Abdelhafid Boussouf University , Mila
Faculty of Mathematics and computer science
Department of Computer Science
3rd Year Informatics

Year: 2025/2026
Computer Security

Directed Work N° 4

Exercise 1:

Let the plaintext (represented in Hexadecimal) be:

i = 3243f6a8885a308d313198a2e0370734

And the key (represented in Hexadecimal):

k = 2b7e151628aed2a6abf7158809cf4f3c

- According to the **AES-128 algorithm**:

1. Give the state tables of the message (plaintext) **"i"** and the key **"k"**.
2. Give the current state table obtained after applying each of the following steps:

   a) The initial addition **i ⊕ k** defined by the **AddRoundKey** operation.

   b) The **"SubBytes"** operation applied to the result of the addition **i ⊕ k**.

   c) The **"ShiftRows"** operation applied to the result of the **"SubBytes"** operation.

3. Give the result of applying the **MixColumns** operation on the following column:

$$\begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix}$$

Exercise 2:

1. User A chooses the prime factors **p = 3** and **q = 11**.
   - Determine a **private key** and a **public key** for the RSA cryptosystem using p and q.
2. Users A and B agree on an RSA protocol in which the letters of a message are encoded by their position in the alphabet (in base 10), and the message is split into blocks of 2 digits (in base 10). B wants to send the message **"CALCUL"**.
   - Give the **encrypted message** that B sends to A.
   - Give the **decrypted message** by A from the message received from B, and verify that it matches what B sent.

Exercise 03:

Let user A have the private key (3, 55) and the public key (27, 55) RSA.

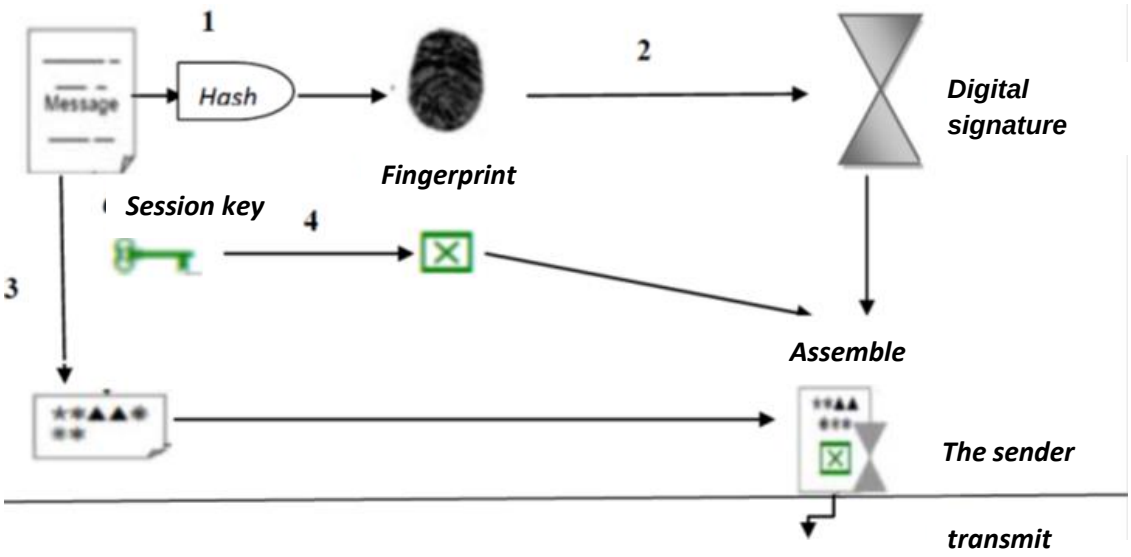
Let user B have the private key (7, 187) and the public key (23, 187) RSA.

1. To ensure the confidentiality of his messages, user A encrypts the message m = 2 using B's RSA key. Give the encrypted message.
2. To ensure the authenticity of his messages, user A signs the message m using RSA signature and encrypts the result using B's RSA key. Give the signed and encrypted message c.
3. User B receives message c. Verify the signature.

Exercise 04:

In order to enhance the security of a commercial transaction over the internet, a **digital signature** is combined with message encryption based on a **hybrid cryptosystem**.

At the time of sending the transaction (see figure):



1. Give the names of the corresponding **cryptographic operations**.
2. What **security services** are ensured by this protocol?