Joachim von zur Gathen (2003). Claude Comiers : the first arithmetical cryptography. *Cryptologia* **XXVII**(4), 339–349. URL https://dx.doi.org/10.1080/0161-110391891946.
This document is provided as a means to ensure timely dissemination of scholarly and technical work on a non-commercial basis. Copyright and all rights therein are maintained by the authors or by other copyright holders, notwithstanding that these works are posted here electronically. It is understood that all persons copying any of these documents will adhere to the terms and constraints invoked by each copyright holder, and in particular use them only for noncommercial purposes. These works may not be posted elsewhere without the explicit written permission of the copyright holder. (Last update 2017/1/29-18 :16.)

CLAUDE COMIERS: THE FIRST ARITHMETICAL CRYPTOGRAPHY

Joachim von zur Gathen

13th December 2002

Abstract. In 1690, the blind French author Claude Comiers described the Vigenère cipher as addition of a key to the plaintext, modulo the alphabet size. The concept of modular arithmetic was then unknown, but Comiers was well aware of its cyclic nature. This seems to be the earliest description of a cryptosystem in arithmetic terms.

1. Key addition systems

A popular type of cryptosystem throughout history was the various forms of "key-addition systems". 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

$$\begin{aligned} \text{ciphertext} &= \text{plaintext} + \text{key}, \\ \text{plaintext} &= \text{ciphertext} - \text{key}. \end{aligned} \tag{1}$$

More formally, we have letters from a fixed alphabet of some size m (in modern English, $m = 26$), and then the plaintext $x = (x_0, x_1, \ldots)$, the key $k = (k_0, k_1, \ldots)$, and the ciphertext $y = (y_0, y_1, \ldots)$ 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 $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$, that is, by doing arithmetic modulo m. The alphabet and $\mathbb{Z}_m$ are related in the (mathematically) natural way: $A \longleftrightarrow 0$, $B \longleftrightarrow 1, \ldots$.

Many ways of producing the required key have been employed. In a Caesar cipher, 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 $Z + k_0 = AA$). In his 1518 *Polygraphia*, Johannes Trithemius used this system with the alphabet in its usual order as the key: $k_i = i \operatorname{rem} m$ for all i, where $i \operatorname{rem} m$ is the

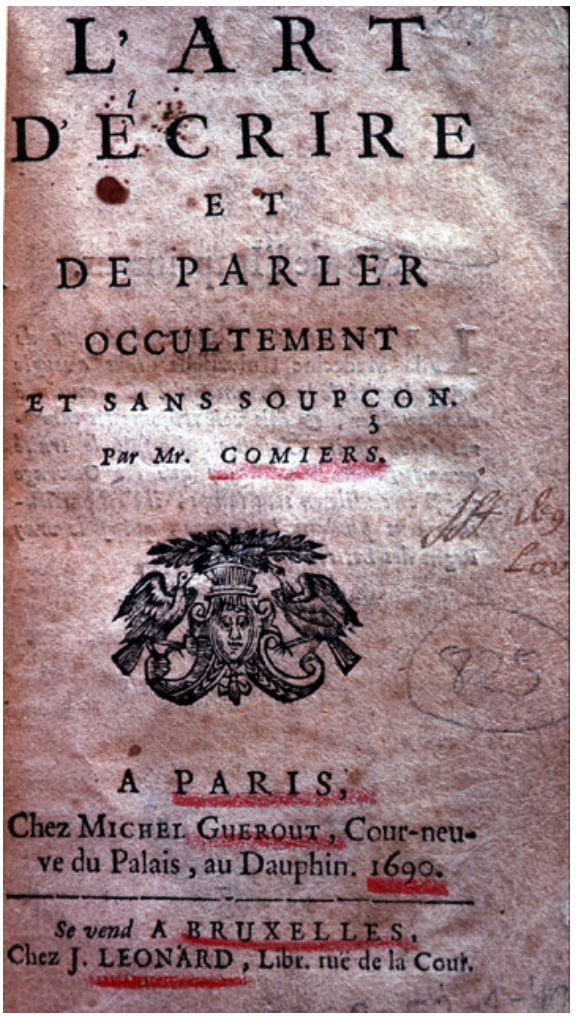

L'ART
D'ECRIRE
ET
DE PARLER
OCCULTEMENT
ET SANS SOUPCON.
Par Mr. COMIERS.
A PARIS,
Chez MICHEL GUEROUT, Cour-neuve du Palais, au Dauphin. 1690.
Se vend A BRUXELLES,
Chez J. LEONARD, Libr. rue de la Cour.

Figure 1: The title page of Comiers' book. The original size is 135 mm × 75 mm. Red underlining by hand.

nonnegative remainder of i on division by m (for example, $35 \operatorname{rem} 26 = 9$). In what is often called a "Vigenère cipher", one has a keyword $k_0, \ldots, k_{\ell-1}$ of some length ℓ, and repeats this as necessary: $k_i = k_{i \operatorname{rem} \ell}$ for all i. Following suggestions of Porta and Cardano, Vigenère proposed in his 1586 *Traicté des Chiffres* two autokey systems, where the next key letter is the previous letter of either the plaintext or the ciphertext:

$$k_i = x_{i-1}, \text{ or } k_i = y_{i-1}.$$

Admiral Sir Francis Beaufort suggested to use a fixed key, say $k'_0, \ldots, k'_{\ell-1}$, and then $k_i = -k'_i$ for $0 \le i < \ell$ in a standard "Vigenère cipher".

Modern variants, usually over the binary alphabet, are the *one-time pad* where k is a random sequence as long as the plaintext, and variations where one has an initial segment of the key (possibly random) and generates the remaining key letters in a pseudorandom fashion (Vernam, Siemens Geheimschreiber, Typex).

A systematic method for breaking the Vigenère system was published by Kasiski (1863). 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 (1), which he writes as

$$\text{Cypher} = \text{Key} + \text{Translation} - 1,$$
$$\text{Translation} = \text{Cypher} - \text{Key} + 1.$$

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

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

2. Claude Comiers

An interesting little booklet (Figure 1) appeared in 1690. Its author, Claude **Comiers d'Ambrun**, a professor of mathematics at Paris, wrote about many subjects, including cabbalistic topics, calendars, medicine, geology, comets, and cryptography. He was blind, and proud to point out his achievements. His sample message throughout the book is *Comiers avevgle Roial*[1] and the publisher's introduction says that *the scientist Mr. Comiers, although blind and mistreated by fortune, continues to work and show the light of his spirit.*[2] Comiers presents

[1] Comiers, royal blind man

[2] Le Sçavant Mr. Comiers [...] tout aveugle & maltraité de la fortune qu'il est, continuë de travailler, & fait voir toûjours les lumieres de son esprit.

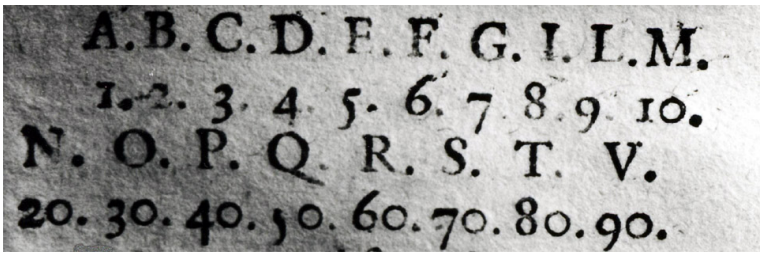


Figure 2: Comiers's 18-letter alphabet and coding

the first "arithmetization" of cryptography. He uses an 18-letter alphabet, and basically writes the Trithemius-Vigenère system as "ciphertext = cleartext + key", with the decryption rule "cleartext = ciphertext − key", computing modulo 18 in both cases.

In fact, he uses the coding of letters in Figure 2. Thus his two-digit number $10 \cdot k$ stands for $9 + k$, and he has a system of representation modulo 18. The fact that he starts at 1 rather than at 0 leads to his formulas

$$\begin{aligned} &\text{ciphertext} = \text{cleartext} \ -1+ \ \text{key}, \\ &\text{cleartext} = \text{ciphertext} \ +1- \ \text{key}. \end{aligned}$$

This is meant to be modulo 18, but, of course, he has neither the terminology nor the notation at his disposal, and has to make awkward distinctions between the first and the second half of his encoding numbers. Modular arithmetic was put on proper footing and given the modern notation by Gauß (1801).

He explains his decryption rule for one-digit letters (on his page 45) in the example "ciphertext $8 + 1 -$ key D (equal 4) = cleartext E":

> add 1 to the number received, and from the sum subtract the key digit. The result will indicate which letter of my alphabet is the cleartext letter. Say if $D = 4$ is the key letter and 8 is received, then you say $8 + 1 = 9$ which is the sum that the sender computed as the sum of the key letter D and the cleartext letter which is still unknown to you. That is why you write $9 - 4 = 5$, meaning that the cleartext letter is the fifth letter E of the alphabet.[3]

[3] *Ajoûtez l'unité au nombre envoyé, & de la somme ôtez-en le chifre du mot du guet, il restera le nombre qui indiquera la quantiéme lettre de mon Alphabet est la lettre du secret. Ainsi D.4. étant la lettre du mot du guet, & le chifre envoyé étant* 8. *dites* 8. *plus 1. égale* 9. *que vôtre amy avoit eu pour la somme du chifre de la lettre D. du mot du guet, & de la lettre du secret qui vous est encore inconnuë. C'est pourquoy dites* 9. *moins* 4. *égale* 5. *c'est à dire que la lettre du secret est la cinquiéme de l'Alphabet qui est la lettre E.*

Comiers also specifies the rules for two-digit letters; they are somewhat more complicated due to the clumsy encoding.

Comiers is well aware of the "cyclic" nature of addition modulo 18: *then take the alphabet of eighteen letters in their natural order, which you must conceive as being written like a rosary, or around the circumference of a circle.*[4] But because of his unfortunate representation, he expresses our $13 \equiv 9 + 1 - 15 \bmod 18$ as: *in order to know for which letter the number* 9 *was sent using the key letter* $R = 60$, *you count from* 60 *inclusive up to* 9, *also inclusive, saying* $60, 70, 80, 90, 1, 2, 3, 4, 5, 6, 7, 8, 9$. *You notice that you have counted thirteen letters, and hence the thirteenth letter* P *is the cleartext.*[5]

With hindsight, modular addition is already visible in Alberti's disk, but Comiers is the first one to relate this to the arithmetic notion. Comiers describes several cryptosystems, for example a monoalphabetic substitution given by a keyword followed by the letter-by-letter addition of another key word as superencipherment. He also addresses distributed cryptography. In order to share a secret among three recipients, he suggests giving one an encrypted version, and one half of the key each to the other two.

Comiers displays the usual inventor's pride in his additive cryptosystem:

> *. . . [the cipher] is nevertheless indecipherable by any human mind. Even if one gave to the decipherer the encryption of each letter, he would still have to guess the initial key element, and then guess the order of the alphabet which provided these encryptions by means of the number agreed upon as the key. You can easily try this out on those who pride themselves on being able to decipher; be it with Mr. Viète, the father of our symbolic algebra and the great decipherer of his times, if he could return to this world.*[6]

Comiers first published this work in the journal *Mercure Galant*, in the

[4] Ayez ensuite devant vous l'Alphabet de dix-huit lettres dans leur ordre naturel, que vous devez concevoir comme écrites en chapelet, ou autour de la circonference d'un cercle.

[5] Afin de connoître pour quelle lettre de l'Alphabet le chifre 9. a été envoyé par le moyen de la lettre du mot du guet R 60. comptez depuis 60. inclusivement, disant 60.70.80.90.1.2.3.4.5.6.7.8.9. & remarquez que vous avez compté treize nombres; dont la treiziéme lettre de l'Alphabet est la lettre P. de secret, pour laquelle on a envoyé le chifre 9.

[6] [. . .] elle est neanmoins indéchifrable à tout esprit humain. Quand même on donneroit au Déchifreur les lettres que chaque chifre signifie, il faudroit encore qu'il pust deviner le nombre qui sert de premiere clef, & qu'aprés cela il devinast encore l'ordre de l'Alphabet qui a donné ces lettres par le moyen du nombre convenu pour clef; de quoy on peut faire facilement l'essay avec ceux qui se piquent de pouvoir déchifrer; fust-ce avec Mr. Viette, le Pere de nôtre Algebre specieuse, & le grand Déchifreur de son temps, s'il pouvoit revenir au monde.

three issues of September and October 1684 and February 1685. It includes a fold-out table shown in Figure 3. In the centre is a "Vigenère table" in his alphabet, and just above it we find:

2	8	a	d	i	e	F	e	b	r	u	a	r	i	i	1	6	90
4	1	10	20	30	1	6	4	6	50	6	9	1	4	1	8	6	8
c	o	m	i	e	r	a	u	e	u	g	l	e	r	o	y	a	l

The top line is the message (somewhat surprisingly with a date of 1690 in a 1684 publication), the bottom one his usual key, and the center line the encryption.

At the sides are standards with two alphabets. The top line at left means that A is to be encrypted as 111, and B as the same with a dot added, maybe as $11 \cdot 1$. In the lower part is a keyword generated unsorted alphabet, made up from *Profetisandum* and the remaining letters *bcglq*, a pigpen cipher, and a line cipher. (The reproduction makes reading hard in some parts.) Comiers does not give any reference to Trithemius or Vigenère, but attributes the general Caesar substitution to the ancient Hebrews. Comiers also describes some steganographic methods, such as marking the value of letters by distances on a thread, or using trumpet signals. He discusses 10-complement subtraction and numerological curiosities such as

$$\underbrace{99\ldots99}_{n} \cdot \underbrace{66\ldots66}_{n} = \underbrace{66\ldots66}_{n-1}\,5\,\underbrace{33\ldots33}_{n-1}\,4,$$

(for $n = 666$), of which he boasts: *I can do in one moment, blind as I am, something that you cannot do in a month and with several quires of paper.*[7]

In another work, the *Pratique Curieuse ou les oracles des Sybilles*, Comiers (here spelled Commiers) provides answers to all important questions about life and the rest of the universe. There are rules to calculate a number from a question (out of a given list) together with the persons named in the question, the day of the week, and the moon's position. Then one looks up the answer in a list, as indicated by the calculated number. Good luck!

Claude Comiers was born in Embrun in the French Alps, early in the 17th century. The exact date is not known. He died in the old-age home of Les Quinze-vingts in Paris, in 1693. He worked for the *Journal des Savans* and wrote on a wide range of topics: *La nouvelle Science de la nature des comètes; Discours sur les comètes; Trois discours sur l'art de prolonger la vie; Traité des lunettes; Traité des prophéties, vaticinations, prédictions et pronoçtications, contre le ministre Jurieu; Traité de la parole, des langues et écritures; Instruction pour réunir les églises prétendues réformées à l'Église romaine.* That is,

[7] Je fais en moment, tout aveugle qui je suis, ce qu'on ne peut faire en un mois & avec plusieurs mains de papier. [A *main de papier* is a quire (about 25 sheets) of paper.]

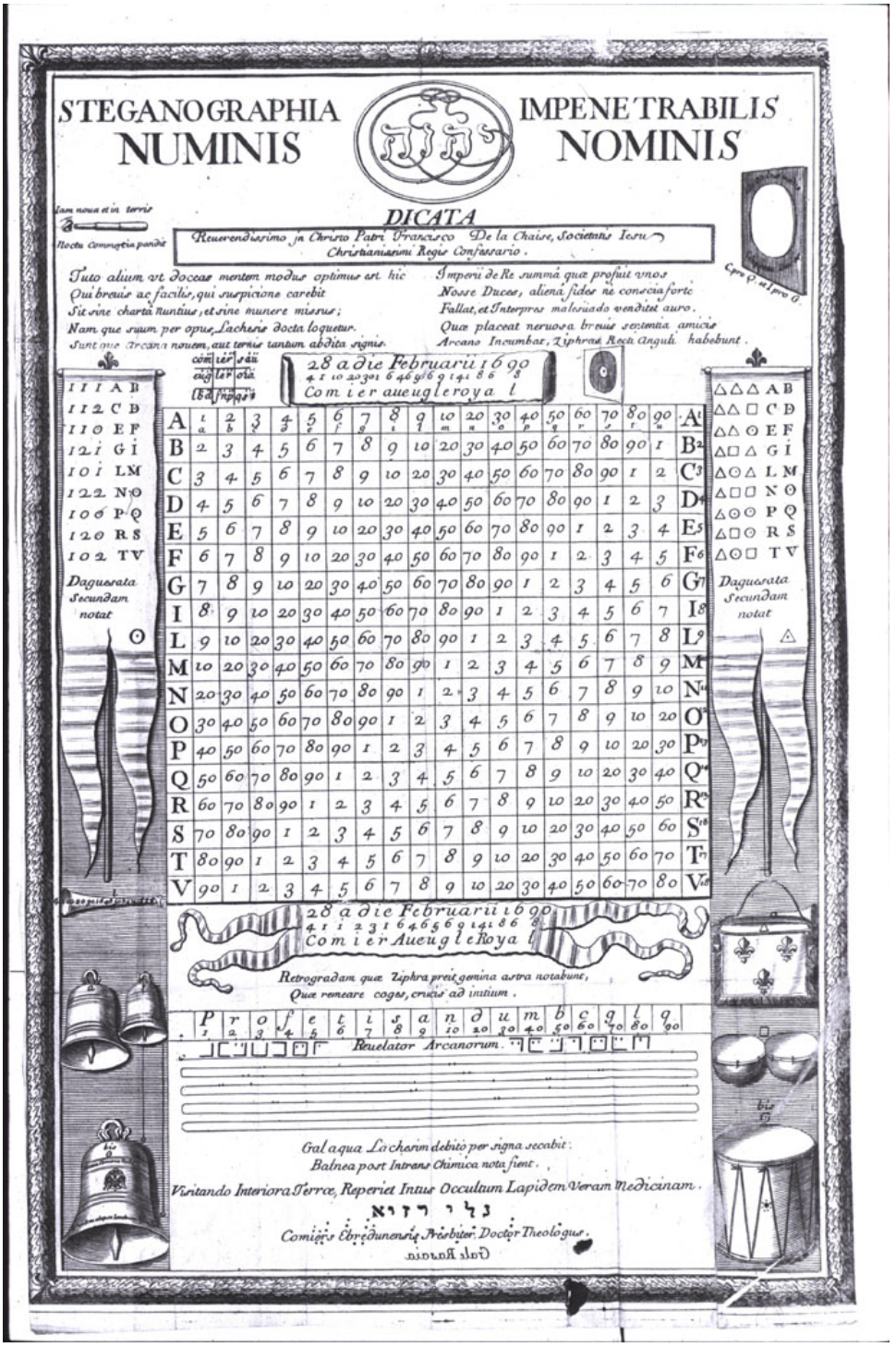


Figure 3: The Vigenère table of Comiers.

about comets, doubling the cube and trisecting angles, church politics, mirrors, spectacles and solar clocks, mineral waters, machines for raising water in channels, phosphor, and the art of prolonging one's life (with a 400-year-old gentleman as example). Rochas writes in his 1856 *Biographie du Dauphiné* deprecatingly: *He was a man possessed by a mania for writing, and succeeded in passing with his contemporaries as a scholar.*[8]

Comiers turned blind around 1684 and took the title of *aveugle royal*, because the King had granted him a pension. His work remained inconsequential in the history of cryptography.

3. Other work on arithmetic cryptography

An anonymous work *Neueröffneter Schauplatz geheimer philosophischer Wissenschaften*[9], published in 1770 (Figure 4), proposes an even more general type of arithmetic cryptography. In Chapter 16 *Von der logistischen Steganographia*[10] the author adds a fixed number to each letter of the plaintext (Caesar) or subtracts one. But then he also multiplies by a number, or divides by one. Figures 5 and 6 illustrate encryption and decryption. He uses a standard alphabet with 24 letters and an offset of 6: $A = 6$, $B = 7, \ldots$, $Z = 5$. This is "table F" from his *number table*[11], which is essentially a Vigenère tableau. The secret key is this "F" and the multiplier 2. The result is taken as an integer, not modulo 24. Since the multiplier 2 is easily revealed as the greatest common divisor of a few encrypted letters, this does not offer any more security than a Caesar cipher. Addition and multiplication by a constant are special cases of affine linear transformations. But it is a long way from here to Hill's 1931 general linear transforms, requiring the development of the appropriate mathematical machinery over the centuries.

In the Greek and in the Arab civilizations, letters had a standard numerical value. This allows encrypting a letter by sending two (or more) letters whose numerical sum equals the given one. This system was described by al-Kindī (801–876); see Mrayati *et al.* (1987).

In his 1819 work on *Den hemmelige Skrivekunst*[12], Lindenfels presents a Vigenère tableau with a 20-letter alphabet. The 16th letter is "S", and he uses the encryption rule (1) with an offset of $S = 16$. On page 177, he encrypts the

[8] C'était un homme possédé de la manie d'écrire, et qui réussit auprès de ses contemporains à se faire passer pour un savant.

[9] Newly opened showplace of secret philosophical sciences

[10] On logistic steganography

[11] Zahltisch

[12] The art of secret writing

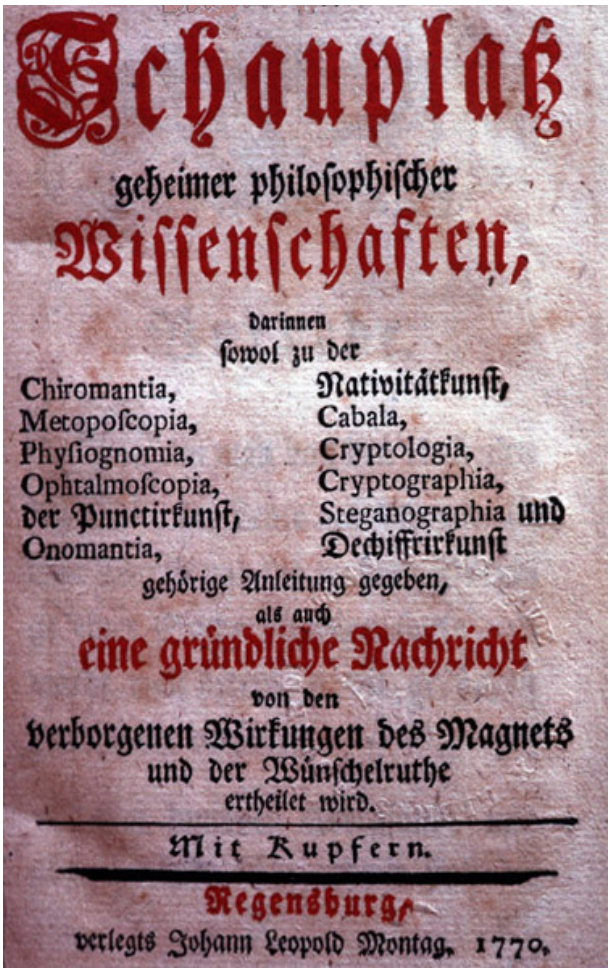
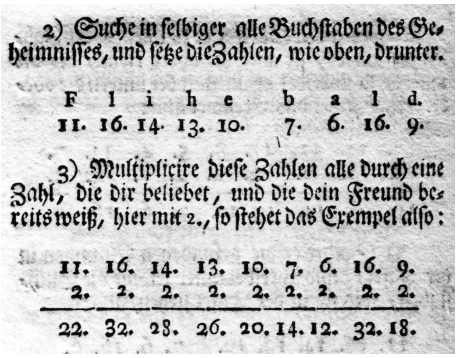

Schauplatz
geheimer philosophischer
Wissenschaften,
darinnen
sowol zu der
Chiromantia,
Metoposcopia,
Physiognomia,
Ophtalmoscopia,
der Punctirkunst,
Onomantia,
Nativitätkunst,
Cabala,
Cryptologia,
Cryptographia,
Steganographia und
Dechiffrirkunst
gehörige Anleitung gegeben,
als auch
eine gründliche Nachricht
von den
verborgenen Wirkungen des Magnets
und der Wünschelruthe
ertheilet wird.
Mit Kupfern.
Regensburg,
verlegts Johann Leopold Montag. 1770.

Figure 4: The *Schauplatz* title page. Note that the title of this journal appears literally.



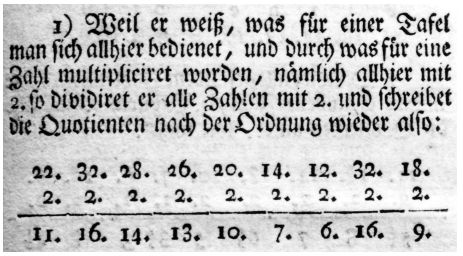
2) Suche in ſelbiger alle Buchſtaben des Geheimniſſes, und ſetze die Zahlen, wie oben, drunter.

F	l	i	h	e		b	a	l	d.
11.	16.	14.	13.	10.		7.	6.	16.	9.

3) Multiplicire dieſe Zahlen alle durch eine Zahl, die dir beliebet, und die dein Freund bereits weiß, hier mit 2., ſo ſtehet das Exempel alſo:

11.	16.	14.	13.	10.	7.	6.	16.	9.
2.	2.	2.	2.	2.	2.	2.	2.	2.
22.	32.	28.	26.	20.	14.	12.	32.	18.

Figure 5: Encryption via multiplication by 2: *2) Find in the number table all letters of the cleartext, and write below them the corresponding numbers, as above. [Flihe bald = Flee soon.] 3) Multiply all these numbers by a number of your choosing and which your correspondent knows. We take 2 here, and have the following example: [...]*



1) Weil er weiß, was für einer Tafel man ſich allhier bedienet, und durch was für eine Zahl multipliciret worden, nämlich allhier mit 2. ſo dividiret er alle Zahlen mit 2. und ſchreibet die Quotienten nach der Ordnung wieder alſo:

22.	32.	28.	26.	20.	14.	12.	32.	18.
2.	2.	2.	2.	2.	2.	2.	2.	2.
11.	16.	14.	13.	10.	7.	6.	16.	9.

Figure 6: First step in the decryption via division by 2: *Because he [your correspondent] knows which table is used and by which number has been multiplied, namely here by 2, he divides all numbers by 2 and writes down the quotients in their order: [...]*

cleartext ABEL with the key CAIN, obtaining the ciphertext UTIS. To explain the encryption of the last letter, he writes "$N_{„}$ + "$L_{„}$ = "$S_{„}$. Thus Lindenfels states rule (1) in some special cases. On page 181, he says about another table: *One of them—the first or the second, depending on the circumstances—is a factor, the other one the product.*[13] The context is not quite clear, but Lindenfels may have recognized somehow the Vigenère tableau as the table of a group operation. Kasiski (1863) points out explicitly that the cryptosystem is addition modulo 26, and that commutativity of addition corresponds to the (anti-)symmetry of the Vigenère table: cleartext + key = key + cleartext.

The key-addition cipher was rediscovered many times. Captain Otto Holstein (1917) writes about a new cipher reported in the *Scientific American* that it is *the old Vinegere* [sic] *cipher of the sixteenth century.* Lubin (1901) describes it and its additive character. He then suggest repeated superencipherment with the same method but different keywords whose lengths are pairwise coprime to obtain a long period.

Acknowledgment

Many thanks go to David Kahn for helpful remarks that improved the presentation, and to Jean-Philippe Prost for a hand with the paper.

References

Ole Immanuel Franksen (1984). *Mr. Babbage's Secret. The Tale of a Cipher—and APL.* Strandberg, Birkerød, Denmark.

Carl Friedrich Gauss (1801). *Disquisitiones Arithmeticae.* Gerh. Fleischer Iun., Leipzig. English translation by Arthur A. Clarke, Springer-Verlag, New York, 1986.

Lester S. Hill (1931). Concerning certain linear transformation apparatus of cryptography. *The American Mathematical Monthly* **38**, 135–154.

Otto Holstein (1917). A New Cipher. *Scientific American Supplement* **83**, 235.

F. W. Kasiski (1863). *Die Geheimschriften und die Dechiffrir-Kunst.* E. S. Mittler und Sohn, Berlin. viii + 95 pp. + 6 tables.

I. B. Lindenfels (1819). *Den hemmelige Skrivekonst eller: Chiffrer= og Dechiffrer=Konsten.* Brummer, Kjøbenhavn, 340 pages .

[13] Det Ene af dem — efter Omstændighederne, snart det Første, snart det Andet — tjener som Multiplicand, det Andet som Product.

Lubin (1901). Méthode de correspondance chiffrée. *Revue Scientifique, Paris* **16**(Sem. 2, Sér. 4), 809–812.

M. Mrayati, Yahya Meer Alam & Hassan Al-Tayyan (1987). *Origins of Arab Cryptography and Cryptanalysis. Volume One. Analysis and Editing of Three Arabic Manuscripts: Al-Kindi, Ibn-Adlan, Ibn-Al-Durahim.* Arab Academy of Damascus publications.

Joachim von zur Gathen
Fakultät für Elektrotechnik, Informatik,
Mathematik
Universität Paderborn
D-33095 Paderborn, Germany
gathen@upb.de