Classical Cryptography

JOACHIM VON ZUR GATHEN, JÉRÉMIE DETREY

1. Tutorial: Substitutions and transpositions

Exercise 1.1 (A fine[1] 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 a numerical representation of the alphabet (A is 0, B is 1, ..., Z is 25), 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
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?

(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.

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

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

[1] Not really actually.

Exercise 1.2 (From Vigenère to one-time pads).

(i) Recall the ideas behind Kasiski's analysis of the Vigenère cipher.

(ii) What simple method can we use in order to increase the security of the Vigenère cipher?

(iii) Pushing this method to its extreme limit, we obtain a *one-time pad*. Prove that this system is perfectly secure.

(iv) Why do we call it *one-time*?

Exercise 1.3 (Breaking columnar transpositions).

(i) Recall the principle of columnar transposition.

(ii) In a $r \times c$ columnar transposition, what are the positions in the ciphertext of two letters which were originally consecutive in the plaintext?

(iii) Devise a way of breaking such a transposition cipher.

(iv) What about composing a columnar cipher with a simple substitution cipher?