Information Security Basics
Public-key Cryptography Part

Jean-Sébastien Coron

Université du Luxembourg

1 The Vernam Cipher

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

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

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

2 OAEP Encryption

From the description of OAEP in the course, provide the pseudo-code of OAEP encryption and decryption.

3 PSS Signature

From the description of PSS in the course, provide the pseudo-code of PSS signature and verification.

4 Is RSA Encryption Anonymous ?

Bob must send 10 messages $m_1, \dots, m_{10}$, either to Alice whose RSA public-key is (N_1, e_1), or to Anais whose RSA public-key is (N_2, e_2).

Therefore if Bob sends his 10 messages to Alice, he is going to send the ciphertexts :

$$c_i = (m_i)^{e_1} \mod N_1$$

for $1 \leq i \leq 10$.

Whereas if Bob sends his messages to Anais, he sends the following ciphertexts :

$$c_i = (m_i)^{e_2} \mod N_2$$

An eavesdropper gets the 10 ciphertexts c_i, and also knows the public-key of Alice and Anais, but she doesn't know the messages m_i. How might she be able to determine whether Bob sent his messages to Alice or Anais ?

Références

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