Problem Set 1

General Concepts

Problem I

We consider a variant of the one-time-pad cipher based on two keys (or pads). Let K_1 and K_2 be the keys, consider

$$K = K_1 \oplus K_2$$

and C the one-time-pad cipher based on K. (We note $\oplus$ the xor operator).

1. Is the cipher C secure if K_1 and K_2 are chosen randomly?

2. Let r be the fonction reversing the order of the bits of a pad (*e.g.* r(10110)=01101). Is the cipher C secure if K_1 is chosen randomly and $K_2 = r(K_1)$?

3. Is the cipher C secure if K_1 is chosen randomly and $K_2 = K_1$?

Problem II

Let M be a message and $n \in \mathbb{N}^*$ be a number of people. Create an algorithm creating n messages such that M can be recovered if and only if the n messages are known and so that no part of M can be recovered otherwise.

Problem III

We mentionned in class the Caesar cipher. The cipher is based on a monoalphabetic substitution. The key is given by a number k between 1 and 26. Each letter of the plaintext is replaced by the letter k places later (with wrap around).

In the The Vigenère[1] cipher, the key is given by a sequence of p numbers between 1 and 26: $k_1, \ldots, k_p$. The cipher is based on a polyalphabetic substitution. The plaintext is broken up into successive strings of p letters and the i-th letter of each string is replaced by its image under the Caesar cipher with key k_i.

Implement the Caesar cipher and Vigenère cipher in C.

[1] Blaise de Vigenère was a 16th century French cryptographer and diplomat. He is known for the Vigenère cipher, even though Giovan Battista Bellaso had invented the cipher earlier.

Blaise de Vigenère (1523–1596)