TP 01: Histoire de la cryptographie

Jean-Sébastien Coron

Université du Luxembourg

1 Chiffrement de César

Déchiffrez le message suivant:

    rtcthieajhjctpgstjgspchbthktxcthrprwtt,
    rthiktcjhidjittcixtgtphpegdxtpiiprwtt.

2 Chiffrement par substitution mono-alphabétique

Les lettres les plus fréquentes dans la langue française sont les suivantes: e (14.0 %), s (7.9 %), a (7.6 %), i (7.5 %), t (7.2 %), n (7.0 %), r (6.5 %), u (6.3 %), l (5.4 %), o (5.3 %).

Déchiffrez le message suivant:

    zbjnzqyxcfhobjrblhcmmxbobkfjvobfxcsebjbmykrbkfjexekboboblzb,
    iyexlhcmmxbxbfrblhcmmxbxekobjjnqb,
    zbixywzbobrblbffbfblhkcsebbjfsebznlzb,
    secrycfxbjfbxfyfnzbobkflykmcrbkfcbzzb,
    rycfbfxbfxnkjocjbnelyxxbjiykrnkfrbmnlykjexb.

3 The Vernam Cipher

The *Vernam Cipher* (see [1]) is a stream cipher defined on $\{0,1\}$. It takes as input a binary message $m_1 m_2 \ldots m_t \in \{0,1\}^t$ and a binary key $k_1 k_2 \ldots k_t \in \{0,1\}^t$ of the same length and outputs a ciphertext $c_1 c_2 \ldots c_t \in \{0,1\}^t$ where

$$c_i = m_i \oplus k_i, \ 1 \leq i \leq t$$

If the key is randomly chosen and used only once, the Vernam cipher is called the *one-time pad*.

1) Explain how to encrypt a text with the Vernam cipher. Give an example with a short text. Optional: implement the Vernam Cipher in C. Your program must take as input a string of character and output the resulting ciphertext. The key string will be generated using the (insecure) C random generator.

The Vernam cipher can proven perfectly secure if the key string is random and only used once. Namely, given a ciphertext, any t-bit binary string of plaintext is equally likely. This implies that an attacker who does not know the key obtains no information about the plaintext.

2) However, if the key is reused then the cipher can be attacked. Assume that the same key-bits are repeated every 32-bits, *i.e.* we have

$$K = k_1 k_2 \ldots k_{32} k_1 \ldots k_{32} k_1 \ldots k_{32} \ldots$$

Explain how the plaintext can be recovered without knowing the key K. Optional: show that your attack works by implementing it in C.

References

1. A.J. Menezes, P. C. van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*. Available online.