7 \cdot 19$
HSM	4	30	$2^4 \cdot 7, 7 \cdot 31, 7 \cdot 37$	MFM	2	191	$2 \cdot 47$
			$3 \cdot 5 \cdot 7, 3 \cdot 7^2, 2 \cdot 3 \cdot 7$	SMK	2	248	$2 \cdot 3 \cdot 7$

Table C.2: Repeated polygrams of length at least three.

prime power	total	length of polygram					prime power	total	length of polygram				
		6	5	4	3	2			6	5	4	3	2
2	72	1	3	8	60		13	10					10
2^2	42	1	2	4	35		19	5				1	4
2^3	21				1	20	23	18	1	2	4	11	
2^4	10				1	9	29	10				2	8
3	53			3	7	43	31	6				1	5
3^2	6					6	37	4				1	3
5	40	1	2	3	6	28	43	7					7
5^2	2					2	47	6				1	5
7	129	1	4	11	28	85	59	2					2
7^2	28		1	3	7	17	109	2					2
11	26			2	5	19	127	4					4

Figure C.2: The number of times that prime powers divide distances between repetitions.

indicates a key length of seven, and we take seven as our first guess for the key length. We split y into seven blocks z_0, \dots, z_6 , consisting of each seventh letter, so that

$$(C.1) \quad z_i = (y_i, y_{i+7}, y_{i+14}, \dots).$$

z_0 : KXQDOYAQFIBQAQDMFNUGGQFUAXMMFKQMOPGZAPUDDMQGNEQMTZ
 z_1 : EPOEEMYONLXNRENHULETTDVUSKNBOYDSFRDDINQSTAAEERJAK
 z_2 : DMUVHJCXKCJNJCPCUMHXXNACNMNDXRNAKHHECDJHMAMMNNUO
 z_3 : GXEASRLYISGGRCISFAEFSRFJVYWZSSSXMSERSEXMSLWPM
 z_4 : DGUZMVWSVLWMVGTWVGGSWWFFGTGMGXJLWEVMGVXJVMFWKXALLL
 z_5 : UMXVYVGKKAHMMNXUVMNWTVTWPXNKKTAHKRRKUXHMMKWKIPLRA
 z_6 : CFDLPACYCDGFYFWIRYZPSJWCRRLCACZCMYZCBSCFFOQMFKQG

Depending on the system used, each block z_i is either enciphered with a Caesar system, or by some arbitrary permutation π_i . We start with the first case, corresponding to the de Vigenère system, and which is indeed used in our example.

The cleartext corresponding to a block z_i is made up of each seventh letter of some English text. Thus it does not consist of English words, but can still be expected to follow the frequency distribution of English letters. The same holds for z_i , except that it is translated by a Caesar shift, and we can expect to solve it by frequency analysis. An inconvenience is that the available ciphertext is much shorter, namely only one seventh of the original length, which comes to about 50 letters in our case.

We set up the seven frequency tables:

$$\begin{aligned}
 z_0 : & \begin{array}{cccccccccccccccc|c} \text{Q} & \text{M} & \text{D} & \text{F} & \text{A} & \text{U} & \text{G} & \text{Z} & \text{X} & \text{P} & \text{N} & \text{K} & \text{Y} & \text{T} & \text{O} & \text{I} & \text{E} & \text{B} & \text{M} \\ \hline 9 & 6 & 5 & 4 & 4 & 3 & 3 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array} \\
 z_1 : & \begin{array}{cccccccccccccccc|c} \text{E} & \text{N} & \text{O} & \text{D} & \text{T} & \text{S} & \text{R} & \text{A} & \text{Y} & \text{U} & \text{L} & \text{K} & \text{X} & \text{V} & \text{Q} & \text{P} & \text{M} & \text{J} & \text{I} & \text{H} & \text{F} & \text{B} & \text{A} \\ \hline 7 & 5 & 4 & 4 & 3 & 3 & 3 & 3 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array} \\
 z_2 : & \begin{array}{cccccccccccccccc|c} \text{N} & \text{M} & \text{C} & \text{H} & \text{X} & \text{J} & \text{U} & \text{D} & \text{A} & \text{K} & \text{V} & \text{R} & \text{P} & \text{O} & \text{E} & \text{J} \\ \hline 9 & 6 & 6 & 5 & 4 & 4 & 3 & 3 & 3 & 2 & 1 & 1 & 1 & 1 & 1 & 1 \end{array} \\
 z_3 : & \begin{array}{cccccccccccccccc|c} \text{S} & \text{R} & \text{E} & \text{X} & \text{M} & \text{I} & \text{G} & \text{F} & \text{Y} & \text{W} & \text{L} & \text{C} & \text{A} & \text{Z} & \text{V} & \text{P} & \text{J} & \text{O} \\ \hline 11 & 6 & 4 & 3 & 3 & 3 & 3 & 3 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 \end{array} \\
 z_4 : & \begin{array}{cccccccccccccccc|c} \text{G} & \text{V} & \text{W} & \text{M} & \text{L} & \text{X} & \text{F} & \text{T} & \text{S} & \text{J} & \text{Z} & \text{U} & \text{K} & \text{E} & \text{D} & \text{A} & \text{C} \\ \hline 8 & 7 & 6 & 6 & 5 & 3 & 3 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array} \\
 z_5 : & \begin{array}{cccccccccccccccc|c} \text{K} & \text{M} & \text{X} & \text{W} & \text{V} & \text{U} & \text{T} & \text{R} & \text{N} & \text{H} & \text{A} & \text{P} & \text{Y} & \text{L} & \text{I} & \text{G} & \text{G} \\ \hline 8 & 6 & 5 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 2 & 1 & 1 & 1 & 1 & 1 \end{array}
 \end{aligned}$$

$$z_6 : \begin{array}{c|cccccccccccccccc|c} \text{C} & \text{F} & \text{Y} & \text{Z} & \text{R} & \text{W} & \text{S} & \text{Q} & \text{P} & \text{M} & \text{L} & \text{G} & \text{D} & \text{A} & \text{O} & \text{K} & \text{J} & \text{I} & \text{B} & \text{Y} \\ \hline 9 & 6 & 5 & 3 & 3 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}$$

The letters that do not occur in z_i are not shown. Now the easiest approach is to assume that the most frequent letter represents E . For z_0 we take Q and obtain the key as $k_0 = Q - E = M$. The seven key letters obtained by this crude guess are given in the last column. But Kasiski (1863) warns: *Man wird jedoch nur in seltenen Fällen so glücklich sein, aus einigen Zeilen alle richtigen Buchstaben des Schlüssels durch die Schlüssel-Tabelle zu ermitteln, [...] weil die Buchstaben der Schrift zwar im Allgemeinen in dem [üblichen] Verhältniß vorkommen; in kürzern Schriften jedoch sehr auffallende Abweichungen stattfinden können.*² And indeed ours is not one of those rare cases. When we decipher with the key MAJOCGY, we find:

YOUSB	OELED	JEGHE	PLQSR	FROMM	XRNCE
YEKPA	MEADT	SROMT	XUACE	YOKQE	ETOB
TEAWN	TEJUE	PLASU	BFEXE	SKGIO	NADTG
HEREO	EHARE	TERRH	ANGUT	OYTHE	DUPKB
UTDEG	TILLO	EHARE	DUQQB	UTYEK	NRETO
RUPUT	DOMDN	LIVEQ	DQYOU	RREJE	LSTER
RTAKE	DEHTA	NDRKE	NTBEV	EEEYO	UHVNC
EYOKH	UEADI	IJBBE	SELUE	EDFRE	CLOUR
BETLA	NDYEK	EBODY	JEOED	IVYTR	DINTE
VBURQ	UQHGE	RSADT	GHATY	EKEHE	ADQDQ
QUARJ	UESBE	DYICO	SEDEV	JHERE	XYFMA
JEIJL	SHALB	JUINK	FYJ		

We recognize some English-looking pieces of text, but clearly we have not deciphered the message.

A more successful method is not to rely just on E as occurring most frequently, but to try to match visually the English frequencies with a shift of the ciphertext frequencies. We only do this for the fourth block z_3 . According to the categories in the small figure on page 38, the most frequent ciphertext letter S ($= 18$) is likely to stand for e , t , a , or o ($= 4, 19, 1, 14$). This corresponds to shifts by O , Z , S , or E ($= 14, 25, 18, 4$).

In Figures C.3, C.4, and C.5 we display English frequencies and those of z_3 , shifted by $-O$, $-E$, and $-A$, respectively.

3 figures on one double page

In which of the three figures do you see the better match? The shift $-E$ looks calmer than the others because the black and colored lines cross each

²Only in rare cases will one be so lucky as to determine all key letters correctly by this table, given a ciphertext of a few lines. The reason is that the cleartext letters occur in general with the usual frequencies, but that there can be considerable fluctuations in short texts.

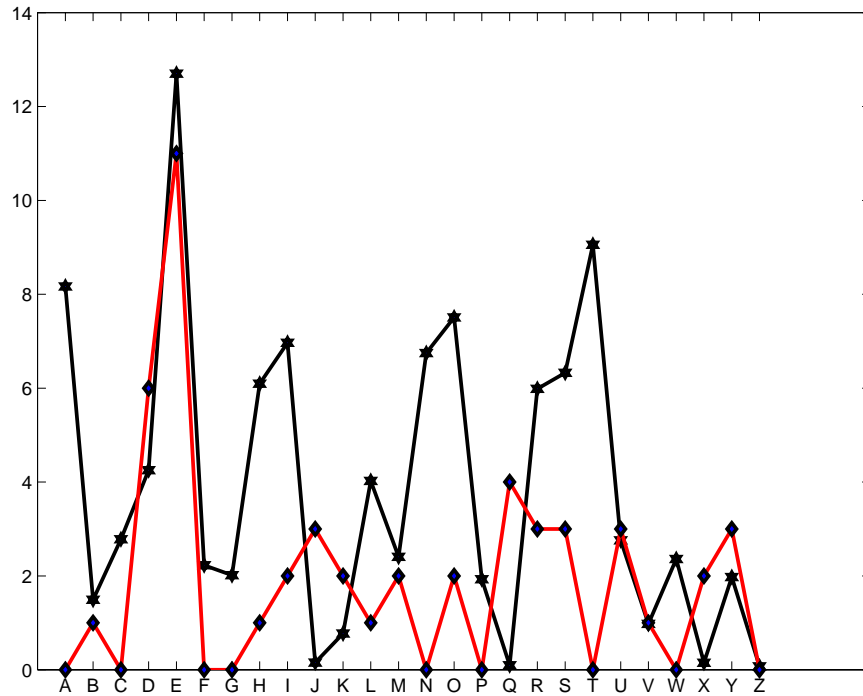


Figure C.3: English frequencies (in black) and the frequencies in z_3 shifted by $-O$ (in red).

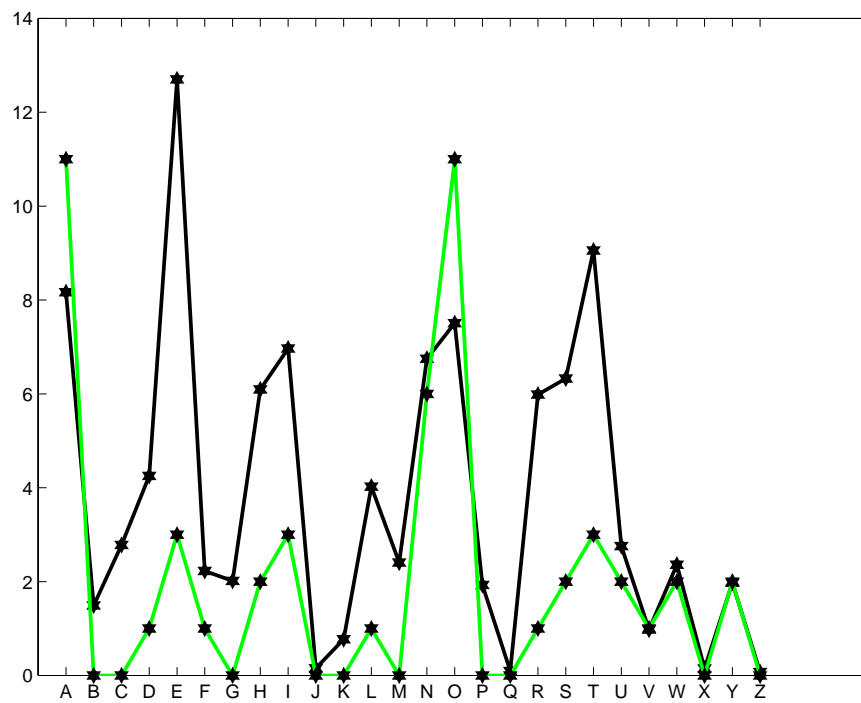


Figure C.4: English frequencies (in black) and the frequencies in z_3 shifted by $-E$ (in green).

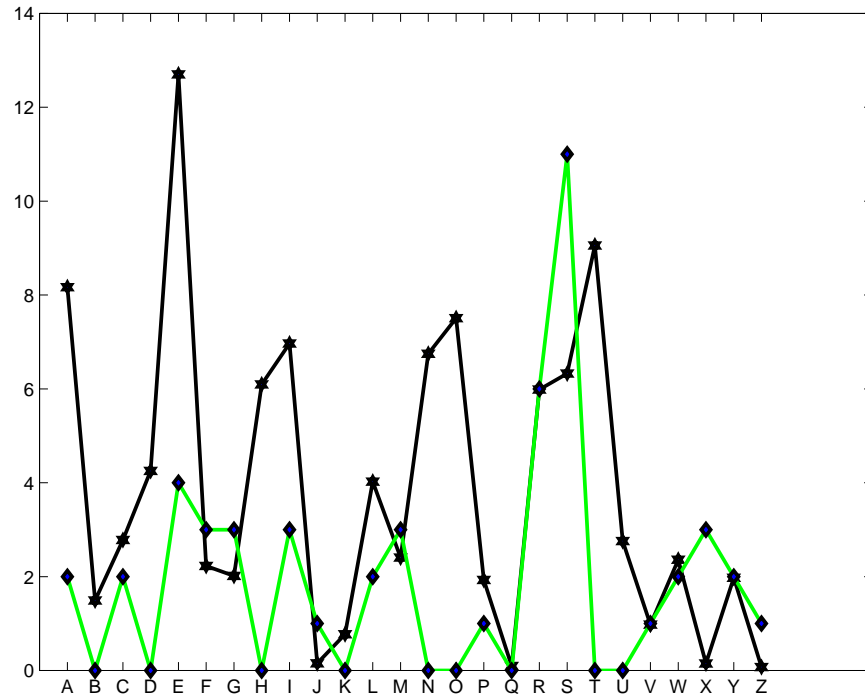


Figure C.5: English frequencies (in black) and the frequencies in z_3 shifted by $-A$ (in green).

other least often. Two standard measures, namely the sum of the absolute values of the differences and the sum of their squares, confirm this impression:

shift	–O	–E	–A
$\sum \text{diff} $	75.73	60.75	73.42
$\sum \text{diff}^2$	366.15	273.81	418.22

In ??, we will learn a computational method, called the index of coincidence, that implements such a visual approach quite reliably.

This visual analysis, applied to all seven subtexts, reveals the correct keyword MAJESTY. The plaintext is the sentence of the British conspirator Layer in 1722 (page ??), and you can check that the “English-looking” parts of the incomplete decipherment on page 67 agree with the plaintext in the four consecutive positions $-1, 0, 1, 2$, corresponding to the correct key letters YMAJ. Somewhat informally, we can describe this cryptanalytic method as follows.

ALGORITHM C.2. Kasiski attack on de Vigenère cipher.

Input: ciphertext y , assumed to be de Vigenère-encrypted.

Output: key length ℓ , key k and cleartext x , hopefully. Otherwise “no Vigenère”.

1. Set up the table of repeated polygrams and their factored positional differences, as on page 64.
2. For each prime power, determine how many positional differences it divides, as on page 65.
3. Guess ℓ as the product of some of the most frequently occurring prime powers in step 2.
4. Form ℓ ciphertexts $z_0, \dots, z_{\ell-1}$ by taking each ℓ th letter from y , as in (C.1).
5. Assume that each z_i is a simple substitution, and cryptanalyze it with Algorithm ?? simple substitution algorithm. If one of these return “no simple substitution”, then go to step 3.
6. Try to match the various answers returned in step 5.

The de Vigenère cipher was considered unbreakable (“chiffre indéchiffrable”) for several centuries. Even Kasiski’s successful attack in 1863 took quite some time to become widely known. But the basic idea of Kasiski’s method had already been glimpsed in the Renaissance!

Giovanni Battista della della Porta (1535–1615) published in 1563 his *De Furtivis Literarum Notis*³. He describes a large variety of cryptosystems, many of them beautifully illustrated and quite impractical to use. Included is an imaginative representation of a skytale, and the della Porta disk (see ?). In the second edition, from 1602, della Porta proudly starts his Chapter 17 on “how

³On secret encryptions of messages

a message prepared with a key may be solved and read without the key” with *NVNC rem arduam & magnam molimur*⁴.

He deciphers the following message of 77 letters, which he has set up himself:

```

0      5      10      15      20      25      30      35      40
mmmbtxco pxb dfbv gst inrgtn gtc cc ctg amhcm ahto

45      50      55      60      65      70      75
xtmoq slqpr mmbbtth mhv, aceohg lll li nxioq.

```

della Porta's original text shows some word divisions, but not the position numbers that we put on top. della Porta makes several observations, most of which are not useful in general. But he points to the repetitions of *mmm* in positions 0 and 51, and the *llll* in position 67. And then he says: *Since there are 17 letters between the 3 letters MMM and the 4 letters LLLL and 51 between the first 3 MMM and the same 3 letters repeated in the thirteenth word, I conclude that the key has been given 3 times, and decide correctly that it consists of 17 letters.*

For the repeated *mmm*, this is Kasiski's argument! della Porta fails to say that he has to take the second *l* of *llll*. He does not look at arbitrary repeated polygrams, as Kasiski does, but only at consecutive repetitions of the same letter in the ciphertext. These arise, for example, when there are arithmetic progressions in the plaintext and the key, one with the negative increment of the other.

He then guesses the 17-letter keyword, first *studens sic deficio* and *studium sic deficio* incorrectly, then *studium hic deficit*⁵ correctly, to find the plaintext

```

0      5      10      15      20      25      30      35      40
pontiane, est uxor tua mortua, vix ut sit nomen suum,

45      50      55      60      65      70      75
nihil manet, pontius cur studet non me latet.6

```

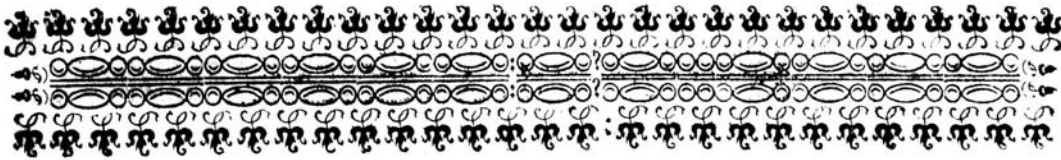
We note that della Porta has taken great care to include the arithmetic sequences *cdef*, *pon* and *[r]stu* for plaintext and key. He has encrypted four letters incorrectly.

della Porta's observations do not yield a general method for breaking de Vigenère systems. The key ingredient of Kasiski's approach is present: the key length is likely to divide positional differences of repeated polygrams. But neither della Porta nor any other cryptographer took up this insight at the time—as far as we know—and the de Vigenère remained secure for another 250 years.

⁴We will now undertake a great and difficult enterprise.

⁵eagerness is missing here

⁶della Porta presumably had a hard time making up a phrase that displays his arithmetic progressions in the right places, and it is not easy to make sense of the cleartext: Pontiane is your wife, recently deceased; let her name be [praised], no [tears] shed; it is not hidden to me why Pontius makes an effort.



Chapter D

Codebooks

Simple substitutions generalize the Caesar cipher. One step further are the nomenclators and codebooks, which we present in this chapter. They work like simple substitutions, except that they have much larger alphabets: not just letters, but also bigrams, syllables, words, and names of people and places. Examples exist already from the 14th century, and a century later we find code factories at work that output series of codebooks by minor variation of a general template. In the First World War, top secret diplomatic messages were encrypted in this way, for example the Zimmermann telegram discussed in Chapter F. These nomenclators encode many frequently occurring words with individual encryptions. We will see examples of their use by British and by Cuban conspirators (Sections ?? and ??), and in private correspondence (Sections ?? and ??). The idea was employed in a different way when the telegraph came into use, namely in the form of commercial codebooks for reduced telegraph costs. If secrecy was needed, they could be superenciphered.

D.1. Nomenclators

A *codebook* (or *code*) is a list of frequently used terms (plus individual letters and, sometimes, syllables) and a codeword for each of them. They have been used since the Renaissance, and had their own renaissance with the rise of telegraphic correspondence, in particular the trans-Atlantic cable in 1866.

Historically, they were called *nomenclators*. This was originally the designation of the ushers who called out (*calamare*) the name (*nomen*) of a dignitary entering a party, and carried over to those secret books that contained the names of many dignitaries.

We do not know when codebooks of substantial size came into use, but an example from 1377 claims to be an original invention by the King of Navarra,

and seems to be the oldest surviving sample. During the hundred-year war, the Spaniards were allied with the English against the French. King Charles of Navarra used a codebook to communicate with his agent Pierre du du Tertre at Bernay in Normandy, and with his English allies. Both the complete codebook and the story of its invention have survived in the *Chronique Normande*, written when?.

En l'an mil .CCC. LXXvij., en Karesme, fu aprocheue une soutilie maniere de faire du roy de Navarre devant dit contre le roy de France, en maniere de traison, d'escripre couvertement et muer les nomz des prinches, des chastiax et bonnes villes en aultres nomz que les euz propres, si comme il aperra cy après, et fais par la sutilité mestre Pierre du Tuetre, conseiller du dit roy de Navarre.¹

When Charles de de Valois, King of France, captured the city of Bernay, du du Tertre was caught, and he and another councillor *ourent les colz trenchez*² on 28 June 1378. The codebook of 124 words includes the following:

Rex Francie, Nummularius;
Imperator, Agrippa;
Rex Anglie, Laceratus;
Rex Arragonie, Possessor;
Rex Castelle, Instrusor;
Rex Navarre, Callidus;
:
Dominus Karolus Navarre infans, Repertus;
Dominus Petrus, Restaurator;
:
Cesarisburgum, Capitolium;
Mare, Planicies;
Naves, Aquatice;
Monspessulanus, Bipennis;
Burdegalis, Ambrosia;
:
Burgundia, Detenta;
Normannia, Bispartita;
Britannia, Vulnerata;

¹Before Easter 1377, a subtle method of acting secretly against the King of France was devised by the King of Navarra. This was by writing covertly and moving the names of princes, castles and larger cities to other names, not their own, as apparent below, and it was made by the subtlety of Master Pierre du du Tertre, councillor to the King of Navarra.

²had their necks cut

:

The cleartext words shown here are: the King of France, the (German) Emperor, the Kings of England, Aragon, Castille, and Navarra; the sons Charles and Peter of the King of Navarra; Cherbourg, sea, ships, Montpellier, and Bordeaux; Burgundy, Normandy, and Brittany.

The King's two sons were held hostages by their uncle, the King of France. A sample letter from the King, written on 1 May 1378 at Pamplona, begins as follows:

S'il estoit ensy que *Nommularius* ne laissast partir de luy *Repertum*,
il est de neccessité que *Vexatus* pense et ymagine aucune voie com-
ment *Repertus* puist venir en *Bispartie* vers *Capitolium*.³

The King of France later did release the two sons and gave them back their lands in Normandy, now as fief of the King of France.

One century later, the new invention has become routine business. Figure D.1 exhibits an example from 1463. It comes from the records of the Milanese *Cancellaria segreta*⁴ which were mainly produced by Francesco Tranchedino (1441–c. 1496). They show an early Renaissance code factory at work. Since 1450, Cicco Simonetta had been First Secretary of the Secret Chancellery at the court of the Sforza Dukes in Milan. He wrote in 1474 the oldest Western text on cryptanalysis that has been conserved. (The Arab cryptographers like Al-Kindi had been centuries earlier; see ??) Nicodemo Tranchedino (1411–1481) was a well-known humanist and occupied a high position in the government. His son Francesco worked for Simonetta and produced in 1475 a catalog of 159 Milanese codebooks up to that time. This forms the nucleus of the manuscript which was continued by other officials and gives 297 such ciphers in total.

The cipher in Figure D.1 is quite typical. It starts with the date *23 August 1463* and the recipient D. [Dominus = Mr.] Antonio de Besana. Then the cipher begins with either two or three encryptions of the 21 letters plus &, con, and ex. The letters A, e, h, l, and q get three possibilities, the others two. Then come 12 dummies (*Nulle*) and 12 signs for doubled letters (*Duplicate*), from bb to tt. The center part has 63 signs for bigrams of the form 'vowel plus consonant'. The last part is the nomenclator proper and has encryptions of 31 *codewords*:

Pope, King of France, René d'Anjou (titular King of Naples), King Ferrante of Naples, Duke Philip the Beautiful of Burgundy, Duke Johannes (?), Duke of Milan, Venetians, Florentinians, Saona, Genova, Genovese, Santa Liga ? federatore ?, your government (La S.^{ria}

³If the king of France will not release my son, it is necessary that du du Tertre think and imagine a way how my son can come to Cherbourg in Normandy.

⁴Italian for MSA = Municipal Security Agency

V̄ra = La Signoria Vuestra), Liga, Johannes, Saona
 soldiers, cavallery, footsoldiers, dollars, ships, galleons, King Alfonso VI of Aragon, Count Iacobo Picinino, Italy, Germany, Duke of Savoy, council of cardinals, France, D. Phillip of Savoy, that, because, not.

The total comes to 165 signs. hide Ferrante was an illegitimate son of Alphonse the Generous (der Grossmütige). Johannes? Liga federatore?

Some of the encrypting symbols resemble letters or digits, but most are phantasy signs. It takes a careful and patient hand, experienced in this kind of cryptTeX, to put down long messages with such contrived symbols. The difficulty in reading them may have suggested a false sense of security, but in fact, a legitimate user faced the same problem, at least initially. Most of the codebooks in Tranchedini's compilation are dated, from 1450 to 1496. The longest one has 283 symbols. The various codebooks all follow the same structure but use varying symbols, with plenty of room for the designer's fancy.

These records form an impressive display of the power of Northern Italian cryptography in the early Renaissance.

We now jump another hundred years ahead. Henry III. (?), a calvinist King of France, had as powerful enemies the family of Guise. They formed the Catholic *Holy League* in 1576, with the goal of putting one of their bloodline on the throne. Henry III. had the two leading brothers murdered in 1588; the narrow passage in the Blois castle on the Loire, where Henri de Guise was assassinated at 8 am on 23 December 1588, is now a favorite tourist sight. A third brother, Charles de Lorraine, Duke of Mayenne, took over leadership of the *League*. After the murder of Henry III. by a Catholic priest in 1589, the Protestant King Henri IV. quickly gained the upper hand militarily. The Duke of Mayenne's ambition was still to become King himself. When it became apparent that the Ligue's military power was not sufficient, he schemed to involve II (1527-1598), the King of Spain and Portugal, in his plans. Besides invoking their common religion—then as now a major excuse for killing the others—he offered a substantial prize: large parts of France, namely the Roussillon in the South, and the Picardie bordering on the Spanish Netherlands. Their possession had been a Spanish goal for some time.

Commander Juan Moreo was delegated in 1589 to the Spanish army ready to aide the Ligue. For his communication with the Spanish court, he had a codebook of 423 terms, plus dummies and signs for doubling letters and for numbers. Figure D.2 shows its initial part in modern type. The original seems to have been lost, but the Spanish archives at Simancas contain another codebook with striking similarities. This was issued for use with John Baptist of Taxis around 1590. Its beginning is shown in Figure D.3; in the original, this is just one column (out of seven in total) which we have split into two for the reproduction.

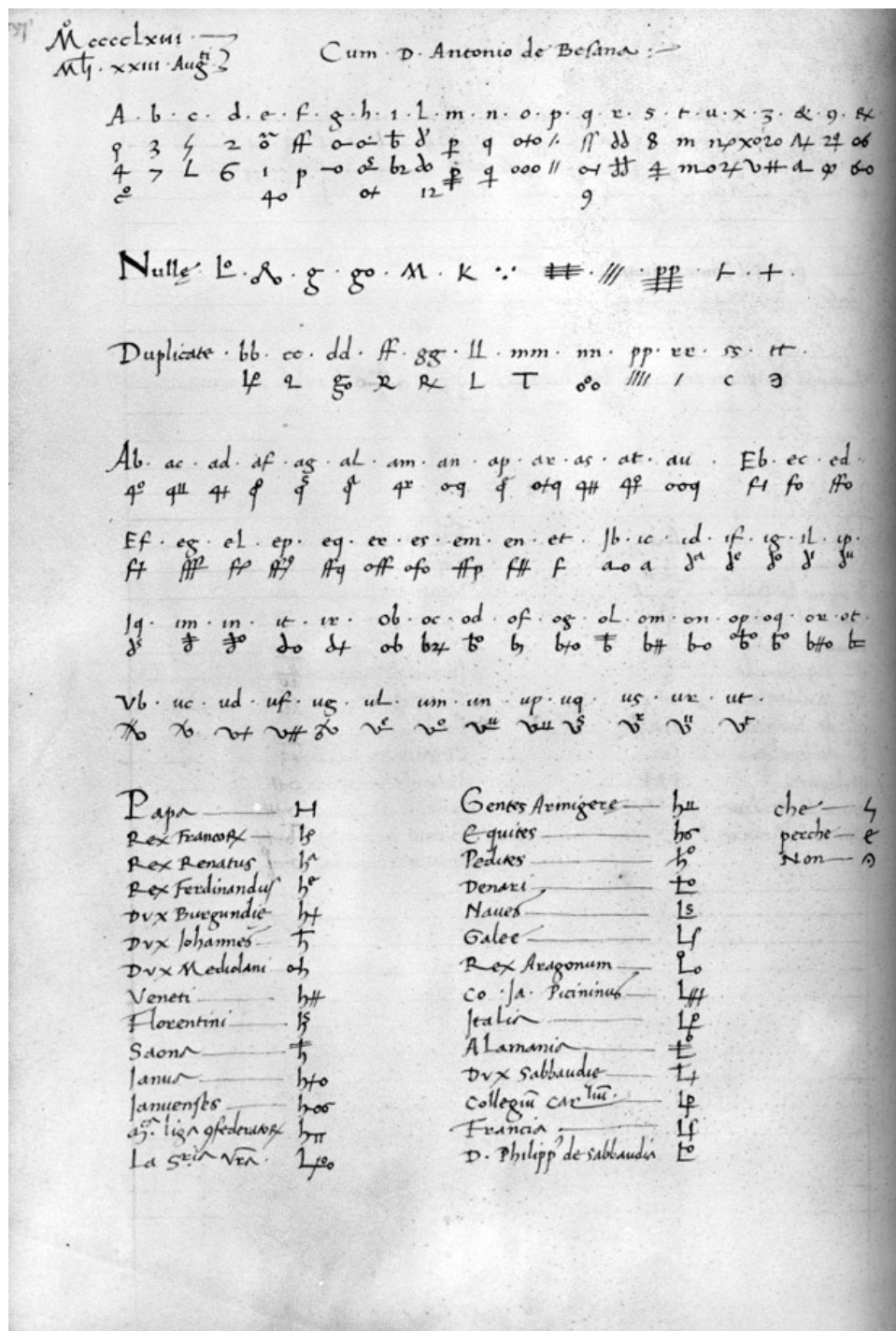


Figure D.1: One of Tranchedini's nomenclators.

The cleartext words are the same in both codebooks, but the encryptions are different. For Moreo's book, they are the underlined numbers from 0 on (and going to 99, not shown here), while in Taxis' cipher they are three-letter syllables "consonant + vowel + m". The consonants are used in descending order: s, r, qu, p, n, m, l, j, h, g, f, d (and continuing to b on another page). For each consonant (except s) the five vowels are used, for example towards the end: fum, fom, fim, fem, fam. In other parts, Moreo's cipher has such two- and three-letter syllables, and Taxis' has underlined numerals.

We see a well-organized cipher factory at work. They have a list of clear-text words, which may be copied for the different ciphers, and standardized (but not identical) types of cipher equivalents, mainly certain two- and three-letter syllables and over/underlined or dotted numerals. These are inserted in several sections, with an alphabetical or numerical order (or reversed order) in each section. The use of standard signs is progress over the contrived symbols in Tranchadini's codebooks.

Both codebooks contain provisions for dummies, double letters and numbers. In Taxis' cipher, this reads in the bottom lines of Figure D.3: *Las Nullas tendran una raya enzima exemplo $\overline{19}$, y las dupplicis un $\overset{0}{0}$, como esto $\overset{0}{46} \overset{0}{25}$ y todos los que fueron num.^{os} tendran una cruz encima $\overset{+}{10} \overset{+}{20}$.*⁵

Henri IV, King of France and Philipp's adversary, had in his services the lawyer François Viète (1540-1603), who also happened to be one of the leading mathematicians of his times. He introduced the use of letters for known quantities in algebra, and expressed by Viète's *formula* the coefficients of a polynomial in terms of its roots; we use this for the elliptic curve addition rules in ???. Viète deciphered Moreo's codebook; this was a major cryptanalytic achievement. After such a success, one usually keeps mum about it, expecting the enemy to continue using it and so to provide more secret messages which can then be deciphered. But here something unusual happened: Viète published a lengthy letter, sent by Moreo from Anvers (Amveres, Antwerp) to Madrid and which he had deciphered, in a booklet pages ?. Figure D.4 shows its title page:

Decipherment of a letter written by Captain Moreo to his chief-in-command, the King of Spain, on 28 October 1589

To the King our Lord
in the hands of Don Martin de Idiaquez, his secretary of state.
Sir. From Rouen I sent a letter to Y. M. with the message whose duplicate goes with the present one. I mentioned that, after returning

⁵The dummies will have an overlining bar, for example $\overline{19}$, and double letters a 0, as $\overset{0}{46}$ and $\overset{0}{25}$, and those that signify numbers have a cross above them: $\overset{+}{10}$, $\overset{+}{20}$.

Cifra particular [1589-1597].			
A			
Aca	<u>0</u>	Bruselas	<u>35</u>
adelante	<u>1</u>	bueno	<u>36</u>
advertimiento	<u>2</u>		
Africa	<u>3</u>	C	
agora	<u>4</u>	camino	<u>37</u>
Aleman	<u>5</u>	campo	<u>38</u>
alla	<u>6</u>	capitan	<u>39</u>
Alteracion	<u>7</u>	capitulo	<u>40</u>
amigo	<u>8</u>	cardenal	<u>41</u>
amistad	<u>9</u>	cargo	<u>42</u>
andamiento	<u>10</u>	carta	<u>43</u>
año	<u>11</u>	caso	<u>44</u>
antes	<u>12</u>	Castellano	<u>45</u>
Amveres	<u>13</u>	castigo	<u>46</u>
apparencia	<u>14</u>	castillo	<u>47</u>
aqui	<u>15</u>	catolico	<u>48</u>
arcabuz	<u>16</u>	cavallo	<u>49</u>
Argel	<u>17</u>	causa	<u>50</u>
armada	<u>18</u>	cautela	<u>51</u>
armas	<u>19</u>	christiandad	<u>52</u>
artilleria	<u>20</u>	cifra	<u>53</u>
assi	<u>21</u>	ciudad	<u>54</u>
assistencia	<u>22</u>	color	<u>55</u>
authoridad	<u>23</u>	comissario	<u>56</u>
aviso	<u>24</u>	comission	<u>57</u>
aún	<u>25</u>	comodidad	<u>58</u>
aunque	<u>26</u>	como	<u>59</u>
		comunicacion	<u>60</u>
B		compañero	<u>61</u>
bastimento	<u>27</u>	compania	<u>62</u>
batalla	<u>28</u>	concierto	<u>63</u>
bateria	<u>29</u>	confederacion	<u>64</u>
beneficio	<u>30</u>	confederado	<u>65</u>
Berberia	<u>31</u>	conclusion	<u>66</u>
Bohemia	<u>32</u>	concordia	<u>67</u>
bondad	<u>33</u>	concurso	<u>68</u>
Brabante	<u>34</u>	condicion	<u>69</u>
		confianza	<u>70</u>
		conformidad	<u>71</u>

Figure D.2: The initial part of the Spanish codebook for Juan Moreo, from Devos (1950), page 329.

A		B	
Aca	som	Bastimento	mem
a dilante	sim	Batalla	Mam
aductivo	tem	Bateria	lem
affica	sam	beneficio	lom
agona	rum	benencia	sim
aleman	rom	bohemia	lem
alla	rim	Bondad	lam
alteracion	rem	Bravante	zum
amigo	ram	Bruselas	zam
amistad	quum	Bueno	sim
andamento	quem	C	
ano	quim	camino	sem
antes	quem	campo	sam
anueles	quam	capitan	hum
aparentia	pum	capitulo	hom
aqui	pom	cardenal	him
arcabuz	pin	caros	hem
argel	pem	canta	ham
armada	pam	casso	gum
armos	num	castellon	gom
artilleria	nom	castijo	gem
assy	nim	castillo	gem
assistencia	nem	catolicos	gam
autoridad	nam	cauallo	fum
caisso	mum	causa	fom
aun	nom	cautela	fim
cuoque	mim	chistandad	fem
		cifra	fam
		ciudad	lum
		color	dom
		comissario	dim
		comission	dem

Las Nullas tendran una raya en cima Exemplo 19,

y Las Duplicas un 0, como esto 2625 y todos los que fueren num. Tendran unacruz en una 10 20

Figure D.3: The initial part of the original codebook for Taxis, from the Spanish archives at Simancas.

to where the Duke of Mayenne was, I found him in open and dangerous territory. This obliged me to drop everything and to come here for help, and to give the Duke of Parma an account of the state of affairs. . . .

Throughout the Spanish text, Viète gives his marginal precis in French, as on the title page:

Moreo has written to the Duke of Parma to induce him to relieve, with his forces from Flanders, the Duke of Mayenne.

We can only speculate about the reason for going public, but it had the effect of rallying the French nobility around Henri IV, enraged about the Duke's proposed betrayal of French territories. He had been so convinced of the security of his nomenclator that he complained to Pope Sixtus V. popes: Gregory XIII 1572—May 1585, Sixtus V 1585—1590, Urban VII 1590, Gregory XIV 1590—1591 that Viète's successful cryptanalysis could only have been possible through black magic. His complaint made him the laughing-stock of all those in the know. Viète's biography mocks the Spanish *qui ad odium & invidiam nihil non comminiscuntur, magicis artibus, nam aliter fieri non potuisse, à Rege id factum, passim & Romæ præcipuè non sine risu & indignatione rectiùs sentientium per emissarios suos publicabant*.⁶

And what happened to King and Duke? Henri IV. eventually became Catholic: *Paris vaut bien une messe*.⁷ The Duke of Mayenne gave up his fight for the crown and Henry treated him generously, praising him for *not having permitted, in good or bad luck, the dismembering of France*.

Viète was a successful cryptanalyst, but his vanity was counter-productive. He bragged in front of Giovanni Mocenigo, the Venetian ambassador in France, about his abilities in code-breaking. The wily diplomat teased him into admitting that he also solved Venetian codes, and even into exhibiting an example. When the Council of Ten, back home in Venice, learnt about this, they immediately changed their codes.

When designing a codebook, one starts with an alphabetical list of the words to be encoded. The number of words may range from a few dozen in the early Renaissance to 10 000 and more in the 20th century. ref for 10 000 words Furthermore, one fixes the type of encryption to be used; underlined numbers and three-letter syllables in Figures D.2 and D.3, respectively, and 5-digit numbers plus 3-letter codes in the German naval codebook from 1913 in Figure F.1. These encodings also have a natural order.

⁶who never stop from making up any slander and bad-mouthing, announced everywhere and to Rome in particular through their emissaries that the King's achievement had been done with magic arts, because it was not possible otherwise, to the amusement and indignation of those in the know.

⁷Paris is well worth a mass.

Now in a *one-part codebook* one simply associates the codes in the words in natural order. This is the case in the three examples mentioned. In Figure D.3, the “natural order” of the codes is s, r, q, p, n, m, l, j, h, g, f, d, that is, the reverse of the alphabetic order. Then the syllables are completed by appending -um, -om, -im, -em, and -am.

This construction provides a great help to the cryptanalyst. In Figure D.2, if catolico=48 and cristiandad=52 are already known, then the code for cavallo⁸ must be 49, 50 or 51. On the other hand, if he encounters the unknown ciphertext 50, then its cleartext is guaranteed to lie between católico and cristiandad in any (contemporary) dictionary. The advantage for the legitimate user is that a single list permits an “alphabetic search” both for encryption and decryption.

In a *two-part codebook*, the codes are assigned to the codewords in random order. This provides much higher security, because now encryptions cannot be inferred from neighboring words, but has the disadvantage of requiring two separate lists for easy encryption and decryption.

An intermediate amount of randomness is used in codebooks that consist of pages of alphabetically ordered words, say numbered from 0 to 99, but where the pages themselves are randomly shuffled. We might call them one-and-a-half-part codebooks. The German diplomatic codebook 13040, in which the Zimmermann telegram (Chapter F) was sent in 1917, was of this type, while the other codebook used in that affair, called 0075, was of the two-part variety.

D.2. Commercial codebooks

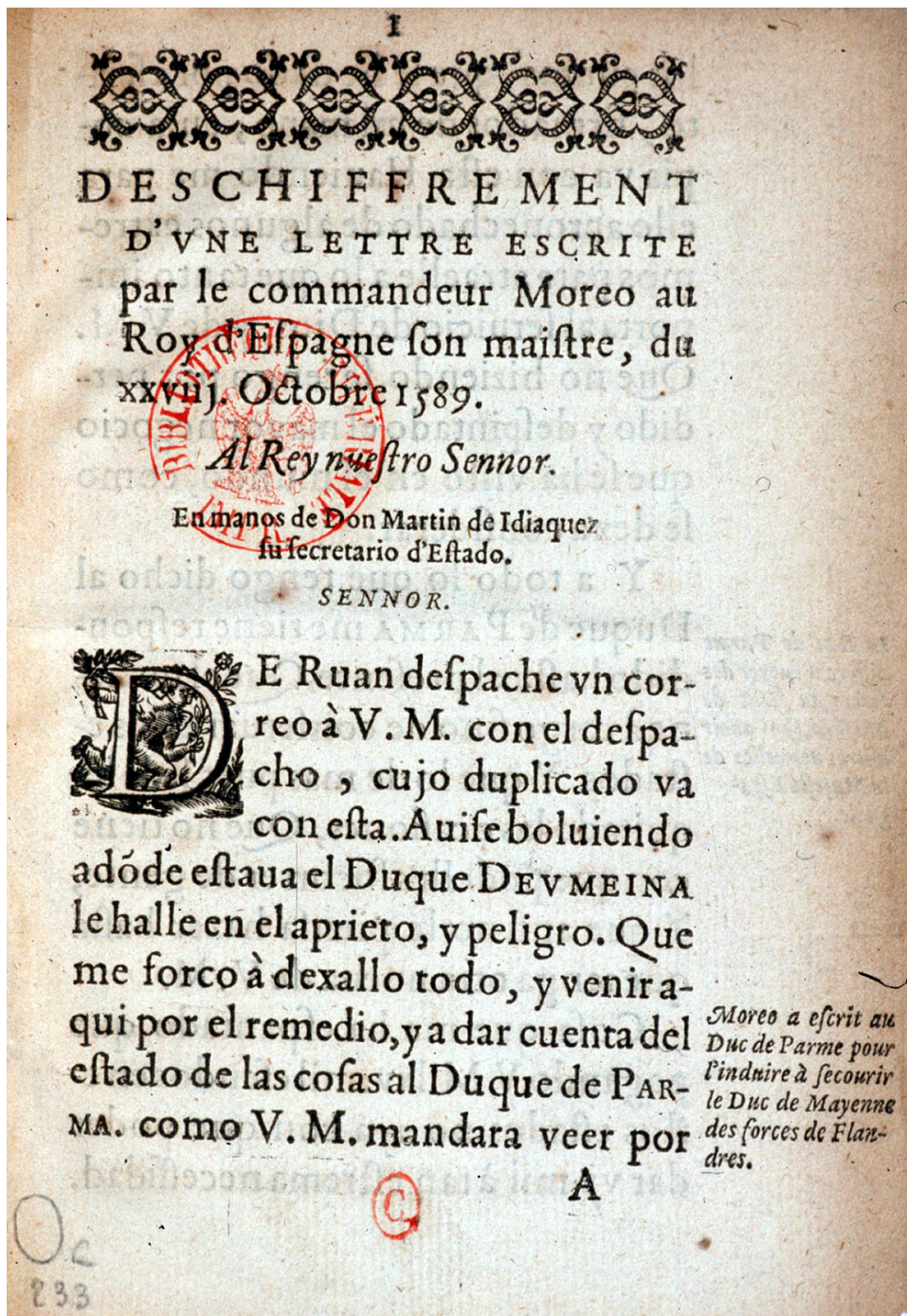
The introduction of the telegraph and its rate structure made it desirable to shorten message. Commercial codebooks catered to this need. Words and whole phrases are replaced by short codewords, regulated by the International Telecommunications Union in 1932 to be at most five letters long. (For the younger reader: Once upon a time there was neither email nor SMS, and people had to rely on primitive forerunners called *telegram* and *telex*.)

The first telegraphic code book was published in 1845, just one year after the start of commercial telegraphic operations.

These codes safeguard against accidental reading, but provide no real security. As an example, Lieber’s 1896 *Standard Telegraphic Code* presents on its 800 pages about 75 000 entries. Each entry associates both a 5-digit number and a (phantasy) word of at most ten letters, beginning with a letter from A to F, to a phrase. The words and the phrases are sorted alphabetically, the latter by keywords. In this code, the message

(D.1) 27556 03529 09715 00029 24695 04305 22454 28909

⁸horse

Figure D.4: Viète's decipherment of a Spanish missive.⁹

of eight words is synonymous with

Babishly, Acerquen, Aggiunsero, Aalkasten, Atortolar, Acontiadae,
Arrozzendo, Barbarizo.

Both encode the less than cheerful (fictitious) message of 70 words:

A great panic prevails here, caused by the news [that] | there has
been a very heavy bank failure here to-day which will seriously
affect our market. | Present acting officers of this corporation |
have absconded; [we] are on their track, utmost secrecy necessary.
| Money market is in a panic. | Bonds are depressed on rumors
that they will default on the interest. | [We] have suffered heavy
losses. | Send immediately for best physician.

The words in brackets have been added, and the vertical strokes separate phrases.

These codebooks serve no cryptographic purpose, being publicly available. A certain level of secrecy can be gained through superencipherment, by choosing a secret key and using it in a (carryless) key-addition scheme. This was proposed (in a slightly different context) by the German cipher bureau during the First World War page?. With their key 718, the message (D.1) would be superenciphered as

98327 80606 17423 71890 01772 12013 93225 05086.

D.3*. Unicity distance for codebooks

So we have a codebook $\sigma: \mathbb{X} \rightarrow \mathbb{Y}$, with $s = \#\mathbb{X}$ codewords. The “words” in \mathbb{X} form the vocabulary of the messages and may be letters, syllables, words, personal names, etc. An attacker will have a reasonable idea of the relevant words, and be able to construct a bigger vocabulary \mathbb{X}' so that almost all words of \mathbb{X} are in \mathbb{X}' . The two extremes are when nothing is known about \mathbb{X} , so that \mathbb{X}' consists of all conceivable words, and when $\mathbb{X}' = \mathbb{X}$, which might occur when a codebook with the same vocabulary has already been broken; see Section F.1. To quantify this scenario, we let \mathbb{X}' have at most cs elements, among them at least $(1 - \varepsilon)s$ elements of \mathbb{X} , for some $c \geq 1$ and $\varepsilon \geq 0$. In the two extreme cases, we would have $\varepsilon = 0$, and $c = (\text{number of all words})/s$ or $c = 1$, respectively. When the number of all conceivable words is L , we have

$$(D.2) \quad m = \binom{cs}{(1 - \varepsilon)s} \binom{L}{\varepsilon s}$$

many choices for \mathbb{X} , given s, L, ε, c and \mathbb{X}' . The first factor stands for the $(1 - \varepsilon)s$ elements of \mathbb{X} in \mathbb{X}' , and the second factor for the other elements of \mathbb{X} . When

$\varepsilon = 0$ and $c \geq 3.6$, then (D.2) simplifies to

$$(D.3) \quad m \approx ((c-1)e^{1+\frac{1}{c-1}})^s \leq (4(c-1))^s.$$

The set \mathbb{Y} of encodings (or a close superset of it) can be guessed from the ciphertext.

Now if the codebook is ordered (“one-part”), then the only secret part of \mathbb{Y} is its offset, the place that encodes the first codeword in \mathbb{X} . There are ℓ choices for this, and so there are $m \cdot s$ many keys.

If the codebook is random (“two-part”), then there are $s!$ possibilities for σ , given \mathbb{X} and \mathbb{Y} , and thus $m \cdot s!$ many keys. one-part def’d?

In a mixed codebook, the ordered encodings \mathbb{Y} are split into b blocks of length s/b each, these blocks are shuffled randomly and then assigned to the codewords. Thus the order within each block is conserved, but not globally. The codebook in Figure which code book is of this nature: The number of keys then is $m \cdot b!$.

Simplifying somewhat, the information content $I(\mathbb{K})$ of a key is $\log_2(\#\mathbb{K})$ for the random keys that we consider, and thus

$$I(\mathbb{K}) \approx \begin{cases} s \cdot \log c & \text{ordered,} \\ s \cdot \log(sc) & \text{random,} \\ s \cdot \log c + b \cdot \log b & b \text{ blocks.} \end{cases}$$

The alphabet size is s , and for the entropy of a single word we have the following measurements:

We can now calculate the unicity distance for some codes:

	Moreo	Layer	Signalbuch	13040
s				
c				
b				
$I(\mathbb{K})$				
$H(p)$				

Chapter E

Transposition ciphers



pieces of text—say, a letter or a word—are changed by a substitution into a different piece. This creates “confusion”. A completely different effect is obtained by transpositions, which move the pieces around in a text without changing them individually; this creates “diffusion”. Suitably combined and generalized, these two operations form the basis of almost any strong cryptosystem. We discuss three types of transpositions in this chapter: the Greek skytale, columnar transpositions and grilles. Get image of 9th c columnar transposition? Quote Friedman/Mendelsohn/Beiler on Verne. Ex of columnar transposition in Section E.3: Wilkins quote in 5 columns? Who is Lysandros Roman partner? Quote book + transl. Skytale: etymology, quote Birds and Gellius precisely

E.1. The skytale tale

Our civilization owes much to the classical culture of the Greeks. Among them, the Spartans contributed little to improving human existence; their forte was warfare. It is not surprising that one of their few novelties was a military cryptosystem, based on transposition and called a *σκυτάλη* (*skytale*, rhymes with *Italy*). The historian Plutarch (c. 45–c. 125) cite Plutarch describes in his *Parallel Lives* the unscrupulous Spartan general Lysandros (died 395 BC) whose motto was: *You cheat children with dice, and men with oaths*. When Lysandros’ brutal and corrupt reign over the Greek cities that he had subdued became too much for the rulers of Sparta, they sent him an encrypted message ordering him back to Sparta. Plutarch writes:

When the ephores, Sparta’s rulers, send out a military expedition, they have two round wooden sticks made, exactly equal in length and thickness and whose ends fit together. One of them they keep, the other they give to the expedition leader. They call this wooden piece a skytale. If they have a secret important message, they prepare a long strip of papyrus or leather like a belt and wind it around their skytale. They leave no spaces, but the surface is covered everywhere with the strip. When this is done, they write their mes-

sage on the strip wound around the skytale. After writing, they remove the strip and send it without the piece of wood to the expedition leader. When he receives it, he cannot read anything, because the letters are not connected but torn apart. So he takes his own skytale and winds the strip around it. If this is done properly as before, the eye can detect the connection of the letters.

Back home in Sparta, Lysandros was able to appease the rulers, went on a pilgrimage, later became a general again and fell in battle some years later.

skytale! This is a very weak form of cryptography, and a few trials with the “strip of papyrus” give away the secret.

In fact, the story is weak as well. Besides Plutarch, several authors including ?Gellius from the third century BC or later mention the skytale’s use in the fifth century or before. But in the older writings, up to the fifth century BC, the skytale usually plays the role of a “message stick”, around which a (plaintext) message is wound for convenient long-distance transportation, but no cryptographic purpose is ever mentioned.

Thus it is quite possible that the cryptographic use of the skytale is a figment of the imagination of later ancient writers, which has been perpetuated in many cryptographic writings to this day. However, there is no final proof one way or the other.

The famous cryptosystems of Caesar and Augustus (Section A.3) are in a similar state of limbo. The later writers tell us profusely about them, but we have no contemporary documents exhibiting their actual use.

skytale etymology. Skytale in 1341?? Journal des Scavans 20 July 1676. Aristophane’s dates, check Kuhoff, insert skytale pix from Porta

E.2. Columnar transpositions

These transpositions were briefly described in Example A.2 (ii): one writes message in rows which are then read columnwise. Such ciphers were used in the Layer conspiracy (??, see page ??). In fact, there exist medieval examples of text written in columns (and read rowwise), already from the 9th century.

The example given of a 3×2 columnar transposition is easy to generalize. For a closed formula for the general $r \times c$ transposition, we put the numbers $0, \dots, \ell - 1$ with $\ell = rc$ row by row in an $r \times c$ array:

$$\begin{array}{ccccccccc} 0 & 1 & 2 & \dots & c-1 & 0,0 & 0,1 & 0,2 & \dots & 0,c-1 \\ c & c+1 & c+2 & \dots & 2c-1 & 1,0 & 1,1 & 1,2 & \dots & 1,c-1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ (r-1)c & (r-1)c+1 & (r-1)c+2 & \dots & rc-1 & r-1,0 & r-1,1 & r-1,2 & \dots & r-1,c-1 \end{array} =$$

Then the row index u and the column index v on the right corresponding to i on the left are given by

$$u = \lfloor i/c \rfloor, v = i - cu.$$

For example, the third entry in the second row corresponds to $i = c + 2$ and to

$$(u, v) = (1, 2) = (\lfloor (c + 2)/c \rfloor, c + 2 - c \cdot 1),$$

provided that $c \geq 3$.

Similarly, we put them column by column into the same array:

$$\begin{array}{ccccccccc} 0 & r & 2r & \dots & (c-1)r & 0,0 & 0,1 & 0,2 & \dots & 0,c-1 \\ 1 & r+1 & 2r+1 & \dots & (c-1)r+1 & 1,0 & 1,1 & 1,2 & \dots & 1,c-1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ r-1 & 2r-1 & 3r-1 & \dots & rc-1 & r-1,0 & r-1,1 & r-1,2 & \dots & r-1,c-1 \end{array} =$$

Now we have for the row and column indices u' and v' corresponding to j :

$$v' = \lfloor j/r \rfloor, u' = j - rv',$$

for $j = 0, 1, \dots, cr - 1$.

Thus the transposition $i \mapsto j$ is given by

$$j = u' + rv' = \lfloor i/c \rfloor + r(i - c\lfloor i/c \rfloor) = ri - (rc - 1)\lfloor i/c \rfloor.$$

More generally, the letters of the message may be arranged in some geometrical pattern which has to be read according to previously fixed rules (the key), as in Figure E.1. Can you discover the message? Wilkins describes several others, and concludes: *All these kinds may be varied unto divers other more intricate transpositions, according as a man's fancy or occasion shall lead him.*

W m r p i t a h h s c t e i n p k e
h a t h f o n o i h k f t o e n i l
a n o e r r o c g t t t h m n v r l
e a u o m h t e i n l e n e t t e s

Figure E.1: A transposition cipher by Wilkins.

Just before its final defeat in the Second World War, the German military used a columnar transposition system they called *Rasterschlüssel 44*, from August 1944 to the end in May 1945. It was hard to use and error-prone, but also much more difficult to break than the Enigma by the cryptanalysts in the US and at Bletchley Park, who called it “practically unbreakable” and said “it defeated our cryptographers”. Columnar transpositions have appeared in literary works. In Jules Verne’s classic *Voyage to the Centre of the Earth*, the hero,



Figure E.2: The Runic columnar transposition in Verne's *Voyage to the Centre of the Earth*.

a German professor named Lidenbrock, has discovered by chance a piece of parchment with Runic writing on it (Figure E.2). He first transcribes it into our letters

m.rnlls	esreuel	seecJde
sgtssmf	unteief	niedrke
kt,samn	atrateS	Saodrrn
emtnaeI	nuaect	rrilSa
Atvaar	.nscrc	ieaabs
ccdrmi	eeutul	frantu
dt,iac	oseibo	KediiI

and then begins his guessed plaintext attack, assuming the presumed author's name Arne Saknussem to appear in the cryptogram. Lo and behold, we see it indeed in the first letters, starting with the S in the third line of the last column, and then reading against the usual direction. Particularly convenient is Lidenbrock's capital S, while Runic writing does not distinguish between small and capital letters. With this much help from the author (Verne, not Saknussem), the brilliant Lidenbrock cannot help but recover the plaintext:

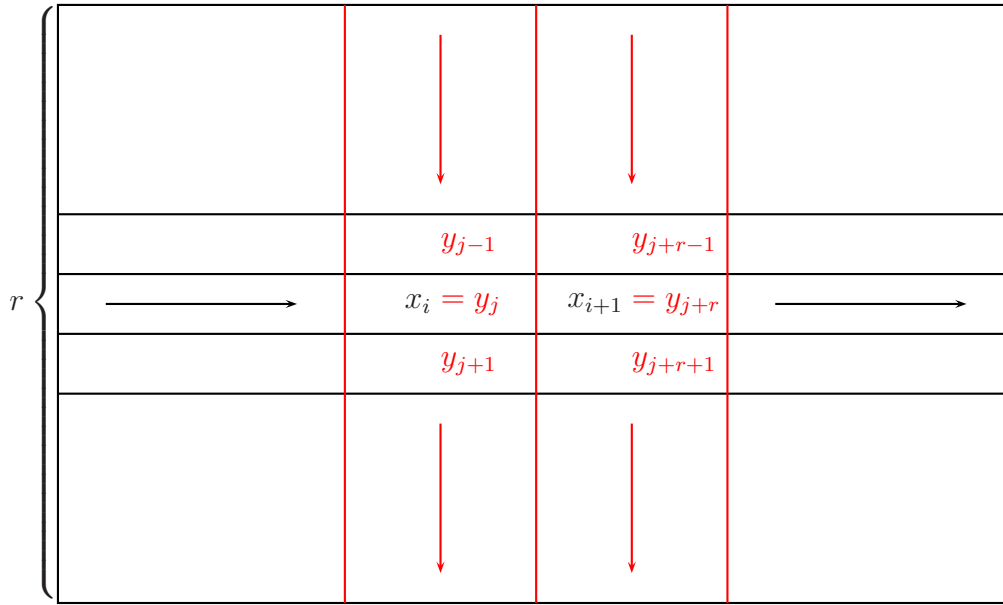
In Sneffels Yoculis craterem kem delibat umbra Scartaris Julii intra calendas descende, audas viator, et terrestre centrum attinges. Kod feci. Arne Saknussem.¹

¹Audacious traveller, descend into the crater of Sneffels Yokul which the shadow of Scartaris caresses during the first days of July, and you will reach the centre of the earth. Which I did. Arne Saknussem.

These instructions by Saknussem send Lidenbrock, his young nephew and a tough Icelandic guide off to a fantastic trip towards the centre of the earth—one of the voyages announced by *Verne Holidays* but still not available for booking.

E.3. Breaking a columnar transposition

When the frequency distribution of some ciphertext y is close to that of English, one may suspect that it was produced from some English plaintext x by a transposition. If it comes indeed from a $r \times c$ columnar transposition, this is easy to find out. Namely, a bigram (= two adjacent letters) $x_i x_{i+1}$ in x is mapped to ciphertext letters y_j and y_{j+r} for some unknown j .



The first step is to prepare a list of bigram frequencies $f_{b,\text{Eng}}$ in percent (including contacts across words) for all bigrams b . Thus $f_{th,\text{Eng}} = z$ means that the bigram $b = (t, h)$ occurs $\frac{z}{100} \cdot 335006$ many times in Harry Potter, since the text consists of 335007 letters and one fewer bigram. ?? shows this list based on *Harry Potter*; see Section A.4 for details. The next step is to guess the number $r = 2, 3, \dots$ of rows, and for each bigram $b = (b_1, b_2) \in \mathbb{A}^2$, where \mathbb{A} is the alphabet, to note how often it occurs with distance r :

$$f_{b,y}^* = \# \{j : y_j = b_1 \text{ and } y_{j+r} = b_2\}.$$

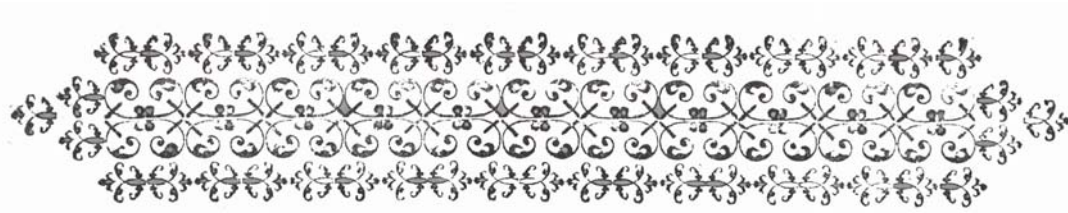
This is normalized into percent as $f_{b,y} = 100 f_{b,y}^* / (\ell - 1)$, when y has ℓ letters in total. Finally, one computes the Euclidean distance

$$d_{\text{bigram}}(y, \text{Eng}) = \sum_{b \in \mathbb{A}^2} (f_{b,\text{Eng}} - f_{b,y})^2$$

of the two bigram frequencies. This distance will be small at the value of r which was the actual number of rows, and also at its integer multiples. Some minor disturbances are created by bigrams that are split onto two (consecutive) rows in the plaintext, and by possible divisions of the plaintext into blocks that were encrypted separately. But these vagaries do not seriously affect the method.

Generally speaking, the combination of substitution and transposition can increase security drastically. However, a columnar substitution plus a simple transposition can still be solved by the method above. Namely, the nine most frequent letters *etaonirsh* in English account for $\frac{1}{3}$ of the top 100 bigrams, and for 40% in all. After guessing the value substituted for *e*, one uses the bigram frequencies among the nine most frequent ciphertext letters to guess the substitutions for some of the letters. Of course, the number of possibilities for c and r is usually quite small, say at most 20 or 100 for each of them. This corresponds to a key space of 400 or 10000 elements, which is easy to search exhaustively by any computer at hand.

This cryptanalytic method can also be applied to grilles, with appropriate modifications, in order to determine (vertically or horizontally) adjacent holes. And trigrams can be used for holes in one row or one column, separated by a single space.



Chapter F

The Zimmermann telegram

Chapter Init missingNo single event decided the outcome of the World War I. But the entry of the USA into the war—after long hesitation—certainly played a major role in the success of the *Entente*, originally led by France and Great Britain. And the (in)famous telegram discussed in this chapter was important in changing the isolationist attitude in large parts of the US population and thus easing President Wilson’s decision to enter the fray. Its solution has been called “the greatest intelligence coup of all time”. The telegram is an instructive display of German failures and British successes, both in cryptography and in diplomacy.

F.1. Capturing the *Magdeburg*’s codebooks

We start with a tale from the early stages of the British cryptographic bureau, concerning a marvellous gift they received and which got them started on their breaks into the German cipher systems. The story begins less than a month after the German military had embarked on the adventure that would lead to their eventual downfall, by attacking Belgium and France. In the middle of the night of 26 August 1914, the German light cruiser *Magdeburg* was sailing in a Baltic Sea flotilla intending to wreak havoc on the Russian ships in the Gulf of Finland. She followed the leading ship, the light cruiser *Augsburg*, who

¹The cleartext words are: insult, to scold; disgraceful, disgrace; umbrella, to protect (against); umbrella (folding) anchor; battle; to offer a battle; to accept a battle; to evade a battle; battle begins; in the battle; after the battle.

¹The words mean: (to) blame; dishonorable; umbrella, to protect, umbrella anchor; battle; to offer battle; to accept battle; to avoid battle; battle begins; during the battle; after the battle.

661 60	Q P F	Schimpf =en (über)
61	Q P G	schimpflich =feit
62	Q P H	Schirm =en (gegen)
63	Q P I	Schirmanfer
64	Q P J	Schlacht
65	Q P K	Schlacht anbieten
66	Q P L	Schlacht annehmen
67	Q P M	einer Schlacht ausweichen
68	Q P N	Schlacht beginnt
69	Q P O	in der Schlacht
661 70	Q P Ö	nach der Schlacht

Figure F.1: Eleven codewords from the *Signalbuch der Kaiserlichen Marine*¹.

tried to sneak south around a suspected Russian mine field. But she lost visual contact in a dense fog, and just as she was turning around from a southerly to an easterly course, she ran aground in shallow waters off the Estonian island of Odensholm, at 12.37 am. After desperate attempts to get her off, also with the help of the torpedo boat V-26, her captain Richard Habenicht ordered her to be blown up, around 9.00 am. By mistake, the fuses were lit too early, and the men had less than five minutes to abandon ship.

The *Magdeburg* had four codebooks on board. One was burned in time. One was jettisoned overboard. Radioman Second Class Neuhaus jumped overboard with the third one and was not seen again. And the fourth—was forgotten.

By then, Russian ships had arrived. Lieutenant Galibin of the torpedo boat *Lejtenant Burakov* boarded the *Magdeburg* and found the codebook in captain Habenicht's cabin. Later, Russian divers also recovered the two other codebooks from the clear waters with a depth of less than ten meters.

The Russian military command immediately recognized the importance of their bounty, and offered it to England, the major naval power of the *Entente*. After a trip on board the H.M.S. *Theseus* from Polyarny (then Alexandrovsk) to Hull in England, the Russian count Constantine Benckendorff handed the *Signalbuch der Kaiserlichen Marine*² to Winston Churchill, first Lord of the Ad-

²codebook of the (German) Imperial Navy

miralty, on 13 October 1914. The British cryptographers then put this gift to good use.

The German military command never recognized the importance of their loss. The commanding admiral downplayed the possibility of the code having been recovered. An investigation by Prinz Heinrich von Preussen, the German emperor's younger brother, came to the opposite conclusion, but was ignored. The very Lieutenant Galibin, retriever of the captain's codebook, was captured in August 1915 and told about his feat. He was ignored. On several occasions, British naval forces happened to be right there where a German fleet was to steam through. Such circumstantial evidence was ignored as well.

British naval cryptography had been nonexistent at the war's outbreak. But an agency was immediately formed. The main player was James Alfred Ewing (1855–1935), an engineer by profession, among whose achievements are the design of seismic instruments, the discovery of hysteresis in magnetic materials, and studies of the structure of metals. After teaching in Tokyo, Dundee and Cambridge UK, he was Director General of Naval Education at the Royal Naval College in Dartmouth from 1902 on. He came to cryptography by accident, when on 4 August 1914, just after the start of World War I, his friend Admiral Sir Henry Oliver showed him some intercepted German cipher telegrams. Ewing said he would look at them, and the Admiral interpreted this quite liberally. Soon after, intercepted cipher messages were pouring into Ewing's office, often over two thousand per day. He acquired a large room numbered "40" in the Admiralty building, and even after a move into new quarters his cryptographic office was called "Room 40"—a name that does not give away much. After some startup difficulties, they broke routinely German military and diplomatic ciphers.

The *Signalbuch* that arrived at Room 40 contained between its heavy lead covers hundreds of pages with three-column entries as shown in Figure F.1:

Thus *Schlacht* (battle) would be encoded as QPJ (usually) or 66164 (less often). But this did not break the intercepts except some items of lesser importance like weather reports.

The clue arrived in the form of the *Handelsschiffsverkehrsbuch*³ seized from a commercial vessel in Australian waters. This also contained a (different) list of codewords, and in addition a superencipherment by which each individual letter of a codeword was changed into another letter, via a simple substitution. Charles Rotter in Room 40 had the flash of insight that the same might be applied to the *Signalbuch* codewords. But the usual frequency cryptanalysis is hard on codewords, for lack of redundancy. But then the Germans helped out by sending a sequence of messages whose consecutive serial numbers they encoded. That was enough to reveal the superencipherment. Alastair Denniston, a scholar of German in Room 40, commented coolly: "Their folly was greater

³merchant navy codebook

than our stupidity.”

From then on, Room 40 read most of the German naval signals. However, a participant like Lieutenant Filson Young, on board the battle cruiser *Lion* from November 1914 to May 1915, bitterly complained about the Admiralty’s inefficiency in using this valuable material, only a small portion of which actually reached the Grand Fleet.

F.2. The telegram

The most spectacular coup of Room 40 gave US President Thomas Woodrow Wilson the popular and political majority for entry into the war on the side of the Entente, thus clenching their victory. Hoping to break the stalemate of the bloody trench battles in Northern France and Belgium, the German military wanted in January 1917 to force Great Britain into submission by cutting her lifelines to North America by all-out submarine attacks. A major concern was that this might lead the USA into the war, while an isolationist attitude had hitherto kept them out of it.

The Germans tried to create a diversion by dragging the Mexicans into the fray. Arthur Zimmermann, Secretary of State for Foreign Affairs since 22 November 1916, sent a top secret message to the German minister Heinrich J. F. von von Eckardt in Mexico, via the German ambassador Graf Johann Heinrich Andreas Hermann Albrecht von Bernstorff in Washington. He offered, if war with the USA broke out, money to the Mexican President Venustiano Carranza and consent for Mexico to regain the states of Texas, New Mexico, and Arizona, which had been conquered by the USA in the war of 1848. The telegram was deciphered by Room 40 and passed to the US ambassador in London, Walter Hines Page. President Wilson gave it to the US Press for publication on 1 March 1917, and the ensuing public outcry led the US Congress to declare war against Germany on 6 April 1917.

In this section, we present the wording of the telegram and a related message to von Bernstorff. The next section deals with questions of transmission and cryptography, then Section F.4 with the political fallout, and Section F.5 with the background and the German reaction.

Figures F.2 through F.4 show the original, from the archives of the German Foreign Office, of the notorious *Zimmermann telegram*. Its text, beginning on line 7 of the right hand column, reads:

Ganz geheim. Selbst entziffern.

[Wir beabsichtigen, am 1. Februar uneingeschränkten U-Boot Krieg zu beginnen. Es wird versucht werden, Amerika trotzdem neutral zu halten.

Für den Fall, daß dies nicht gelingen sollte, schlagen wir Mexico auf folgender Grundlage Bündnis vor: Gemeinsame Kriegführung.

[illegible]

Figure F.2: The first page of the Zimmermann telegram, as prepared at the German Foreign Office.

[illegible]

Figure F.3: The second and final part of the Zimmermann telegram, and the first part of the separate message to von Bernstorff.

zwischen uns und Olmanika zum Feind
 kommt, wir werden auszuweichen und
 ihn gleichzeitig nachzulassen, gegen
 von uns zum Feind auszuweichen.

H. G.

F 13/1

M. T. 12.7.13

M. T. 13.7.13

Figure F.4: The last part for von Bernstorff, and the initials of the officials at the Foreign Office.

Gemeinsamer Friedensschluß. Reichlich finanzielle Unterstützung und Einverständnis unsererseits, daß Mexico in Texas, Neu-Mexico, Arizona früher verlorenes Gebiet zurückerobert. Regelung im einzelnen Euer Hochwohlgeboren überlassen.

Euer Hochwohlgeboren wollen Vorstehendes Präsidenten streng geheim eröffnen sobald Kriegsausbruch mit Vereinigten Staaten feststeht und Anregung hinzufügen, Japan von sich aus zu sofortigem Beitritt einzuladen und gleichzeitig zwischen uns und Japan zu vermitteln.

Bitte Präsidenten darauf hinweisen, daß rücksichtslose Anwendung unserer U-Boote jetzt Aussicht bietet, England in wenigen Monaten zum Frieden zu zwingen.]

This translates into English as:

Most secret. Decipher yourself.

[We intend to begin on the first of February unrestricted submarine warfare. We shall endeavour in spite of this to keep the United States of America neutral.

In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: Conduct war jointly. Conclude peace jointly. Substantial financial support and consent on our part for Mexico to reconquer lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to your Excellency.

Your Excellency will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain, and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence, and at the same time mediate between Japan and ourselves.

Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace.]

The original record contains several notes about encryption and transmission, which we discuss below. Furthermore, there is another note to von Bernstorff which explains the instructions given to von Eckardt. It reads:

In Postziffern. Ganz geheim. Selbst entziffern. Zu Euer Hochwohlgeboren ausschließlich persönlicher Information.

Der Kais. Gesandte in Mexico ist angewiesen, Carranza für den Fall, daß es zwischen uns und Amerika zum Kriege kommt, ein Bündnis anzutragen und ihm gleichzeitig nahezu legen, Japan von sich aus zum Beitritt einzuladen.

That is:

In cipher. Most secret. Decrypt yourself. Personal information for your Excellency only.

The Imperial envoy in Mexico is instructed to propose to Carranza an alliance, in case war breaks out between us and America, and to suggest to him at the same time to invite Japan to enter, on his own initiative.

There are two marginal notes expanding on the contents which were not sent with the telegram. The first, inserted at the German *Einverständnis* (= consent), says that no guarantee (for reconquering the three states) is given. The second one, after the mention of Arizona, reads *Californien dürfte für Japan zu reservieren sein*, that is, California should be reserved for Japan. It had also been taken by the USA in the 1848 war, and its mention indicates a discussion at the German Foreign Office about whether they should throw in California as a bonus—it would not increase their cost.

California does not appear in the decryption of the telegram in Figure F.5. But somewhat mysteriously, Millis (1935) mentions California in the quote given below on page 111. Friedman & Mendelsohn note this and ask: *Is it possible that the Germans were reserving California as bait for Japan?* Good guess!

The initials on the last page are, from bottom up: von von Kemnitz 11/1., Montgelas 12/I, Wilhelm August von von Stumm 12. I., Hilmar Freiherr von dem Bussche-Haddenhausen 13/1, St. S. [Staatssekretär = Secretary of State] Zimmermann 13/1.

The Zimmermann telegram has always played a major role in the American historiography of the First World War, and a very minor one in the German view. The basic difference is that on one side it is regarded as an evil and immoral plot, and on the other side as a legitimate if stupid diplomatic enterprise in times of war. Inexact translations of the central phrase have contributed to this rift; the noncommittal *Einverständnis, daß Mexico ... zurückeroberet* = *consent for Mexico to reconquer ...* has usually become the exhortation of an *understanding* (or even *undertaking*) *that Mexico is to reconquer ...*

F.3. Transmission and cryptanalysis

There are several versions of how the Zimmermann telegram was encrypted and transmitted by the Germans and cryptanalyzed by the British, and some of the finer points still await clarification.

This much is clear: the telegram was sent from Berlin to Washington, and then on to Mexico City. The British intercepted it on its first leg, cryptanalyzed it, and then also obtained a copy of the message in Mexico.

WESTERN UNION TELEGRAM
NEW YORK CARLTON BUILDING

Read the following telegram, subject to the terms on back hereof, which are hereby agreed to:

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11209 18276 18101 0317 0228 17694 4473
22224 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17653 67893 5870 5454 16102 15217 22801 17138
21001 17388 7416 23638 18222 5719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22401 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52242 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22404 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76056 14215
5144 2831 17920 11347 17142 11264 7667 7762 15099 9410
10482 97556 3569 3670

BERNSTOPFF.

George German Embassy..

via Galveston
JAN 29 1917

Figure F.5: The Zimmermann telegram, as forwarded from New York to Mexico.

This second leg is quite well known: von Bernstorff sent the telegram, shown in Figure F.5, via Western Union to the German legation in Mexico, encrypted in the German diplomatic code 13040. It encodes the text in Figures F.2 and F.3, and von Bernstorff has added at the beginning *Nr. 130, 13042, Auswärtiges Amt telegraphiert am 16. Januar: Nr. 1*. Here 130 is the Washington number of the telegram, the 13042 indicates code 13040, and the rest says that the *Foreign Office has telegraphed on 16 January, Nr. 1*. At the end, Zimmermann's signature is followed by *stop end-of-message*, and finally *Bernstorff* in cleartext.

The first leg of the transmission is less clear. There are four transmission routes possible: US diplomatic cable, "Swedish roundabout" Berlin – Stockholm – Buenos Aires – Washington, radio Nauen-Sayville, or U-boat *Deutschland*. We will see that there is firm evidence only for the first option. The Swedish and the radio routes have been put forward in several earlier publications, but unless new documents come to light, they must be rejected as being unproven.

On 4 August 1914, one day after England's declaration of war, the British ship *Telconia* severed the transatlantic cables linking Germany to America. Now how could the Kaiser speak to his most obedient underlings in Washington?

Since the *Lusitania* crisis in May 1915, the US State Department transmitted from time to time German code messages on their diplomatic cable Washington–London–Copenhagen–Berlin, in the context of peace initiatives and at the instigation of Colonel Edward Mandell House, an influential advisor of President Wilson. The Americans did not have the keys to the code, a procedure in contravention of accepted practice for neutral nations. This route had been used several times in January 1917. The Zimmermann transmission also went via this US diplomatic line, a brazen abuse of American hospitality. A long cipher message registered as Telegram Nr. 157 was delivered to the US embassy in Berlin at 3 p.m. on 16 January 1917 and thence transmitted via Copenhagen and London to Washington. In it, the German chancellor Theobald von Bethmann von Bethmann Hollweg explained to von Bernstorff the German U-boat decision and instructed the ambassador to inform Wilson on 1 February (later changed to 31 January). Nr. 158 was attached to it; it is the famous Zimmermann telegram. Both arrived in Washington on 17 January and were handed to von Bernstorff on the 18th.

A second possibility is indicated by the "Stockholm" instruction on the record from the Foreign Office (Figure F.2); it may have been followed or not. The Swedish government was officially neutral but with a pro-German inclination. They allowed the use of their own diplomatic traffic to the Germans for their transatlantic communications. These lines passed through the UK and were read by the British. Even if they could not read the German ciphers, they could tell their origin, and they protested in Stockholm in the summer of

1915. The Swedes promised not to allow German messages to Washington any more. They kept their promise literally, but now allowed the use of their communications with Buenos Aires in South America. The messages were given to the Germans there, who then forwarded them to their embassy in Washington. These lines also passed through Great Britain, and Room 40 became aware of it rather quickly. This time, they kept mum; seeing those messages was presumably deemed more important than protesting against illegal acts by a neutral power.

After the foundation of the Second Reich in 1871, Germans felt they had an inferior position among the world powers for lack of a world-wide presence. Even though a late-comer, they acquired colonies in Africa, China, and the Pacific. The brief colonial intermezzo ended in 1914, when all possessions were occupied by the *Entente* powers. Beginning in 1906, the German *Telefunken* company built a giant radio transmitter at Nauen, 30 km west of Berlin. It was used for broadcasting to the colonies, ships at sea, and also to the German-owned station at Sayville on the South shore of Long Island NY, which had been working since 1912. The station was closed in 1914, but from 20 April 1915 on the Germans were allowed to transmit between Nauen and Sayville. Even encrypted messages were allowed, but only under supervision. Namely, the German operators had given to the US Navy Department censors two copies of the codebook used for this traffic. The encrypted messages were carefully examined, and in some cases refused to be forwarded because they were not clearly understandable. It seems unlikely that the Zimmermann telegram, together with the long message No. 127, would have escaped this scrutiny. A second transatlantic radio connection between Eilvese near Hannover and Tuckerton on Hickory Island NJ was also taken over by the US government in 1914.

The US State Department had informed von Bernstorff on 26 January 1915 that *radio messages in code or cipher are only permitted to be exchanged between diplomatic missions in this country and their respective Governments, and then only when copies of code or cipher used have been deposited with the Naval Officials in charge of the radio station through which the message is to be sent or received*. If the Zimmermann telegram was transmitted by radio, then the US censors must have ignored the last condition. Radio traffic was stopped on 10 April 1917, at least for private telegrams.

A major purpose of U-boats is to sink freighters, but the *Deutschland* was built to be one herself. As a cargo submarine she was to run the Atlantic blockade with which the British Navy was preventing international trade with Germany. After her second trip across the Atlantic, she docked on 2 November 1916 at New London CT. She brought 750 tonnes of paint, chemicals, and pharmaceuticals—and the 0075 codebook for the German legation in Washington. A US Customs inspection concluded that she had no weapons or ammu-

niton on board. Sailing on 17 November she scored her first “hit” by accident, colliding with a tow ship which then sank, with seven people drowned. The sturdy U-boat did not suffer any damage. She arrived back home in Bremen on 10 December 1916, “after a fast trip”. She was to sail again in January 1917, carrying the Zimmermann telegram on board. The marginal note at top left, lines 4 and 5, in Figure F.2 instructs *Mit U-Boot am 15. d. M. über Washington*⁵, and indeed the note at bottom left says that *Items 1. and 2. Entnommen für U-Boot. 13/1.*⁶ This was a few days after the decision to wage unrestricted U-boat warfare, her trip was cancelled and she was drafted into active service on 10 February. She was outfitted with guns and torpedoes, and sortied on 23 May 1917, now as *U-cruiser U-155*, with Lieutenant Captain Karl Meusel as her skipper. She sunk 19 Allied vessels, none by accident, before her return on 5 September.

We may conclude the following about the transmission.

The Zimmermann telegram from Berlin to Washington

- went via US diplomatic cable,
- probably did not go on the Swedish roundabout,
- probably was not transmitted by radio,
- did not travel by U-boat.

A second question is: in which system was it encrypted? One of the codes used by the German Foreign Office at the time was called Code 13040. It consisted of about 11000 words, to which 3-, 4-, or 5-digit encryptions were assigned. There were 100 words per page, numbered from 00 to 99 in their alphabetical order. Four pages were printed on one sheet, and these sheets could be rearranged to vary the code; the encoding of a word consisted of the page number plus its number on the page. The shorter codewords served for numbers, dates, common phrases, and grammatical inflections. Common words like *Komma* or *Stop* were sprinkled on each page. Some pages were given two numbers, so that frequencies of words on that page could be halved.

We can see a partial alphabetic order even in the relatively few words of the Zimmermann telegram:

⁵By U-boat on the 15th of this month via Washington

⁶Items 1. and 2. removed for U-boat on 13 January.

14814	einladen	22049	sich
14936	eingeschränkten	22096	Sie
14991	Einverständnis	22200	stop
15021	einzeln	22260	sobald
15099	Empfang	22284	sollte
		22295	sofortiger

Unteutonic alphabetical levity seems to have flipped 14814/14936 and 22284/22295; frequent words like *stop* often occur out of order.

The other system used by the Germans was the 10000-word codebook called 0075 (or 7500), which had been brought to the USA in November 1916 by the U-boat *Deutschland*. It was a two-part codebook (ciphertext numbers assigned randomly to cleartext words (see end of Section D.1)), and had not been sent to Mexico. The German original in Figures F.2 and F.3 gives clear instructions: send the message to von von Eckardt from Berlin in 13040, and the one for von Bernstorff in 0075. This is in perfect agreement with the availability of the codes in the two embassies. In fact, we can even follow the process leading to this decision: at top right in line 5, the scribe has noted *In Postziffern* (= in transmission cipher), and someone else has noted in parentheses *Mit geh. Chiffre vers.* (= to be sent with secret cipher), in the centre, crossreferenced to this note, someone has penned the question: *Hat Mexico geh. Chiffre vorliegen?* (= is the secret cipher available in Mexico?), and this interchange leads to the clear instruction at left to send the missive in 13040:

Chiffrierbüro: Ang. 1 ist mit Chiffre 13040 zu chiffrieren, der in Mexico vorhanden und, soweit bekannt, nicht kompromittiert ist.⁷

Similarly in agreement with the availability of the codes is the note 0075 to the left of the message to von Bernstorff.

A central source about the British cryptanalytic effort against the Zimmermann telegram is a note composed by Nigel de Grey on 31 October 1945 and published in Kahn (1999). He was the main codebreaker in Room 40 dealing with the telegram, and wrote: *The version of the telegram upon which we worked was the version in 13040, which reached us from the Cable office in transit [...] we had been at work some time on 13040. Only one person worked on it for many months then two and later three. It was a long code, our experience of book building was at its beginnings and there were many gaps unfilled. [...] We could at once read enough for Knox to see that the telegram was important. Together he and I worked solidly all the morning upon it. [...] Work [...] was slow and laborious.*

Now de Grey obfuscated the issue—as befits an able cryptographer—by writing in the same note that *the version that went through Bernstorff's office*

⁷To the cipher bureau: Document 1 is to be encrypted with code 13040, which is available in Mexico and, as far as is known, not compromised.

was in 7500 so far as I recollect. There are two interpretations of this remark: either the telegram was sent from Berlin to Washington both in 13040 and in 0075 (a capital crime in cryptography), possibly over different channels, or de de Grey's recollection failed him and only the second message to von Bernstorff was sent in 0075. The further text of de de Grey's note makes it clear that the 13040 version is definitely not the copy obtained by the British in Mexico sometime later, also in 13040. De de Grey also explains the ensuing cloak-and-dagger action: *Although we had the 13040 version and knew von Eckardt had no 7500 book, without disclosing our drop copy source, we could not produce it. Nor could we prove that the telegram had actually been delivered in Mexico to the German Legation and had not been faked in London. The only thing therefore was to steal a copy in Mexico City in the form delivered to the German Legation. We had two chances (a) the cable copy (b) the copy sent from Washington by Bernstorff which we banked on being also in 13040. Hence the delay till the end of February. How we succeeded in stealing the copy I never knew but money goes a long way in Mexico and steal it we did.*

An affidavit by Hall, dated 28 December 1926, includes a message from Berlin to Washington dated 26 January 1915 that was sent in code 13040 and decrypted. This can be taken as an indication that Room 40 had broken 13040 already in early 1915, in contradiction to de de Grey's statement. However, Hall also presents the cock-and-bull story of the German agent in Persia arrested while he was cutting an oil pipeline with the 13040 codebook in his luggage. In the conflict between de de Grey and Hall, the former's professional statements carry more weight, in my opinion, than Hall's affidavit which may still be colored by a desire for secrecy or obfuscation. Berlin knew that the Zimmermann telegram would go from Washington to Mexico in code 13040. Good practice would have forbidden to send it in code 0075 from Berlin to Washington. A further consideration is that the telegram had been transmitted in code, and its cleartext published. A professional cipher bureau would have considered the possibility that the encrypted version was also known to the enemy cryptanalysts and inferred that the code was then insecure. However, the German Foreign Office considered code 0075 secure still in February 1918. We may conclude that either the telegram was not sent in 0075, or else the German cryptographers were not good professionals. We may conclude the following.

The Zimmermann telegram was encrypted

- in code 13040 Berlin-Washington and Washington-Mexico,
- not in code 0075.

On 1 March Secretary of State Robert L. Lansing had the two cipher tele-

9 January	Imperial U-boat decision
13 January	Zimmermann signs message
16 January	telegram(s) from Berlin to Washington in 13040 (and 0075?)
17 January	partial decrypt of 13040 message at Room 40
19 January	telegram from Washington to Mexico in 13040
31 January	Germany declares unrestricted U-boat warfare
3 February	Wilson breaks diplomatic relations with Germany
10 February	Room 40 receives 13040 message from Mexico
22 February	Hall gives complete decrypt to Page
24 February	Wilson receives the telegram
1 March	story published in US newspapers
3 March	Zimmermann admits responsibility by a press communiqué
6 April	US congress declares war on Germany

Table F.1: The Zimmermann chronology in early 1917.

grams to and from von Bernstorff in his hands (which differed in the address line), but presumably not the copy obtained by the British in Mexico. He cabled *the original message* to London; it was the 13040 cable from Washington to Mexico and deciphered by de de Grey (see below). Now if the Berlin to Washington message had been in 0075, would Lansing have referred in a definitive way to *the original message*?

The US cryptographers of the Signal Security Agency (MI-8) reviewed in 1945 the German codes of World War I and concluded: *in spite of [some] defects the German codes were distinctly better than those of other governments which MI-8 studied during the war [... They] were much better, it must be admitted, than the corresponding systems in use by the United States Army at the beginning of the war.*

F.4. The drama unfolds

The salient dates in the history of the Zimmermann telegram are given in Table F.1. At an Imperial war conference, the “ruthless” employment of total U-boat warfare was decided on 9 January, and the foreign minister Zimmermann signed the message on 13 January.

The two British cryptographers, Dillwyn Knox and Nigel de de Grey, dealing with the telegram worked feverishly on their task, but progress was slow. The first partial decrypt was handed to Admiral Sir Reginald Hall, the head of Room 40, around 10.30 a.m. on 17 January. Right away, it was clear to everybody that the telegram was a bombshell that could serve to draw the US into the war—on the *Entente* side, of course. Three problems had to be addressed:

- how to prove authenticity of the telegram,
- how to prove correctness of the decryption,
- how to safeguard the secret of Room 40.

Admiral Hall had a brilliant idea. He charged a British agent—only known as Agent T—in Mexico City with obtaining copies of all recent telegrams to the local German embassy. T became friends with a Mexican telegraph office clerk. He may have paid for it, or “stole it he did”, as de de Grey says—in any case, Hall had the Zimmermann telegram as received in Mexico City in his hands on 10 February. The clever move paid off handsomely.

Now it was time for a series of subtle diplomatic moves. How to hand this god-sent message to the US government without raising suspicion about its authenticity? There was a sense of urgency. At the German announcement of unrestricted U-boat attacks, President Wilson had broken off diplomatic relations and sent ambassador von Bernstorff packing. But he kept stalling with the declaration of war that the *Entente* hoped for.

Finally, on 22 February 1917, Hall gave the telegram and its decipherment, completed on 19 February, to Page, the US ambassador in London. Hall recruited the British Foreign Secretary Arthur James Balfour for an official act of passing the document to Page, the next day. He had been First Lord and Prime Minister in his long career, and was the most respected British politician at this time. President Wilson had the message on 24 February. The US State Department found at the Washington office of Western Union the encrypted Zimmermann telegram that had travelled over its own lines. Indignation ran high in the White House at this abuse of American generosity. On 28 February, they obtained from Western Union a copy of the Washington to Mexico message, shown in Figure F.5.

US Secretary of State Robert Lansing gave the story to E. M. Hood of Associated Press, and it hit the newspaper headlines on 1 March. A wave of patriotism swept through the nation, as even the South-Westerners and Westerners realized that the war was not as far away as they had thought. But some skeptics still thought this might all be a British ruse. On 1 March, Lansing cabled to Page in London *the original message which we secured from the telegraph office in Washington*, and de de Grey deciphered it at the Admiralty under the eyes of Edward Bell, a secretary at the American embassy. Actually, this almost ended in disaster. De de Grey had brought an incomplete version of the codebook, and had to extemporize many codewords—which he knew by heart and, luckily for him, Bell did not ask to check in the codebook. Conjuror’s magic in cryptography. It was more than enough to convince Wilson.

But it might not have been enough for a suspicious outsider. However, Zimmermann obliged again and came to rescue. An official German press

communiqué appeared on 3 March 1917 in the papers. It stated that the German envoy in Mexico had been instructed to offer, in case of a US declaration of war against Germany, an alliance to Mexico. The communiqué also speculated how the Americans might have obtained the telegram, and proposed that this was most likely by treason on US territory. President Wilson had won his election on 7 November 1916 with the slogan “He kept us out of war”. Germany’s declaration of unrestricted U-boat warfare changed his mind, but not yet that of the population. Zimmermann achieved this with his telegram. Even the German-Americans “retreated across their hyphen to take their stand, somewhat sullenly, on the American side”. But the USA would most likely have entered the war anyway, for several reasons:

- Germany’s U-boat war was a slap in Wilson’s face, who had dreams of ending the war in early 1917 with a peace conference, and von Bernstorff tried honestly and hard to convince his government that this was a more beneficial solution than the submarines and war with the USA,
- pro-British feelings in part of the population, major exceptions being the German and the Irish immigrants,
- the ideological closeness with the Western democracies under attack from the Old European Emperors. A contradiction here was that the Russian Tsar was on the *Entente* side, but the February Revolution in March 1917 corrected this problem. The Tsar resigned on 15 March, Kerenski took over in July, and Lenin’s October Revolution in November 1917 brought seventy years of workers’ paradise to Russia and later the Soviet Union. American public opinion sympathized more with the Russian revolutionaries than with the Tsar.
- Pressure from the financial and industrial establishment that had made massive loans, mainly war materials, to the *Entente* powers. The French IOUs stated *L’Allemagne paiera*⁸.

One can only speculate how much longer the USA would have hesitated without the Zimmermann telegram. De de Grey writes that *it gave Wilson his big stick for the West and South West, and America came into the war months earlier than she would otherwise have done*.

The secret of Room 40 was well guarded. Wild speculations abounded of how the message had been given away by treason or stolen in Mexico, or a messenger intercepted on the Rio Grande frontier. Nobody suspected the Berlin-Washington transmission, or deciphering of a code.

The rest is history: the massive deployment of American troops and arms, effective in early 1918 after almost a year of armament, helped to push the

⁸Germany will pay

weakened German military over, enfeebled by a starved economy and disillusioned population.

The Americans were not amused, as Millis writes in his *Road to War*:

What made it particularly shocking, of course, was the suggestion that the Japanese (with whom we were about to become allied) should be invited into the American Continent, or that the principle upon which many Americans had demanded the restoration of Alsace-Lorraine (because they had been acquired by force) should be applied to California and Texas, which we had forcibly detached from Mexico. Informed Americans understood perfectly well that the Allies had bribed Japan, Italy and Rumania into the war with the promise of slices from the enemy carcass; but they were sincerely and profoundly horrified by the thought that Germany could be so base as to bribe Mexico and Japan with the promise of slices from the flanks of the United States.

The *Entente* governments also had a relaxed view on territorial integrity. On 8 May 1915, Ambassador Page reported to President Wilson *that England, France, and Russia made a bargain with Italy on April 30th [1915], agreeing to cede to Italy very large parts of Austrian territory [...] if Italy comes into the war within a month.* And indeed, after the war, the losing countries had their territories cut up and large chunks amputated.

Von Bernstorff was German ambassador in Washington from 1908 to 1917. He worked hard trying to avoid war between Germany and the USA, mediating in various peace initiatives and alerting his government to the dire consequences of a US entry into the war. He warned particularly strongly against unbridled submarine warfare—to no avail. No one who reads Bernstorff's telegrams can remain unconvinced of his absolutely sincere desire for peace between the United States and Germany. Outside business hours, he was a society lion and successful charmer of the ladies. After the war, he continued his efforts as president of the *German League for the League of Nations*, but peaceful goals were not really popular at that time. He emigrated in 1933 and died in Geneva in 1939. His son Albrecht was murdered by the Nazis on 24/25 April 1945.

The literature about the Zimmermann telegram is substantial. Among the first works were the (auto-) biographies of von Bernstorff (1920), Hendrick (1922), and House (1926). Next came the cryptographic analysis of Friedman & Mendelsohn (1938), the political circumstances in Tuchman (1958), and the comprehensive treatment in Kahn (1967), pages 282-297. Further contributions were Kahn's publication of memoranda by Bell and de Grey, and Nassua (1992) who studied the reaction of the German press in the USA, and also the debates in the Reichstag committee.

Hall's involvement in the Zimmermann decode was not made public until 1955, when James's book appeared. He wrote in 1932 an account of his work in Room 40, but the British Admiralty did not permit its publication . . .

James Alfred Ewing, the founder of Room 40, gave a lecture on *Some Special War Work* in Room 40 on 13 December 1927 at the University of Edinburgh, which *disturbed the serenity of Admiralty circles* so much that they prohibited publication of even newspaper articles about it. In Strother (1918), the reader is enticed by the remark that *the story of the Zimmermann note cannot yet be told*.

F.5. Wright or wrong, my country

The political background of the Zimmermann telegram is somewhat convoluted. The upshot is that it was more likely intended for use in the political struggle between government and military in Germany rather than as a serious treaty proposal to Mexico.

One part of the background was the fundamental animosity between Mexico and the United States at the time. Mexican oil was vital for the British Navy. US troops had occupied the port town of Veracruz on 22 April 1914, leaving 126 Mexicans and 19 US soldiers dead. Carranza had overthrown the elected president Victoriano Huerta in 1915 and made himself president. The resulting civil war was gleefully kindled by the Germans. Francisco "Pancho" Villa, one of the leaders, attacked the border town of Columbus in New Mexico on 9 March 1916, killing 17 Americans. In response, President Woodrow Wilson sent a punitive expedition under Colonel (later General) John J. Pershing into Mexico in order to apprehend Villa. The 12 000-man expedition was a dismal failure, and the marauding cavalry's behavior during its one-year rampage in Northern Mexico increased widespread *yanquifobia* in Mexico: "Poor Mexico, so far from God and so close to the United States", in the words of former president Porfirio Díaz.

On 15 June 1916, Colonel Gonzalo C. Enrile presented himself in the German Foreign Office in Berlin as an emissary of the deposed president Huerta. He proposed a pact between the two countries, demanding financial support, offering military action against the United States, and mentioning an agreement with Japan as Mexico's option. And on 3 November 1916, the Mexican ambassador in Berlin proposed an alliance, which would include German military help to Mexico and the installation of direct radio communications. Some of these elements reappear in Zimmermann's telegram. But in 1916, the German government was not interested in the Mexican proposals.

A second part of the background was Germany's political isolation at the time. The German envoy Hellmuth Freiherr Lucius von von Stuedten had negotiated in 1916 with the Japanese ambassador ??? Ushida in Stockholm.

These talks had been broken off unsuccessfully, and in 1917 the German government looked for Mexico's help as an intermediary to get into contact with Japan again. Japan was then a member of the *Entente*, the coalition of Germany's war enemies.

The major part of the background is the political struggle between government and army command in Germany. On 7 May 1915, the German submarine U-20 had sunk the passenger ship *Lusitania*, causing a loss of 1400 lives. The *Lusitania* was outfitted as an auxiliary cruiser and carried 2160 passengers. The German government, scared of the prospect of the United States entering the war, agreed after protracted negotiations to curb their submarine warfare in the North Atlantic. But the bloody stalemate in the European trench war led the German military High Command to the conviction that only unrestricted submarine warfare would bring England to her knees. Chancellor Bethmann von Bethmann Hollweg opposed this plan resolutely. In turn, the influential top brass demanded the resignation of Bethmann von Bethmann Hollweg and his government. Von Bernstorff cautioned from Washington, painting a scenario amazingly close to what was to happen in reality. On 9 January 1917, the politically unsophisticated military prevailed at a conference in the Imperial headquarters at Pleß in Upper Silesia, and the Kaiser signed the order for an all-out submarine war. In this atmosphere, Hans Arthur von von Kemnitz, the *ständiger Hilfsarbeiter* (Permanent Assistant) directing the Far Eastern and Latin American (except Mexico) department had the brilliant idea that condensed into the infamous telegram. He initialled a first version on 11 January 1917, the official dealing with Mexico, Graf Montgelas, initialled it on 12 January, and Zimmermann on the 13th. The Chancellor was under attack from the military blockheads, and Zimmermann tried to move out of the line of fire with his diplomatic initiative, designed to take the fear out of the generals' hearts of having to face the US as a formidable enemy.

The German Foreign Office was not sufficiently naïve to believe that the United States of Mexico could make war on the other United States successfully. They tried to use Mexico as a pawn in their Weltpolitik rather than as a partner. This may explain why Zimmermann committed the further blunder or miracle—depending whose side you're on—of acknowledging authorship of the telegram.

The diplomats felt a responsibility to procure partners wherever possible in case of the US entering the war. However, the subtle point that the German ambassador in Mexico was carefully instructed to act only after the US gave up their neutrality was overlooked by the infuriated readers of American newspapers. On 5 February, Zimmermann sent a telegram directly to von von Eckardt: *Sofern nicht Verrat Geheimnisses an Vereinigte Staaten zu befürchten, wollen Euer Hochwohlgeboren Bündnisfrage schon jetzt mit Präsidenten erörtern. Jedoch bleibt definitiver Abschluß Bündnisses abhängig von*

*Kriegsausbruch zwischen Deutschland und Vereinigten Staaten. Präsident könnte von sich aus schon jetzt Japan sondieren. Sollte Präsident aus Furcht vor späterer amerikanischer Rache ablehnen, sind Sie ermächtigt, Defensivbündnis nach Friedensschluß anzubieten, wofern es Mexiko gelingt, Japan in Bündnis einzubeziehen.*⁹

Von von Eckardt presented this offer to the Mexican Foreign Minister Cándido Aguilar Vargas on 20 February. After some deliberation and the US declaration of war against Germany, President Carranza rejected it on 14 April.

In the memorable debate on 5 March 1917 of the 28-member Main Committee of the German parliament—secret matters were not discussed in full session—the Social Democrat member Dr. Eduard David gave short shrift to the foreign ministry: *Bezüglich des Inhalts des Schriftstücks betont Redner, dass es ein gewisses Kopfschütteln erregen müsse, dass wir Mexiko Teile der Vereinigten Staaten gewissermassen anbieten. Dieser Vorschlag verrate eine merkwürdige Einschätzung der in betracht kommenden Kräfte. Kein Kenner der Verhältnisse werde im Ernst glauben, dass Mexiko mit seinen militärischen Mitteln imstande sei, gegen Amerika einen so erfolgreichen Krieg zu führen, dass es ihm dauernd Gebietsteile entreissen könne. Ein solches Anerbieten könne von massgebenden Leuten in Mexiko selbst nicht ernst genommen werden.*¹⁰ In his reply, Zimmermann admits: *Auch ich bin der Ansicht, dass die Mexikaner nicht in der Lage sind, gegen die Union einen derartigen Krieg zu führen, dass sie solche Provinzen erobern können. Mir lag aber daran, so schnell wie möglich Carranza zum Losgehen zu veranlassen. [...] Mir kam es darauf an, unsern braven Feldgrauen nicht neue Feinde auf den Hals zu hetzen und wenigstens dafür zu sorgen, dass die amerikanischen Söldner, die etwa für Europa in Frage kommen sollten, sofort gegen Mexiko Beschäftigung fanden. Deshalb habe ich gerade auf diese Provinzen hingewiesen, damit die Mexikaner sofort in amerikanisches Territorium einfielen und die Amerikaner so verpflichteten, ihre Truppen dort hinzusenden und sie uns fern zu halten. [...] In diesem Kriege ist die Moral zu den Akten gelegt worden. [...] Gewiss, Mexiko hat keine Waffen im modernen Sinne, aber die Banden [struck*

⁹Provided no treason of this secret to the United States is to be feared, your Excellency may already now broach the question of an alliance to the President [Carranza]. However, the definite conclusion of an alliance depends on the outbreak of war between Germany and the United States. The President might already now sound out Japan on his own initiative. Should the President decline for fear of subsequent American revenge, you are empowered to offer a defensive alliance after conclusion of peace, provided Mexico succeeds in drawing Japan into the alliance.

¹⁰Concerning the contents of the telegram, the speaker [Dr. David] stressed that one cannot help but wonder how we can essentially offer parts of the United States to Mexico. This proposal suggests a bizarre assessment of the forces involved. Nobody familiar with the situation would seriously believe that Mexico would be able, given its military strength, to wage a war against America with sufficient success to occupy parts of its territory for any length of time. Such an offer could not be taken seriously by the relevant people in Mexico.

out: *Räuberbanden*] sind immerhin genügend mit Waffen versehen, um in den Nachbarprovinzen von Amerika Unbequemlichkeiten und Unruhen hervorzurufen.¹¹

The member Dr. Oskar Cohn points out that Zimmermann *habe Wilson eine glänzende Argumentation in die Hand gespielt, um das amerikanische Volk geschlossen um sich zu scharen*.¹² Zimmermann explains the arrangement which allowed encrypted German diplomatic traffic on US State Department lines: *Meine Instruktion ist telegraphisch hinübergegangen, und zwar durch Vermittlung des hiesigen amerikanischen Botschafters. Der amerikanische Botschafter hatte das Recht vom States Department, gewisse Telegramme für uns hinüberzubefördern, und andererseits hatte unser Botschafter in Washington das Recht, gewisse Telegramme an uns durch Vermittlung des States Department herüberzugeben. Angeblich handelte es sich bei diesen Telegrammen um solche, die auf allgemeine Friedensbestrebungen hinzielten. An ein derartiges Telegramm habe ich dieses Telegramm angeschlossen. Es ist selbstverständlich, dass ich dabei eine Chiffre benutzt habe, die absolut geheim war und die der hiesige amerikanische Botschafter jedenfalls nicht kannte; darüber habe ich keinen Zweifel. Die Sache ist rechtzeitig nach Washington gekommen. Wie dann nachher die Sache verraten worden ist, ist mir unbekannt*.¹³ Quite some chutzpah, sending a war-mongering telegram over a line that the Americans generously provided for peace efforts. And then good luck for the British cryptanalysts. In an earlier debate, Zimmermann had pointed out: *Der Präsident hat eben in Amerika eine ganz kolossale Macht. Wie man in England sagt: wright or wrong my country, so heißt es in Amerika:*

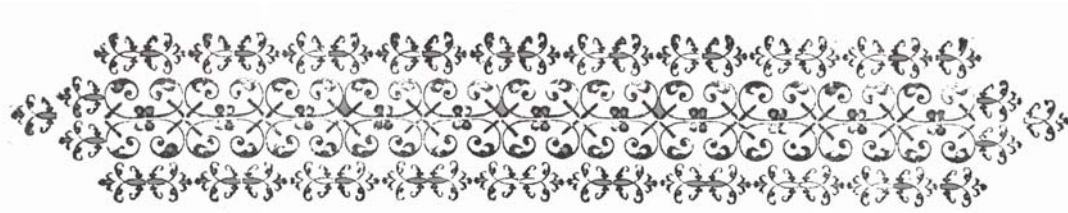
¹¹I share the opinion that the Mexicans are unable to wage war successfully against the United States and conquer provinces. My intention was to convince Carranza to start marching as soon as possible. [...] It was important to me to avoid exposing our faithful field-gray uniforms to new enemies, and to provide employment against Mexico for the American soldiers of fortune who might otherwise go to Europe. That was the reason why I pointed out precisely these provinces so that the Mexicans immediately invade American territory and thus oblige the Americans to send their troops there and keep them away from us. [...] In this war, moral has been filed away. [...] Of course, Mexico has no weapons in the modern sense, but the gangs [struck out: robbergangs] are sufficiently supplied with weapons to stir up inconveniences and unrest in the neighboring provinces of America.

¹²has played a brilliant argument into Wilson's hands to rally the American people in unison around him.

¹³My instruction [the Zimmermann telegram] went out by telegraph, namely with the assistance of the American ambassador here. The State Department had granted their ambassador the right to transmit certain telegrams of ours over there, and on the other hand, our ambassador in Washington had the right to transmit certain telegrams to us via the State Department. Allegedly this applied to telegrams that were directed at general efforts for peace. I attached the telegram under discussion to such a telegram. It goes without saying that I used a cipher that was absolutely secret and which the American ambassador here certainly did not know; I have no doubt about this. The matter arrived in Washington on time. How the matter was then betrayed is unknown to me.

*wright or wrong my president. Der Mann mag Dummheiten machen, wie er will, die Nation steht immer hinter dem Präsidenten. Ich wünschte, bei uns wäre das auch so. (Große Heiterkeit.) Das ist natürlich nicht so wörtlich zu nehmen, denn bei uns macht die Regierung Gott sei Dank keine Dummheiten. (Heiterkeit.)*¹⁴ The misspelled English quote in this official document illustrates how little the Germans knew their enemies. This ignorance doomed their military, and their evil successors two decades later repeated such blunders.

¹⁴The President actually has enormous power in America. As they say in England: right or wrong my country, so they say in America: right or wrong my president. The man can commit stupidities as he likes, the nation will always stand behind the president. I wish it were like this in this country. (Great amusement.) Of course, this is not to be taken literally, because thank God our government does not commit stupidities. (Amusement.)



Chapter G

ENIGMA, Turing, and COLOSSUS

What memorable names! How they shine compared to bland technocratic acronyms like RSA, DSA, or AES!

ENIGMA was the cryptographic workhorse of the German military in World War II. It was originally broken by Polish mathematicians, who then handed their methods to French and British cryptographers. The latter eventually built up a large organization, whose most famous member was Alan Turing and whose cryptanalytic successes helped to shorten the war considerably. The team also designed COLOSSUS, the world's first electronic (valve) computer, for use in cryptanalysis.

G.1. ENIGMA

In Section 1.1, Alberti's disk provided a hardware implementation of the set $\{\sigma^i \tau : 0 \leq i \leq 23\}$ of substitutions, where σ is the cyclic shift by one (the *Augustus cipher*), and $\tau \in \text{Sym}_A$ arbitrary. Figure 1.1 shows three positions of an Alberti disk.

This can also be implemented with simple electrical wiring. We illustrate this on the six letter alphabet $\mathbb{A} = \{A, B, C, D, E, F\}$, with $\tau = (AFCE)(BD)$ in cycle notation. It requires two circular boxes that touch each other at six contact points, and can be rotated in six positions. The left one has τ hard-wired, and rotating the right one implements σ^i for various i .

Figure 1.1 rotor τ rotation σ stator

For the illustration, we have pulled apart the two cylinders. In the actual apparatus, the two would be so close together that there is electrical contact at the six contact points, and so that the rotor can be turned into the six possible positions.



Figure G.1: An Enigma machine.



Figure G.2: Two Enigma rotors.

So now we imagine the two cylinders pushed together, and the key “E” pressed at right. The current flows along the red wires, and the lamp “A” lights up; we have $\tau \circ \sigma^0(E) = \tau(E) = A$. Now if we turn the rotor in the direction indicated by one position and press “C”, then the green wires carry current and “B” lights up; we have

$$\tau \circ \sigma^1(C) = \tau(\sigma(C)) = \tau(D) = B.$$

Now this electrical implementation has a problem: the wires connecting the lamps to the minus pole have to be flexible. It would be hard to build this contraption without those wires suffering after thousands of rotations. The remedy is genially simple. Instead of two we take three such cylinders, fix the two outer ones, and only rotate the middle one. Then the only wear is at the contact points between two adjacent cylinders; this is manageable.

Figure?

The null position of the rotor still implements τ . What happens if we rotate it by one turn? The movement between the rotor and the right stator still implements σ , but between the left stator and the rotor, the “opposite” rotation is implemented, that is, the inverse $\sigma^{-1} = (A F E D C B)$ if $\sigma = (A B C D E F)$. If we press the key “C”, then the lamp “A” lights up; we have

$$\sigma^{-1}\tau\sigma(C) = \sigma^{-1}(\tau(\sigma(C))) = \sigma^{-1}(\tau(D)) = \sigma^{-1}(B) = A.$$

Thus this machine implements the set $\{\sigma^{-i}\tau\sigma^i : 0 \leq i \leq 5\}$ of six permutations of $\{A, B, C, D, E, F\}$.

As is often the case in the history of ideas, the time was ripe and the possibilities of such a cryptosystem were realized by four men in four countries around the same time. Apparently the US American Edward Hugh Hebern (1869–1952) was the first to have the idea, in 1917, but he made a US Patent application only in 1924. The German Arthur Scherbius (?) applied for a patent on 23 February 1918, the Dutch Hugo Alexander Koch (1870–1928) on 7 October 1919, and the Swede Arvid Gerhard Damm three days later.

Their common idea was to use the apparatus as described above, but with several rotors instead of one. Hebern took five, and Scherbius four rotors. He called his machine the ENIGMA. It was initially sold to the same clientele that was using commercial codebooks (Chapter D). The German military adopted it as a major cryptographic tool starting in 1926. Eventually the ENIGMA was used by various government agencies, including the post office, the railroad system and the police. It went through several stages of development, some of which increased security and others decreased it, unwittingly. Our description in the following applies to one specific model. The estimated number of ENIGMA machines built is around 200 000. Like Ford’s Tin Lizzy, it could be had in any color, provided the color was black.

The main parts of an ENIGMA are as follows:

- steckerbrett,¹
- key board,
- lamp board,
- wheels.

After pressing a key on the key board, say E , current flows to the E connector on the steckerbrett. The latter consists of 26 connectors, some of which may be connected in pairs. In the early days of the war, up to five pairs were connected, later exactly ten pairs. If E was not connected (“steckered”), then current would continue to flow to the E connector on the right-hand wheel. But if E was steckered, say to X , then current would go to the X plug on the right-hand wheel. Then it transits the wheels to and fro, and exits at some point, say P , on the right-hand wheel. Steckerbrett? This causes the P lamps to light up, and then the electrical circuit closes. Two operators are required: FRITZ reads out the cleartext aloud (ALICE seems inappropriate). EMIL types it into the Enigma, which he has set up with the current keys, and reads the ciphertext letter by letter back to FRITZ, who taps it in Morse code into his radio transmission unit. The recipients have to set up their ENIGMA in the same way, type in the ciphertext, and the cleartext lights up, letter by letter, to be copied down.

The setting used for encryption also serves for decryption, for the following reason. The encryption process can be viewed as a composition

$$\pi = \varrho \circ \sigma_r^{-1} \circ \sigma_m^{-1} \circ \sigma_\ell^{-1} \circ \sigma_u \circ \sigma_\ell \circ \sigma_m \circ \sigma_r \circ \varrho$$

of the steckerbrett permutation ϱ , the three wheel permutations σ_r , σ_m , and σ_ℓ , and the umkehrwheel permutation σ_u . Now if E is sent to X on the steckerbrett, that is, $\varrho(E) = X$, then also $\varrho(X) = E$. That means that applying ϱ twice does not change anything: $\varrho \circ \varrho$ is the identity. This also holds for the four wheel permutations involved, in particular, for σ_u . When we take the composition $\pi \circ \pi$, adjacent terms cancel one after the other, and we also find $\pi \circ \pi$ to be the identity.

According to Kerckhoff’s Principle ? (and the early commercial availability), the ENIGMA system must be assumed to be known to the enemy. Security only relies on the secret key. This consists of three parts:

- sequence of wheels,
- setting of wheels,
- stecker connections.

¹also *stecker board* in English, *Steckerbrett* in German

Initially, a further secret ingredient was the internal wiring of the rotors. It would be unwise to rely on this for security, because then a single stolen or captured machine would jeopardize the whole system. Furthermore, Section G.3 presents in detail how Polish mathematicians figured out the wheel wiring from intercepts and an espionage coup.

The wheels came in a wooden box. Initially, there were three to choose from, which allows six possible permutations. A later version had five to choose from, giving $5 \cdot 4 \cdot 3 = 60$ possibilities. Each wheel could be set in one out of 26 positions. Furthermore, the stepping position of the middle and rightmost-hand wheel could be chosen out of 26 positions, giving in total $26^5 = 11881376$ possibilities. The stecker board, with five steckered pairs, gives

$$\frac{1}{5!} \binom{26}{2} \binom{24}{2} \binom{22}{2} \binom{20}{2} \binom{18}{2} \approx 5 \cdot 10^9$$

possibilities, and about $1.5 \cdot 10^{14}$ with ten connected pairs.

With the latter value, the total number of possibilities comes to about

$$1.1 \cdot 10^{23}.$$

This is a very large key space, whose exhaustive search would not have been possible (at least at the time). But the second most common mistake of crypto system designers is to take a large key space as a guarantee of security. This particular system fell prey to a combination of implementation errors and known plaintext attacks. (The most common mistake is to take the designer's failure to break his own system as proof that everybody else will fail, too.)

The three rotors of the German Navy ENIGMA could be chosen from a set of eight. This rotor setting was first changed monthly, later daily, and from mid-1942 on every eight hours.

The ENIGMA rotors advanced after the encryption of each letter by various amounts. In the 1923 ENIGMA A the four rotors moved by 11, 15, 17, and 19 positions, respectively. correct?

G.2*. Bletchley Park

No single event can be pinpointed that brought about Allied victory in the Second World War, but the British cryptanalysts at Bletchley Park played a vital role in many battles whose outcome eventually saved the world from brutal Nazi domination.

Alan Turing (1912–1954), a famous British mathematician and computer scientist, had proposed in 1937 a precise mathematical model of computers—the *Turing machine*—invented the idea that programmes could be stored as data (namely, for his *universal Turing machine*), and proved that deceptively simple questions cannot be solved by any algorithm. For example: as input you

take a string which represents a program in any reasonable programming language, and as output you want to know whether it does not go on working forever (with all variables initially set to zero, say). Turing undecidability result about this *Halting Problem* is devastating. It says that there exists no algorithmic method that can answer this question correctly. None at all! Not because programmers are stupid, but because it is inherently impossible! It resembles somewhat *Heisenberg's uncertainty principle*, which also says that some reasonably posed problems have no solution. After the war, he devised the *Turing test* of artificial intelligence: can you tell whether you are interacting with a human or a machine? If you cannot, then you are interacting with artificial intelligence. Half a century later, this remains an unfulfilled hope (or despair, depending on your outlook). Our distinguishers between pseudorandom and truly random generators in ?? apply the same principle in a different setting.

The cryptanalytic success against the ENIGMA was started by a team of Polish cryptographers, including the mathematician Marian Rejewski. They had completely solved the then standard machine in 1939. Section G.3 describes in full detail their cryptanalysis of the Enigma rotors, which was completed in 1932. later! In August 1939, just a month before Hitler's blitzkrieg attack on Poland and while most people were still happy with the seeming success of appeasement politics at München, they were wise enough to share their secrets and machinery with French and British cryptographers. Later, they were treated in a cavalier way: while in exile in England, they were not allowed to participate in the British cryptanalytic effort.

One of their main inventions was the *bombe*, an electromagnetic device.

A vital ingredient to the initial Polish Enigma break was a classical espionage coup by the French Secret Service. Hans-Thilo Schmidt, working in the *Chistelle* of the *Reichswehrministerium* (cipher bureau of the Reich's Defense Ministry) offered his services in October 1932. Directed by Colonel Gustave Bertrand and under the codename Asché, he divulged many secrets. Among them were complete key schedules for certain periods, as discussed in Section G.3 below. The French secret agent Lemoine, captured and interrogated by the Germans, betrayed Asché, who was arrested at home in Fürstenwalde and executed in July 1943.

The British Foreign Office set up a team of cryptographers at Bletchley Park on 4 September 1939, one day after Hitler attacked Poland. A little later, Turing joined the team. One of their main task became the breaking of the Enigma-encrypted communication between the German Navy headquarters at Kiel and the submarines in the North Atlantic. These inflicted crippling losses on Allied transports from North America to Europe. After a long struggle, Bletchley Park started deciphering Enigma messages regularly in 1942.

The unfortunate U-Boot captain who had just radioed his coordinates to headquarters did not know that the P-2's dropping depth charges all around



Figure G.3: The main building at Bletchley Park manor?, used by the administration. Umbrella and shorts illustrate the versatile weather of a Buckinghamshire summer day.

him were secretly directed by the brain of a mathematical genius.

expand Ultra

At the highest level of secrecy, German military messages were enciphered on a different system, the *Siemens Geheimschreiber*. It also used rotors, in one version ten of them. But the principle differed from the Enigma's: the rotors generated a pseudorandom bit string (see ??), and each letter of the message was encoded by five bits, according to the standard *Baudot code*. These two bit streams were then added bitwise (XORed), just as one does in a one-time pad (Section 2.1). By a brilliant stroke of cryptanalytic genius, who? Bill Tutte? discovered this principle. And then Bletchley Park, in collaboration with British Post Office engineers, set out for one of their main achievements: the world's first computer. This COLOSSUS had about 1500 valves. Its input was fed on rapidly moving paper tape, at right in Figure ? showing the replica now standing in the Bletchley Park museum. The 1943 model was replaced on 1 June 1944, just before D-day, by the 2500-valve COLOSSUS MARK I. Their main purpose was to decipher radio traffic between the Berlin headquarters and German armies in Greece, North Africa, and Russia.

photo Bletchley Park, Colossus rebuild

Swedish breaking of Siemens Geheimschreiber; Ulfving

G.3. Rotor cryptanalysis

The Polish cryptanalytic success against the Enigma was the basis for all subsequent work, and quite possibly the major effort at Bletchley Park would not even have been started without the previous results.

Marjan Reweski conceived the basic mathematical ideas required for this cryptanalysis, and was later aided by other Polish mathematicians. In 1932, he reconstructed the secret interior wiring of the Enigma rotors, and then they could read the German messages. We present in detail the discovery of the rotor wirings, a clever piece of applied mathematics. It is sufficiently simple to be presented here, and sufficiently complicated to give an idea of the ingenuity required. The success of the approach is based on

- interception of many encrypted messages,
- systematic cryptographic mistakes by the Germans,
- a French espionage coup,
- Polish mathematical ingenuity.

The Enigma instructions, valid until 15 September 1938, provided a daily setting for the three rotors and the plugboard. Then the operator had to choose a three-letter message key, say XIX, type it twice: XIX XIX, and read off the result:

	0	1	2	3	4	5
0	AJUOEZ	AOCORQ	AZUOFZ	BPTNXY	CLZHTK	CQJHPL
6	DDOUKH	DKIUGU	DZVUFA	EAAXCG	ECLXSB	FTXQLF
12	GGRIBW	GMYYIS	HYJLJL	ITMJLV	IWAJDG	JAGZCI
18	JERZVW	JZTZFY	KANMCE	KSAMZG	LLMDTV	MVUFHZ
24	NXSPOX	ONDBUC	PDGKKI	PICKWQ	QUGYNI	RSIAZU
30	SCPCSD	SCQCST	SRPCQD	TVLRHB	UCYGSS	VHFTMO
36	WSHEZN	XCSSSX	XFWSAJ	YLZVTK	ZDBWKM	ZLKWTR

Table G.1: 42 intercepts, sorted alphabetically, of the six-letter beginnings of messages with identical daily key.

AJUOEZ. Then he set the three rotors to the corresponding positions X , I , and X , typed the message, and finally sent as ciphertext AJUOEZ followed by the encryption of the message. On a given day, all operators in a given net started in the same position, so that the permutation $A: \mathbb{A} \rightarrow \mathbb{A}$ corresponding to the first key stroke was identical for all of them. Here, $\mathbb{A} = \{A, B, C, \dots, Y, Z\}$ is the 26-letter alphabet and in our example we have $A(X) = A$. And also the next five permutations $B, C, D, E, F: \mathbb{A} \rightarrow \mathbb{A}$ are identical for everyone.

Table G.1 shows a list of six-letter beginnings of intercepts from a single day. We will now deduce one Enigma rotor wiring from these intercepts.

Some terminology relating to permutations of the alphabet \mathbb{A} is useful for our cryptanalysis. Two such permutations ρ and σ can be composed, so that if $\rho(a) = b$ and $\sigma(b) = c$, then $(\sigma\rho)(a) = \sigma(\rho(a)) = \sigma(b) = c$. (This operation provides the structure of a group on the set of permutations.) The inverse ρ^{-1} of ρ is again a permutation, with $\rho^{-1}(b) = a$ if and only if $\rho(a) = b$. If ρ and ρ^{-1} happen to coincide, so that $\rho(a) = \rho^{-1}(a)$ for all letters $a \in \mathbb{A}$, then $\rho^2(a) = \rho\rho(a) = \rho\rho^{-1}(a) = a$ and hence $\rho^2 = \text{id}$ is the identical permutation, which maps each letter into itself. Then ρ is called an *involution*. The permutations given by the Enigma rotors and plugboard are involutions, in particular our A, B, C, D, E , and F . We note that $(\rho\sigma)^{-1} = \sigma^{-1}\rho^{-1}$, since

$$\sigma^{-1}\rho^{-1}(\rho\sigma) = \sigma^{-1}\rho^{-1}\rho\sigma = \sigma^{-1}\sigma = \text{id};$$

we have used the associativity, and the uniqueness of an inverse. In other words, the inverse of a product is the product of the inverses, but in the inverse order! There are two useful data structures to represent a permutation σ . The first is a *table of values* of σ :

$$(G.1) \quad \begin{array}{c|cccccccccccccccccccccccc} \mathbf{a} & \mathbf{A} & \mathbf{B} & \mathbf{C} & \mathbf{D} & \mathbf{E} & \mathbf{F} & \mathbf{G} & \mathbf{H} & \mathbf{I} & \mathbf{J} & \mathbf{K} & \mathbf{L} & \mathbf{M} & \mathbf{N} & \mathbf{O} & \mathbf{P} & \mathbf{Q} & \mathbf{R} & \mathbf{S} & \mathbf{T} & \mathbf{U} & \mathbf{V} & \mathbf{W} & \mathbf{X} & \mathbf{Y} & \mathbf{Z} \\ \hline \sigma(\mathbf{a}) & \mathbf{C} & \mathbf{I} & \mathbf{S} & \mathbf{K} & \mathbf{V} & \mathbf{A} & \mathbf{B} & \mathbf{M} & \mathbf{W} & \mathbf{E} & \mathbf{G} & \mathbf{T} & \mathbf{Y} & \mathbf{U} & \mathbf{R} & \mathbf{X} & \mathbf{P} & \mathbf{Q} & \mathbf{Z} & \mathbf{L} & \mathbf{N} & \mathbf{H} & \mathbf{D} & \mathbf{O} & \mathbf{J} & \mathbf{F} \end{array}$$

The second one is the *cycle decomposition*. It is obtained by taking the first letter A , then $\sigma(A)$, then $\sigma^2(A)$, and so on until we come back to A : $\sigma^i(A) = A$.

These values form the first cycle $(A \sigma(A) \sigma^2(A) \cdots \sigma^i(A))$. Then the first letter not occurring here is taken, say B, and the cycle generated by B is formed. This is continued until all elements are exhausted.

We usually write the cycles in order of decreasing length, and order those of the same length alphabetically by the smallest element occurring in them. Thus σ as in (G.1) has the cycle decomposition

$$(G.2) \quad (BIWDKG) (EVHMYJ) (ACSZF) (ORQPX) (LT) (NU)$$

The *cycle structure* of σ is the sequence of cycle lengths in this representation, $(6, 6, 5, 5, 2, 2)$ in the example.

A cycle (a) of length 1 is a *fixed point* of σ . A cycle (ab) of length 2 is called a *transposition* and has the special property that $(ab)^2 = \text{id}$. More generally, the permutations σ with cycle structure $(2, \dots, 2, 1, \dots, 1)$, so that only transpositions and fixed points occur, are precisely those with the property that $\sigma^2 = \text{id}$, that is, the involutions σ .

Now we suppose that we see the encryption DZVUFA in some intercepted message, as recorded as number 8 among the 42 messages numbered $0, \dots, 41$ in Table G.1. Then D and U are encodings of the same (unknown) letter x by the two permutations A and D , respectively. Here x is the first letter of the message key. In other words, $A(x) = D$ and $D(x) = U$ for some unknown letter x . But then also $A(D) = x$, and $DA(D) = U$. Thus any intercepted message DZVUFA tells us that

$$DA(D) = U, \quad EB(Z) = F, \quad FC(V) = A.$$

We have thus obtained one value each of the three compositions DA , EB , and FC . If we have sufficiently many of these single values, we have the three permutations DA , EB , and FC completely in our hands. This is called the *characteristic* of the given day. Its determination from intercepts was the first step in the Polish solution of the rotor wirings.

As an example, we determine the first cycle of DA as follows:

x	A	O	B	N	P	K	M	F	Q	Y	V	T	R
$DA(x)$	O	B	N	P	K	M	F	Q	Y	V	T	R	A
k	0	25	3	24	26	20	23	11	28	39	35	33	29

An entry corresponds to the message number k ; thus the second entry $DA(0) = B$ is derived from message number 25. One finds the second cycle in the same way, as well as the cycle representations of the other two permutations:

$$(G.3) \quad \begin{aligned} DA &= (AOBNPKMFQYVTR) (CHLDUGIJZWEXS), \\ EB &= (BIWDKG) (EVHMYJ) (ACSZF) (ORQPX) (LT) (NU), \\ FC &= (AGIUZKRWJLBMV) (CQTYSXFOHNEPD). \end{aligned}$$

The cycle lengths are $(13, 13)$ for DA and FC , and $(6, 6, 5, 5, 2, 2)$ for EB which is the permutation (G.1). A general theorem of Rejewski says that in any such product of involutions each cycle length appears an even number of times; this certainly happens for our three permutations.

How can we get the individual permutations, like A , from the characteristic? If the system is properly used, then there is no easy way of doing so. But—fortunately for the Polish mathematicians—the German operators did not follow the rule of choosing message keys at random, but had a small set of preferred keys: three repeated letters, like JJJ, or three letters adjacent on the keyboard, usually from the outside towards the inside, like SDF, or three-letter female names like EVA. In a sufficiently large set of intercepts, there would then be repetitions: two operators had chosen the same key. The cryptanalyst takes one of those repetitions and assumes it to be one of the “preferred” keys. We will now see how to compute the involutions A, \dots, F from this assumption, and also that we get a way of checking its correctness.

This approach illustrates an important tool of the Polish and (later) British cryptanalysis: the *known-plaintext attack*, called a *crib* in those days. Here the 3-letter message key was not chosen at random, but with heavy preference on particular keys. At later stages of the decryption, there were stereotyped beginnings or endings of messages, such as salutations, signatures, or texts such as weather messages or ship positions. In fact, at some point the British laid mines near the German-occupied French coast just in order to intercept Enigma-encrypted messages from German minesweepers. Their text could be guessed, and then decipherment of these (uninteresting) messages yielded the (highly interesting) daily Enigma keys.

So suppose that some of the intercepts in Table G.1 have been intercepted several times, say the PICKWQ. The cryptanalyst now makes the assumption that it corresponds to one of the “popular” keys, say that the message key generating them is JJJ. Thus $A(J) = P$. From this simple assumption about just a single value, the whole permutations unravel by magic. Namely, we also have $A(P) = J$, by the involutory property of A , and hence $D(P) = DA^2(P) = DA(J) = Z$. We present the start of the unravelling in the following diagram.

	A	D
1	J → P	
2	P → J	
3	J →	Z
4		P → Z
5		Z → P
6	N →	P
7	N → Z	
8	Z → N	
9	Z →	W
10		N → W

Lines 1 through 4 have been explained. Lines 5 and 8 follow from 4 and 7, respectively, because A and D are involutions. Lines 3, 6, and 9 are part of the characteristics, with lines 3 and 9 occurring in the second cycle of DA , and line 6 in the first one; see (G.3). Lines 7 and 10 are new; line 7 is deduced as above:

$$A(N) = D^2 A(N) = D(DA(N)) = D(P) = Z.$$

This process can now be repeated, and concludes the second step of the cryptanalysis. The first four permutations are determined as:

$A = (AX) (BW) (CT) (DQ) (EO) (FU) (GM) (HV) (IK) (JP) (LY) (NZ) (RS)$
 $B = (AQ) (BE) (CR) (DM) (FP) (GV) (HK) (IJ) (LN) (OS) (TU) (WY) (XZ)$
 $C = (AH) (BP) (CJ) (DL) (EM) (FI) (GO) (KY) (NV) (QW) (RT) (SZ) (UX)$
 $D = (AS) (BE) (CR) (DY) (FG) (HT) (IM) (JK) (LV) (NW) (OX) (PZ) (QU)$

As an example, we can verify the first entry of DA in (G.3):

$$DA(A) = D(A(A)) = D(X) = O.$$

We now know the six permutations A, \dots, F , and next see how we can determine the wiring of the rightmost Enigma rotor. In the Enigma block diagram (Figure?), if one of the keyboard keys in k is struck, current flows through the plugboard (*Steckerbrett*) S , then through the three movable rotors N , M , and L , is reflected at the fixed rotor R , goes back through L , M , N , and S , and finally lights a lamp \otimes . Using the same letters for the corresponding permutations on \mathbb{A} , we have

$$(G.4) \quad A = S^{-1}N^{-1}M^{-1}L^{-1}RLMNS.$$

The rotor N turns by 1 after every key stroke, the rotor M after 26 strokes, and L after 26^2 strokes—as in an odometer. The positions where this happens are set by the daily key, in a random fashion. For the cryptanalysis, we assume that the first five key strokes do not provoke a movement of M , and therefore

not of L , either. This happens for 21 out of the 26 possibilities, which is good enough for our purposes. We can therefore abbreviate

$$(G.5) \quad Q = M^{-1}L^{-1}RLM,$$

and have

$$(G.6) \quad A = S^{-1}N^{-1}QNS.$$

Figure ? shows the flow A of current through the whole system at the top, when J is typed on the keyboard. At the bottom is the same picture for the second permutation B . Now the rotor N has moved by one position, and we show again the keystroke J. Figure? shows the same situation, but now using our abbreviation Q . We can describe B easily using the cyclic shift

$$P = (\text{ABCDEFGHIJKLMNOPQRSTUVWXYZ}).$$

Namely, after S comes P , then the old rotor N , then the downshift P^{-1} , and the similarly on the way back. That is,

$$(G.7) \quad B = S^{-1}P^{-1}N^{-1}PQP^{-1}NPS.$$

In the same way, we have

$$(G.8) \quad \begin{aligned} C &= S^{-1}P^{-2}N^{-1}P^2QP^{-2}NP^2S, \\ D &= S^{-1}P^{-3}N^{-1}P^3QP^{-3}NP^3S. \end{aligned}$$

There are two more equations, for E and F , which we do not need at the moment. We know the left-hand sides of the four equations (G.6) – (G.8), but it is not clear how to determine S , N , and Q efficiently from them.

Next comes a further non-mathematical tool in cryptanalysis, besides the cribs. Namely, old-fashioned espionage.

The story of the German traitor Asché is related in ?. He provided much secret material to Colonel? Bertrand of the French Secret Service. Among it were the daily Enigma keys for some period in 1932, including the plugboard connections S . Enough intercepted messages were available from those days, and now S , and also P , can be brought to the left-hand side of the equations for A , B , C , and D :

$$(G.9) \quad \begin{aligned} U &= SAS^{-1} &= N^{-1}QN, \\ V &= PSBS^{-1}P^{-1} &= N^{-1}PQP^{-1}N, \\ W &= P^2SCS^{-1}P^{-2} &= N^{-1}P^2QP^{-2}N, \\ X &= P^3SDS^{-1}P^{-3} &= N^{-1}P^3QP^{-3}N. \end{aligned}$$

The left-hand sides are known, as is P , and we want to determine N . The solution requires some further notions about permutations, which we now introduce.

If ρ , σ , and τ are permutations of the alphabet \mathbb{A} with $\rho = \tau\sigma\tau^{-1}$, then ρ is a *conjugate* of σ . Suppose that $\sigma(a) = b$. Then

$$\rho(\tau(a)) = \rho\tau(a) = \tau\sigma\tau^{-1}\tau(a) = \tau\sigma(a) = \tau(b).$$

Thus if (x_1, x_2, \dots, x_k) is a cycle of σ , so that $\sigma(x_i) = x_{i+1}$ for all i , including $\sigma(x_k) = x_1$, then $(\tau(x_1), \tau(x_2), \dots, \tau(x_k))$ is a cycle of ρ . In particular, ρ and σ have the same cycle structure.

The cycle structure of an involution consists of some transpositions, like (ab) , and fixed points, like (c) . If six connecting cables are used for the plug-board, then S is the product of six transpositions and $26 - 2 \cdot 6 = 14$ fixed points.

Example!

The Enigma rotors did not have any fixed points, so that they consist of 13 transpositions. Equations (G.4) through (G.8) imply that A, B, C, D and Q are conjugates of R , and hence also products of 13 (disjoint) transpositions.

Pretending that we knew Q , the four equations (G.9) are of the form

$$(G.10) \quad \rho = \tau^{-1}\sigma\tau,$$

where ρ and σ are known and $\tau = N$ is unknown. Our solution will be by enumerating all possibilities for τ . How many are there? To start with the worst case, if $\rho = \sigma = \text{id}$, then (G.10) collapses to nothing and all $26!$ permutations are possible for τ . If ρ and σ are products of 13 disjoint transpositions, there are $2^{13} \cdot 13! = 51\,011\,754\,393\,600 \approx 5 \cdot 10^{13}$ possibilities for τ (see ??), far too many for our purposes. However, a simple trick both eliminates the unknown Q and cuts down substantially the number of possible τ .

Namely, we multiply the equations in (G.9) together in sequence:

$$\begin{aligned} UV &= N^{-1} QPQP^{-1}N, \\ VW &= N^{-1}P QPQP^{-2}N, \\ WX &= N^{-1}P^2QPQP^{-3}N. \end{aligned}$$

We eliminate the unknown QPQ by plugging in UV and VW :

$$\begin{aligned} VW &= N^{-1}PNUVN^{-1}P^{-1}N = (N^{-1}PN)(UV)(N^{-1}PN)^{-1}, \\ WX &= N^{-1}PNVWN^{-1}P^{-1}N = (N^{-1}PN)(VW)(N^{-1}PN)^{-1}. \end{aligned}$$

Thus $VW = \tau UV \tau^{-1}$ is a conjugate of UV , and we determine all possible conjugations τ . For each τ , we also check whether $WX = \tau VW \tau^{-1}$, and keep only those which pass the test. There are two further equations—which we did not write down—that can be used as tests.

Only a few values, often a single value, of τ will survive those tests. We solve $\tau = N^{-1}PN$ for N . Since P is a single cycle of length 26, there are exactly

26 solutions. There will be a few, often just one, values of N that are a product of 13 disjoint transpositions. This is then the wiring of the right-hand Enigma rotor!

The German procedures for the Enigma included a random placement of the three (later five and eight) rotors into the three (later four) positions. Thus each rotor occurred reasonably often as the rightmost one, and they could all be broken by Rejewski's method.

In the course of the war, several Enigma machines were captured by the British (and by the Russians at Stalingrad), and their rotor wiring was no secret anymore. But Rejewski's early break into the rotors was an important link in the chain leading to Ultra.

Acronyms

AES Advanced Encryption Standard	MD4 Message Digest 4
ATM Automatic Teller Machine	MD5 Message Digest 5
CBC Cipher Block Chaining	NBS National Bureau of Standards
CESG Communications-Electronics Security Group	NIST National Institute of Standards and Technology
CFB Cipher Feedback	NSA National Security Agency
DEC Digital Equipment Corporation	OFB Output Feedback
DES Data Encryption Standard	PIN Personal Identification Number
DSA Digital Signature Algorithm	PKCS Public Key Cryptography Standard RSA Inc. issued some of these.
DSS Digital Signature Standard	PRG Pseudo Random number Generator
ECB Electronic Codebook	RSA Rivest, Shamir and Adleman Cryptosystem
EFF Electronic Frontiers Foundation	RC6
FIPS Federal Information Processing Standard	SHA Secure Hash Algorithm
IBM International Business Machines	SHS Secure Hash Standard
IDEA International Data Encryption Algorithm	TDEA Triple Data Encryption Algorithm
MARS A candidate cipher for AES. missing long name	

Bibliography

The numbers in brackets at the end of a reference are the pages on which it is cited. Names of authors and titles are usually given in the same form as on the article or book.

FRIEDRICH L. BAUER (1995). *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie*. Springer-Verlag. English translation: *Decrypted Secrets. Methods and Maxims of Cryptology*, 1996.

COUNT BERNSTORFF (1920). *My three years in America*. Charles Scribner's sons, New York. [111]

GUSTAVE BERTRAND (1973). *Enigma—ou la plus grande énigme de la guerre 1939-1945*. Librairie Plon, Paris. 295, [5] pages. 32 pages.

ELI BIHAM & ADI SHAMIR (????). Differential Cryptanalysis of DES-like Cryptosystems. In *Advances in Cryptology: Proceedings of CRYPTO '90*, Santa Barbara CA, A. J. MENEZES & S. A. VANSTONE, editors, number 537 in Lecture Notes in Computer Science, 2–21. Springer-Verlag, Berlin. ISSN 0302-9743. URL <http://link.springer.de/link/service/series/0558/tocs/t0537.htm>.

ELI BIHAM & ADI SHAMIR (1991). Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology* **4**, 3–72.

ELI BIHAM & ADI SHAMIR (1992). Differential Cryptanalysis of the Full 16-round DES. In *Advances in Cryptology: Proceedings of CRYPTO '92*, Santa Barbara CA, ERNEST F. BRICKELL, editor, number 740 in Lecture Notes in Computer Science, 487–496. Springer-Verlag. ISSN 0302-9743.

BERNHARD BISCHOFF (1931). Wer ist die Nonne von Heidenheim? *Studien und Mitteilungen zur Geschichte des Benediktiner=Ordens und seiner Zweige, Neue Folge* **18**, 387–388.

BERNHARD BISCHOFF (1954). Übersicht über die nichtdiplomatischen Geheimschriften des Mittelalters. *Mitteilungen des Instituts für österreichische Geschichtsforschung* **62**, 1–27. Reprint by Hermann Böhlaus Nachf., Graz/Köln, 1954. Also reprinted in *Mittelalterliche Studien*, 1981, volume 3, pages 120–148.

FRIEDERICH JOHANN BUCK (1772). *Mathematischer Beweis: daß die Algebra zur Entdeckung einiger verborgener Schriften bequem angewendet werden könne*. Königsberg. [34]

PIERRE COCHON (1870). *Chronique Normande*. A. Le Brument, Rouen. Edited by Ch. de Robillard de Beaurepaire.

CLAUDE COMIERS (1690). *L'Art d'Écrire et de Parler Occultement et sans Soupçon*. Michel Guerout, Paris, 72.

CLAUDE COMIERS (1691). *Traité de la parole, langues, et écritures, contenant la stéganographie impénétrable, ou L'art d'écrire et de parler occultement*. Jean Léonard, Bruxelles, 16, 276.

THOMAS H. CORMEN, CHARLES E. LEISERSON & RONALD L. RIVEST (1990). *Introduction to Algorithms*. MIT Press, Cambridge MA. ISBN 0-262-03141-8, xx+1028.

MICHAEL J. COWAN (2004). Rasterschlüssel 44—The Epitome of Hand Field Ciphers. *Cryptologia* **XXVIII**(2), 115–148.

C. A. DEAVOURS (1981). The Black Chamber: A Column Shutting off the Spigot in 1981. *Cryptologia* **5**(1), 43–45. ISSN 01611194. [2]

DEUTSCHE NATIONALVERSAMMLUNG (editor) (1920). *Stenographische Berichte über die öffentlichen Verhandlungen des 15. Untersuchungsausschusses der Verfassungsgebenden Nationalversammlung nebst Beilagen*, volume II. Verlag der Norddeutschen Buchdruckerei und Verlagsanstalt, Berlin.

J.-P. DEVOS (1946). La cryptographie espagnole durant la seconde moitié du XVI^e siècle et le XVII^e siècle. In *Miscellanea historica in honorem Alberti de Meyer*, volume 2, 1025–1035.

J. P. DEVOS (1950). *Les chiffres de Philippe II (1555-1598) et du despacho universal durant le XVII^e siècle*. Palais des Académies, Bruxelles. [79]

WHITFIELD DIFFIE & MARTIN E. HELLMAN (1976). New directions in cryptography. *IEEE Transactions on Information Theory* **IT-22**(6), 644–654. [1]

A. W. EWING (1939). *The Man of Room 40, The Life of Sir Alfred Ewing*. Hutching & Co. Ltd., 295 pages.

PENELOPE FITZGERALD (1977). *The Knox Brothers*. Macmillan London Limited, 294 pages.

OLE IMMANUEL FRANKSEN (1984). *Mr. Babbage's Secret. The Tale of a Cipher— and APL*. Strandberg, Birkerød, Denmark. [59]

OLE IMMANUEL FRANKSEN (1993). Babbage and cryptography. Or, the mystery of Admiral Beaufort's cipher. *Mathematics and Computers in Simulation* **35**, 327–367. [61]

WILLIAM F. FRIEDMAN (1936). Edgar Allan Poe, cryptographer. *Signal Corps Bulletin* **97**, 41–53. Also in *Cryptography and cryptanalysis articles*, ed. William F. Friedman, 1936, reprinted 1976 by Aegean Park Press, Laguna Hills CA, pp. 145–156.

WILLIAM F. FRIEDMAN (1937). Edgar Allan Poe, cryptographer (Addendum). *Signal Corps Bulletin* **98**, 54–72. Also in *Cryptography and cryptanalysis articles*, ed. William F. Friedman, c. 1938, reprinted 1976 by Aegean Park Press, Laguna Hills CA, 167–189.

WILLIAM F. FRIEDMAN & CHARLES J. MENDELSON (1938). *The Zimmermann Telegram of 16 January 1917, and its Cryptographic Background*. War Department, Office of the Chief Signal Officer, US Government Printing Office, Washington DC, [8], 54, [3] pages. Reprint 1976 and 1994 by Aegean Park Press, Laguna Hills CA. [101, 111]

FRUS (1931). *Papers Relating to the Foreign Relations of the United States—1917, Supplement 1: The World War*. U.S. Government Printing Office, Washington.

HELEN FOUCHE GAINES (1956). *Cryptanalysis: a study of ciphers and their solution*. Dover Publications, Inc. [38]

JOACHIM VON ZUR GATHEN (2004). Friederich Johann Buck: arithmetic puzzles in cryptography. *Cryptologia* **XXVIII**(4), 309–324. URL <http://dx.doi.org/10.1080/0161-110491892953>. [34]

JOACHIM VON ZUR GATHEN & JÜRGEN GERHARD (2003). *Modern Computer Algebra*. Cambridge University Press, Cambridge, UK, 2nd edition. ISBN 0-521-82646-2, 800. URL <http://cosec.bit.uni-bonn.de/science/mca.html>. First edition 1999.

BURTON J. HENDRICK (1922). *The Life and Letters of Walter H. Page*. Doubleday, Page & Company, Garden City NY. 3 volumes. [111]

BURTON J. HENDRICK (1925). *The Life and Letters of Walter H. Page*, volume III. William Heinemann Ltd., London, vii, 440 pages.

F. H. HINSLEY *et al.* (1984). *British Intelligence in the Second World War*. Her Majesty's Stationary Office, London. ISBN 978-0116309334, 978-0116309341, 0-11-630935-0, 978-0116309525, 978-0116309549.

COLONEL HOUSE (1926). *The Intimate Papers of Colonel House. Volume II. From Neutrality to War 1915-1917. Arranged as a narrative by Charles Seymour.* Ernest Benn Limited. [111]

ADMIRAL SIR WILLIAM JAMES (1956). *The Eyes of the Navy: A Biographical Study of Admiral Sir William Hall.* Methuen & Co. Ltd., London. xxv, 212 pages. [112]

R. V. JONES (1979). Alfred Ewing and 'Room 40'. *Notes and Records of the Royal Society of London* **34**, 65–90.

DAVID KAHN (1967). *The Codebreakers.* The Macmillan Company, New York. xvi, 1164 pages. [19, 111]

DAVID KAHN (1991). *Seizing the Enigma.* Houghton Mifflin Company, Boston.

DAVID KAHN (1999). Edward Bell and his Zimmermann Telegram Memoranda. *Intelligence and National Security* **14**(3), 143–159. ISSN 0268-4527. [106, 111]

F. W. KASISKI (1863). *Die Geheimschriften und die Dechiffir-Kunst.* E. S. Mittler und Sohn, Berlin. viii + 95 pp. + 6 tables. [59, 61, 67]

THOMAS KELLY (1998). The myth of the skytale. *Cryptologia* **XXII**(3), 244–260.

DONALD E. KNUTH (1997). *The Art of Computer Programming, vol. 1, Fundamental Algorithms.* Addison-Wesley, Reading MA, 3rd edition. First edition 1969.

ROBERT LANSING (1935). *War Memoirs.* Bobbs-Merrill, Indianapolis and New York, 383 pages.

J. H. LEOPOLD (1900). De scytala laconica. *Mnemosyne* **2**, 365–391.

WILHELM LEVISON (1946). *England and the continent in the eighth century.* Clarendon Press.

CHARLES J. MENDELSON (1939). Cardan on cryptography. *Scripta Mathematica* **6**, 157–168.

CARL H. MEYER & STEPHEN M. MATYAS (1982). *Cryptography: A new Dimension in Computer Data Security.* John Wiley & Sons. [38]

A. RAY MILLER (2001). The Cryptographic Mathematics of Enigma. In *NSA Historical Publications*, 6. Public and Media Affairs Office.

WALTER MILLIS (1935). *Road to War. America: 1914–1917.* Houghton Mifflin Company, Boston and New York, xiv, 466 pages. [101, 111]

- H. MORANVILLÉ (editor) (1891). *Chronographia Regum Francorum*, volume 2.
- GEORG ALEXANDER VON MÜLLER (1959). *Regierte der Kaiser?* Edited by Walter Görlitz. Musterschmidt-Verlag, Göttingen, 455 pages.
- BVT. BRIG. GEN. ALBERT J. MYER (1879). *Manual of Signals for the Use of Signal Officers in the Field and for Military and Naval Students, Military Schools, etc.* Government Printing Office, Washington. [27]
- MONI NAOR & ADI SHAMIR (1995). Visual cryptography. In *Advances in Cryptology: Proceedings of EUROCRYPT 1994*, Perugia, Italy, ALFREDO DE SANTIS, editor, number 950 in Lecture Notes in Computer Science, 1–12. Springer-Verlag. ISBN 3-540-60176-7. ISSN 0302-9743. [1, 16]
- MARTIN NASSUA (1992). “Gemeinsame Kriegsführung. Gemeinsamer Friedensschluß.” *Das Zimmermann-Telegramm vom 13. Januar 1917 und der Eintritt der USA in den 1. Weltkrieg*, volume 520 of *Europäische Hochschulschriften, Reihe III, Geschichte und ihre Hilfswissenschaften*. Peter Lang, Frankfurt am Main, [8], 163 pages. [111]
- DAVID PAULL NICKLES (2003). *Under the Wire - How the Telegraph Changed Diplomacy*. Harvard University Press, Cambridge, Massachusetts, & London, England.
- P.-M. PERRET (1890). Les règles de Cicco Simonetta. *Bibliothèque de l'École des Chartes* **51**, 515–525. *Revue d'Érudition*.
- EDGAR ALLAN POE (1902). *The Gold Bug*. Rand, McNally & Company, Chicago, New York, London. Edited by Theda Gildemeister, Illustrated by G. C. Widney.
- R. L. RIVEST, A. SHAMIR & L. M. ADLEMAN (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM* **21**(2), 120–126.
- SECOUSSE (1755). *Recueil de pièces servant de preuves aux mémoires Sur les Troubles excités en France par Charles II. Dit le mauvais. Roi de Navarre et comte d'Evreux*. Durand, 677 pages.
- G. J. (WILLEM JACOB) VAN S'GRAVESANDE (1748). *Introduction à la philosophie, contenant la métaphysique, et la logique*. Jean and Herm. Verbeek, Leiden. [10], 472, [blank] pages. [46]
- C. E. SHANNON (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal* **28**, 656–715. [20]

SIGNAL SECURITY AGENCY (1945). German Cryptographic Systems During the First World War. Prepared under the Direction of the Chief Signal Officer. Now in the National Archives, Washington, NARA RG 459 Historical Cryptographic Collection, Box 1059; Folder German Cryptographic Systems During WWI.

DAVID STEVENSON (2004). *Cataclysm - the First World War as political tragedy*. Basic Books, Perseus Books Group, xix, [20], 564 pages.

FRENCH STROTHER (1918). German Codes and Ciphers. *The World's Work* **36**, 143–153. [112]

GEORG SWARZENSKI (1969). *Die Regensburger Buchmalerei des X. und XI. Jahrhunderts*. Anton Hiersemann, Stuttgart, 228 pages.

JACQUES-AUGUSTE DE THOU (1734). *Histoire Universelle*. Translated from 1604 Latin original. London.

FRANCESCO TRANCHEDINO (1970). *Diplomatische Geheimschriften*. Akademische Druck- und Verlagsanstalt, Graz-Austria, 43, 338 pages.

JOHANNES TRITHEMIUS (1561). *Polygraphie, et Vniuerselle escripture Cabalistique de M. I. Tritheme Abbé, traduite par Gabriel de Collange, natif de Tours en Auuergne*, volume [18]. Jacques Kerver, Paris, 300 leaves.

BARBARA W. TUCHMAN (1958). *The Zimmermann Telegram*. Macmillan Publishing Company, New York. xii, 244 pages. [111]

A. M. TURING (1937). On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society, Second Series* **42**, 230–265, and **43**, 544–546.

JULES VERNE (1881). La Jangada. *Magasin d'éducation et de récréation* **33**.

STEPHANIE WEST (1988). Archilochus' Message-Stick. *Classical Quarterly* **38**, 42–48.

JOHN WILKINS (1641). *Mercury or, the Secret and Swift Messenger. Shewing how a man may with privacy and speed communicate his thoughts to a friend at a distance*. Printed by I. Norton for John Maynard and Timothy Wilkins, London. 172 pages.

JOHN WILKINS (1802). *The Author's Life, and an Account of his Works*. C. Whittingham, London. In two volumes.

W. K. WIMSATT, JR. (1943). What Poe knew about cryptography. *Publications of the Modern Language Association of America* **58**, 754–779. [46]

FILSON YOUNG (1922). *With the Battle Cruisers*. Cassell and Company, Ltd., London, New York, Toronto, Melbourne. [18], 296 pages.

Players

The numbers in brackets at the end of a reference are the pages on which it is cited. Names of authors and titles are usually given in the same form as on the article or book.

ALBERTI (????). [26, 34, 117]

CHANDLER P. ANDERSON (????).

GIOVANNI BATISTA ARGENTI (????). [38]

AUGUSTUS (????). [30, 36, 37, 58, 88]

CHARLES BABBAGE (????). [59, 61]

ARTHUR JAMES BALFOUR (????). [109]

BAZERIES (????).

EDWARD BELL (????). [109, 111]

THEOBALD VON BETHMANN HOLLWEG (????). [103, 113]

GAIUS IULIUS CAESAR (100 B.C.-44 B.C.). *B.C.13 July 100, Rom, Italy.
†B.C.15 March 44, Rom, Italy. URL http://de.wikipedia.org/wiki/Gaius_Iulius_Caesar. [20, 24, 30, 36, 37, 58, 61, 62, 66, 73, 88]

VENUSTIANO CARRANZA (????). [96, 100, 101, 112, 114, 115]

WINSTON CHURCHILL (????). [94]

CLAUDE COMIERS (????). [57]

DON COPPERSMITH (????). URL http://en.wikipedia.org/wiki/Don_Coppersmith.

ARVID GERHARD DAMM (????). [120]

ALASTAIR DENNISTON (????). [95]

DEVOS (????).

PORFIRIO DÍAZ (????). [112]

WHITFIELD . DIFFIE (1944-). *5 June 1944. URL http://de.wikipedia.org/wiki/Whitfield_Diffie. [35]

HEINRICH J. F. VON ECKARDT (????). [96, 100, 106, 107, 113, 114]

EMMERAN (????). [31]

GONZALO C. ENRILE (????). [112]

JAMES ALFRED EWING (????). [95, 112]

WILLIAM F. FRIEDMAN (????). [45, 61]

GALIBIN (????). [94, 95]

AULES GELLIUS (????). [37]

KURT GÖDEL (????).

GEORGE R. GRAHAM (????).

GREGORIUS (????). [38]

NIGEL DE GREY (????). [106, 107, 108, 109, 110, 111]

R. W. GRISWOLD (????).

HENRI DE GUISE (????). [76]

RICHARD HABENICHT (????). [94]

REGINALD HALL (????). [107, 108, 109, 112]

HARRISON (????).

EDWARD HUGH HEBERN (????). [120]

ADOLF HITLER (????). [123]

E. M. HOOD (????). [109]

EDWARD MANDELL HOUSE (????). [103]

FELIPE II (????). [76, 81]

JEFFERSON (????).

KASISKI (????). [iii, 26, 34, 61, 62, 64, 66, 68, 70, 71, 72]

HANS ARTHUR VON KEMNITZ (????). [101, 113]

KERCKHOFF (????). [121]

KERENSKI (????). [110]

ALFRED DILLWYN (DILLY) KNOX (????). [106, 108]

HUGO ALEXANDER KOCH (????). [120]

ROBERT LANSING (????). [107, 108, 109]

LEMOINE (????). [123]

LENIN (????). [110]

TITUS LIVIUS (????).

CHARLES DE LORRAINE (????). [76]

J. R. LOWELL (????).

LYSANDROS (????). [87, 88]

KARL MEUSEL (????). [105]

GIOVANNI MOCENIGO (????). [81]

ADOLF GRAF MONTGELAS (????). [101, 113]

WILLIAM MONTGOMERY (????).

JUAN MOREO (????). [76, 78, 79, 81, 85]

SAMUEL MORSE (????).

BERND MÜTTER (????).

ALBERT C. MYER (????). [30]

NEWTON (????).

HENRY OLIVER (????). [95]

WALTER HINES PAGE (????). [96, 108, 109, 111]

PLAYFAIR (????). [22, 26]

PLUTARCH (????). [87, 88]

EDGAR ALLAN POE (????). [41, 45, 46]

POLYBIOS (????). [27, 29, 30]

GIOVANNI BATTISTA DELLA PORTA (????). [71, 72]

PRINZ HEINRICH VON PREUSSEN (????). [95]

RAMWOLD (????). [31, 33]

MARIAN REJEWSKI (????). [123, 128, 132]

CHARLES ROTTER (????). [95]

JOSEPH SAILER (????).

KLAUS SAUL (????).

ARTHUR SCHERBIUS (????). [120]

WILLEM JACOB S'GRAVESANDE (????).

CLAUDE SHANNON (????). [35, 46, 47, 48, 49, 50, 52]

CICCO SIMONETTA (????). [75]

SIXTUS (????). [38]

FRANCIS O. J. SMITH (????).

HELLMUTH FREIHERR LUCIUS VON STOEDTEN (????). [112]

WILHELM AUGUST VON STUMM (????). [101]

PIERRE DU TERTRE (????). [74, 75]

FRANCESCO TRANCHEDINO (????). [75]

GAIUS SUETONIUS TRANQUILLUS (????). [36, 37]

JOHANNES TRITHEMIUS . (1462-1516). *1 February 1462, Trittenheim, Germany. †13 December 1516, Würzburg, Germany. URL <http://de.wikipedia.org/wiki/Trithemius>. [34, 35, 58]

ALAN TURING (????). [iv, 117, 118, 120, 122, 123, 124, 126, 128, 130, 132, 134]

CHARLES DE VALOIS (????). [74]

CÁNDIDO AGUILAR VARGAS (????). [114]

GILBERT SANDFORD VERNAM (????). [35]

VERNE (????). [89, 90, 91]

FRANÇOIS VIÈTE (????). [78, 81, 83]

BLAISE DE VIGENÈRE (1523-1596). *15 April 1523, Saint-Pourçain, France.
†1596. URL [http://de.wikipedia.org/wiki/Blaise_de_Vigen\C3\A8re](http://de.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re). [iii,
20, 21, 25, 26, 34, 35, 47, 58, 59, 61, 62, 64, 66, 68, 70, 71, 72]

WILKINS (????). [89]

WILLIBALD (????). [31]

N. P. WILLIS (????).

THOMAS WOODROW WILSON (????). [93, 96, 103, 108, 109, 110, 111, 112, 115]

WYNNEBALD (????). [31]

FILSON YOUNG (????). [96]

ZIMMERMANN (????). [iii, 73, 82, 93, 94, 96, 97, 98, 100, 101, 102, 103, 104,
105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116]

