Cryptography

PROF. DR. JOACHIM VON ZUR GATHEN, JÉRÉMIE DETREY

1. Tutorial: From paleo-cryptography to AES

(in one hour and a half!)

Exercise 1.1 (When in Rome...).

The Caesar cipher is probably the simplest and most widely known cipher, named after the Roman emperor Julius Caesar, who reportedly used it to encode confidential messages (typically military orders).

The key used to encrypt (and decrypt) a message is a single letter of the alphabet. Each occurrence in the plaintext of the letter "A" is then encoded using this letter, each occurrence of "B" using the next letter in the alphabet, and so on, wrapping around from "Z" back to "A" in the ciphertext alphabet[1].

For instance, Julius Caesar always used the key "D", which would give the following plaintext and ciphertext alphabets:

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P

Plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

(i) Encode the message "ALEA JACTA EST" using the same key "D":

Solution. "DOHD MDFWD HVW". ○

(ii) Given the key "Z", decode the message "UDMH, UHCH, UHBH!".

Solution. "VENI, VIDI, VICI!". ○

(iii) Is this cipher secure? Can you think of ways to break it?

Solution. No, the Caesar cipher is not secure. It can easily be broken by means of frequency analysis or brute force attack. ○

[1] For simplicity's sake, we are not using the actual Latin alphabet they had at the time but our good old 26-letter alphabet.

Now let's try to look at this cipher from a bit more mathematical point of view, and represent each letter by a number, "A" being 0, "B" being 1, and so on, until "Z" which is mapped to 25.

(iv) What is this set of numbers? What are its properties?

Solution. The numbers $\{0, 1, \ldots, 25\}$ can be seen as the cyclic group $\mathbb{Z}/26\mathbb{Z}$, also noted $\mathbb{Z}_{26}$. ◯

(v) How would you represent the encryption operation, given a key $k \in \{0, 1, \ldots, 25\}$?

Solution. For all $x \in \mathbb{Z}_{26}$, we have $\text{Encrypt}_k(x) = (x + k) \bmod 26$. ◯

(vi) What about decryption?

Solution. Similarly, for all $x \in \mathbb{Z}_{26}$, $\text{Decrypt}_k(x) = (x - k) \bmod 26$. ◯

(vii) Can the Caesar cipher benefit from double encryption? Why?

Solution. The addition in $\mathbb{Z}_{26}$ being associative, a double encryption with keys k and k' is rigourously equivalent to a single encryption using key $(k + k') \bmod 26$:

$$\text{Encrypt}_{k'}(\text{Encrypt}_k(x)) = (x + k + k') \bmod 26 = \text{Encrypt}_{(k+k') \bmod 26}(x).$$

This is also trivial when looking at the alphabet transformations induced by two successive encodings. ◯

Exercise 1.2 (A fine[2] cipher).

The affine cipher is a variant of the Caesar cipher, and is almost as weak in terms of security, although it is still possible to use the same kind of trick as in the Vigenère cipher in order to strengthen it.

Using the numerical notation introduced for the Caesar cipher, the key of the affine cipher is given by a pair of numbers a and b between 0 and 25. The encryption of a plaintext letter x is given by

$$\text{Encrypt}_{a,b}(x) = (ax + b) \bmod 26.$$

For instance, for $a = 3$ and $b = 2$, we have the following alphabet substitution:

[2] Not really actually.

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
Ciphertext	C	F	I	L	O	R	U	X	A	D	G	J	M

Plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	P	S	V	Y	B	E	H	K	N	Q	T	W	Z

(i) How is this cipher related to the Caesar cipher?

Solution. The Caesar cipher is just an affine cipher for $a = 1$. ◯

(ii) Build the alphabet substitution for $a = 4$ and $b = 3$.

Solution.

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
Ciphertext	D	H	L	P	T	X	B	F	J	N	R	V	Z

Plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	D	H	L	P	T	X	B	F	J	N	R	V	Z

◯

(iii) What seems to be the problem here?

Solution. Several letters have the same ciphertext. For example both "A" and "N" are mapped to "D". This will be a problem in the decryption phase! ◯

(iv) What is the mathematical expression of the decryption of a ciphertext letter x?

Solution. We have $\mathrm{Decrypt}_{a,b}(x) = a^{-1}(x - b) \bmod 26$. ◯

(v) Deduce from that a condition on a and b for the affine cipher to be actually invertible.

Solution. The condition is that a has to be be co-prime to the size of the alphabet (26 in our case) so that it has a multiplicative inverse. ◯

(vi) How many possible keys combinations does that leave us with?

Solution. Not counting the Caesar ciphers, we have 11 possible values for a, and 26 for b, hence 286 different keys. ◯

(vii) Conclude on the strength of such a cipher. Devise an efficient mean of breaking it.

Solution. As previously mentioned, the affine cipher is almost as weak as the Caesar cipher. Given the limited key space, brute force attacks are obviously good solutions.

Using frequency analysis, one can also work out the plaintext of two ciphertext letters and, from that, compute the actual parameters a and b by solving a simple system of two modular equations. ◯

But now, let's double back a bit, and focus on the decryption phase, which may appear to be a bit more tricky than it looked at first glance.

(viii) Show that the decryption for a and b is actually another encryption, only with a different key (a', b'). What are the values of a' and b'?

Solution. We have

$$\begin{aligned}\text{Decrypt}_{a,b}(x) &= a^{-1}(x-b) \bmod 26\\ &= a^{-1}x - a^{-1}b \bmod 26\\ &= \text{Encrypt}_{a',b'}(x),\end{aligned}$$

with $a' = a^{-1} \bmod 26$ and $b' = -a^{-1}b \bmod 26$. ◯

(ix) Compute those parameters a' and b' for $a = 3$ and $b = 2$. Check your computations with the substitution table of the beginning of the exercise.

Solution. As $9 \times 3 \equiv 1 \pmod{26}$, $a' = a^{-1} \bmod 26 = 9$, and $b' = -a^{-1}b \bmod 26 = 8$. We obtain the following substituion, which is as expected the inverse of the encoding transformation:

Ciphertext	A	B	C	D	E	F	G	H	I	J	K	L	M
Plaintext	I	R	A	J	S	B	K	T	C	L	U	D	M

Ciphertext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plaintext	V	E	N	W	F	O	X	G	P	Y	H	Q	Z

◯

Exercise 1.3 (A tad more on multiplicative inverses).

We now want[3] to devise an efficient way to compute a^{-1}, the multiplicative inverse of an integer a modulo another integer n.

[3] Well, at least *I* want you to! If you are not sure of why we are doing that, which rightfully seems quite disconnected from affine ciphers after all, just wait a few more minutes. It shall all become clear at some point. Or so I hope...

(i) Let a be a number in $\mathbb{Z}_n$ relatively prime to n. What is the value of $\gcd(a, n)$, the greatest common divisor of a and n?

Solution. $\gcd(a, n) = 1$, since a and n are coprime. ◯

(ii) Recall Bézout's identity for two integers u and v. Apply it to a and n and find an expression of a^{-1} from that.

Solution. Given u and $v \in \mathbb{N}$, Bézout's identity states that there exist x and $y \in \mathbb{N}$ so that $ux + vy = \gcd(u, v)$.

Plugging a and n instead of u and v, we get $ax + ny = \gcd(a, n) = 1$. Taking this modulo n, we obtain $ax \equiv 1 \pmod{n}$, hence $a^{-1} = x \bmod n$.

◯

(iii) Give an algorithm to compute the $\gcd$ of two integers u and v.

Solution. The $\gcd$ is computed by the Euclidean algorithm:

Input: u and $v \in \mathbb{N}$.
Output: $\gcd(u, v)$.

1. **while** $v \neq 0$ **do**
2. $\quad t \leftarrow v$
3. $\quad v \leftarrow u \bmod v$
4. $\quad u \leftarrow t$
5. **end while**
6. **return** u

◯

(iv) Apply this algorithm to $n = 26$ and $a = 15$. You should obtain $\gcd(26, 15) = 1$.

Solution.

Iteration	u	v	$u \bmod v$
0	26	15	11
1	15	11	4
2	11	4	3
3	4	3	1
4	3	1	0
5	1	0	–

The greatest common divisor of 26 and 15 is the value of u on the last iteration of the algorithm. Namely 1, here, as expected. ◯

(v) Use this execution trace of the $\gcd$ algorithm to compute the multiplicative inverse of 15 modulo 26.

Solution. We just have to keep track of how many times 15 is added or subtracted in the intermediate results. For that, we express each value of $u \bmod v$ as a sum of multiples of 15 and 26.

Iteration	u	v	$u \div v$	$u \bmod v$	**Side computations**
0	26	15	1	11	$11 = 1 \times 26 - 1 \times 15$
1	15	11	1	4	$4 = 1 \times 15 - 1 \times 11$ $= 2 \times 15 - 1 \times 26$
2	11	4	2	3	$3 = 1 \times 11 - 2 \times 4$ $= 3 \times 26 - 5 \times 15$
3	4	3	1	1	$1 = 1 \times 4 - 1 \times 3$ $= 7 \times 15 - 4 \times 26$
4	3	1	3	0	–
5	1	0	–	–	–

The computation on iteration 3 gives us Bézout's identity: $7 \times 15 - 4 \times 26 = 1$. Hence, $15^{-1} \equiv 7 \pmod{26}$. ◯

(vi) Modify your $\gcd$ algorithm to compute the multiplicative inverse of v modulo u, given u and v two coprime integers.

Solution. This algorithm is called the extended Euclidean algorithm:

Input: u and $v \in \mathbb{N}$, such that $\gcd(u, v) = 1$.
Output: $v^{-1} \bmod u$.

1. $rem[0] \leftarrow u$
2. $rem[1] \leftarrow v$
3. $aux[0] \leftarrow 0$
4. $aux[1] \leftarrow 1$
5. $i \leftarrow 1$
6. **while** $rem[i] > 1$ **do**
7. $\quad i \leftarrow i + 1$
8. $\quad quo[i] \leftarrow rem[i-2] \div rem[i-1]$
9. $\quad rem[i] \leftarrow rem[i-2] \bmod rem[i-1]$
10. $\quad aux[i] \leftarrow aux[i-2] - quo[i] \times aux[i-1]$
11. **end while**
12. **return** $aux[i]$

◯

Exercise 1.4 (Towards AES).

While designing the Rijndael cipher, Daemen and Rijmen wanted the S-boxes of the `SubBytes` step to implement a non-linear substitution. For that purpose, they chose the multiplicative inverse function[4].

(i) The S-boxes map their 8-bit input word to another 8-bit word. How many values can these 8 input bits take?

Solution. Simply $2^8 = 256$ different values. ◯

(ii) Can we use the multiplicative inverse over $\mathbb{Z}_{256}$ for the S-boxes? Why?

Solution. Only the odd numbers of $\mathbb{Z}_{256}$ have multiplicative inverses, since all of the even numbers in this group divide zero. ◯

So instead on considering only numbers, Daemen and Rijmen looked at polynomials with boolean coefficients. That is, polynomials of the form

$$P(x) = \sum_{i=0}^{\deg(P)} p_i x^i,$$

where $p_i \in \mathbb{Z}_2 = \{0, 1\}$. We note the set of all these polynomials $\mathbb{Z}_2[x]$.

Now let's take the degree-8 polynomial $M(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$, which is irreducible over $\mathbb{Z}_2$, and consider the set of polynomials over $\mathbb{Z}_2$ modulo $M(x)$. We note this quotient set $\mathbb{Z}_2[x]/(M(x))$.

(iii) What is the highest degree of the polynomials in this set?

Solution. As $x^8 \equiv x^4 + x^3 + x + 1 \pmod{M(x)}$, we can reduce all polynomials to be of degree at most 7. ◯

(iv) How many polynomials are there?

Solution. Each polynomial has 8 coefficients, each possibly 0 or 1, which gives $2^8 = 256$ different polynomials. ◯

[4] At last! This is the reason why we spent so much time on multiplicative inverses in the previous exercise. Although Rijndael doesn't only use a simple inversion for its S-boxes... But this is an altogether different story, which you shall learn during the lectures.

(v) Find a way to represent each polynomial $P(x) \in \mathbb{Z}_2[x]/(M(x))$ using only 8 bits. For instance, how would you reprensent $x^6 + x^4 + x^2 + x + 1$?

Solution. Each bit corresponds to a particular coefficient p_i of $P(x)$. We represent $x^6 + x^4 + x^2 + x + 1$ as the 8-bit word 01010111. ◯

And now let's get back to our multiplicative inverse problem.

(vi) Show that, except for 0, all the elements of $\mathbb{Z}_2[x]/(M(x))$ have a multiplicative inverse.

Solution. Suppose we have $P(x) \in \mathbb{Z}_2[x]/(M(x))$, $P(x) \neq 0$, such that $P(x)$ doesn't have a multiplicative inverse. $\mathbb{Z}_2[x]/(M(x))$ being finite, it actually means that $P(x)$ divides 0: there exists another polynomial $Q(x) \in \mathbb{Z}_2[x]/(M(x))$, $Q(x) \neq 0$, such that $P(x)Q(x) \equiv 0 \pmod{M(x)}$. Hence, factoring $P(x)$ as a product of irreducible polynomials, at least one of these factors has to divide $M(x)$, which contradicts the hypothesis that $M(x)$ was irreducible. ◯

(vii) Try to use the algorithm from the previous exercise to compute the multiplicative inverse of $x^6 + x^4 + x^2 + x + 1$ in $\mathbb{Z}_2[x]/(M(x))$.

Solution.

i	$rem[i]$	$quo[i]$	$aux[i]$
0	$x^8 + x^4 + x^3 + x + 1$	–	0
1	$x^6 + x^4 + x^2 + x + 1$	–	1
2	x^4	$x^2 + 1$	$x^2 + 1$
3	$x^2 + x + 1$	$x^2 + 1$	x^4
4	x	$x^2 + x$	$x^6 + x^5 + x^2 + 1$
5	1	$x + 1$	$x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$

We can then check that $(x^6+x^4+x^2+x+1)\cdot(x^7+x^5+x^4+x^3+x^2+x+1) \equiv 1 \pmod{M(x)}$. ◯