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":

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

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

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.

[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.

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

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

(vi) What about decryption?

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

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:

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z

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

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

(iii) What seems to be the problem here?

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

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

[2] Not really actually.

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

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

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'?

(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.

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.

(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?

(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.

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

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

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

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

[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...

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?

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

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?

(iv) How many polynomials are there?

(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 $x^6 + x^4 + x^2 + x + 1$?

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.

(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 $\mathbb{Z}_2[x]/(M(x))$.

[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.