Université Libre de Bruxelles
Faculté des Sciences

January 19, 2017

INFO-F-405 Introduction to cryptography

This assessment has to be realized without the use of personal notes, books or any other support. A portfolio with needed algorithms is given. You may use a calculator (it is not required). You have to justify each of your answers. Indicate your name, first name and year of study on every answer sheets.

Question 1 (theory)

1. What is, in general, the purpose of the modes of operations for encryption (CBC, OFB, CFB, ...) ?
2. When considering two messages m_1 and m_2 both symmetrically encrypted with the CTR mode, is there a security risk of using the same nonce in this mode of operation?
3. "CTR-chained encryption" is a stateful CTR mode of operations where the nonce for the next message encryption is the last encrypted bloc of the previous encryption. Is there a risk to proceed in this way?

Question 2 (theory)

1. On what mathematical principle is based the security of the El Gamal encryption scheme and where this principle appears in the scheme?
2. What happens in case of misuse of k?
3. What are the advantages and disadvantages of using El Gamal to encrypt messages?

Question 3 (theory)

1. What is the purpose of the here-under protocol?

   Alice chooses randomly a
   Bob chooses randomly b
   The values of a prime p and of a generator g of Z_p^* are public

   Alice $\rightarrow$ Bob : $g^a \bmod p$
   Bob $\rightarrow$ Alice : $g^b \bmod p$

   $c = g^{ab} \bmod p$
2. Is this protocol secure?
3. How is it possible to improve it?

Question 4 (theory)

What is the meaning and the result of the computation of the symbol $\left(\frac{3}{45}\right)$?

Question 5 (practice)

Your goal is to design a system that can be used for a full disk encryption. The idea is simple, the user wants to store valuable information of the hard-drive, but instead of encrypting each file he wants to use full disk encryption. The user wants to be able to interact with the system in the following way:

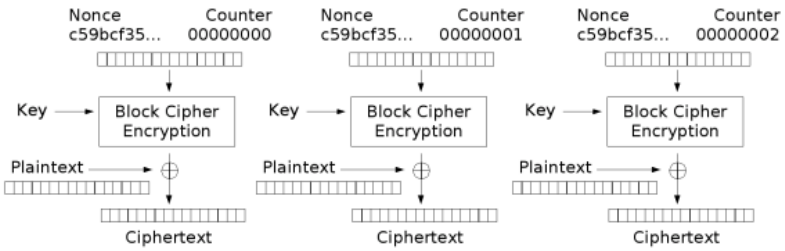
- Start the computer,
- Enter a password,
- [..some crypto-magic happens here..],
- The Operating System (OS) starts booting,
- Normal interactions with the OS. The OS, with the exception of the driver, has no knowledge about the fact that the disc is encrypted.

Suppose that programmers will code the appropriate initialisation procedures and the driver for the encrypted filesystem. Your goal is to describe the 3 following procedures (the cryptographic part of them) to the programmers:

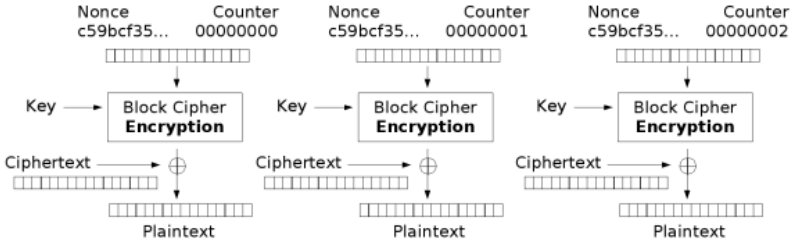
- Initialisation of the system — The user wants to do it by typing the password during the installation procedure;
- Reading from memory — the OS passes an address to the driver, the driver reads an encrypted chunk, decrypts it and gives a plaintext data to the OS;
- Writing into memory — the driver gets an address and a plaintext data from the OS and stores an encrypted version of data in memory at the desired address.

We ask you to draw 3 flow charts for the 3 procedures described above. We also ask you to justify your choices of cryptographic protocols and algorithms, your justifications should not exceed 3 phrases per algorithms (or protocol) that you are using.

Portfolio



Counter (CTR) mode encryption



Counter (CTR) mode decryption

El Gamal Encryption scheme

A. Keys generation

1. choose randomly a large prime p
2. find a generator α of the multiplicative group $\mathbb{Z}^*{}_p$
3. choose randomly an integer $a \in [1, p-2]$
4. compute $\beta = \alpha^a \mod p$

Keys: The public key is (p, α, β) and the private key is a

B. Encryption

To encrypt the plaintext $x \in \mathbb{Z}_p$, choose randomly an integer $k \in [1, p-2]$ and compute:

$$\begin{cases} y_1 = \alpha^k \mod p \\ y_2 = x \cdot \beta^k \mod p \end{cases}$$

C. Decryption

Let (y_1, y_2) be the ciphertext: $x = {y_1}^{-a} \cdot y_2 \mod p$