**University Djilali Bounaâma of Khemis-Miliana**
**Department of Computer Science**
**L3 – Computer Systems (S6)**
**Final Examination – Computer Security & Cryptography / Correction**
**May 2025**

**Exercise n°1 (12 pts):** Consider a PKI-based encryption scheme (**See Part 4: PKI (Public Key Infrastructure) explained in course class**) implemented between two entities: Entity A (server) and Entity B (client). The PKI certificate provided includes the following cryptographic parameters: Public exponent e=7, Modulus n=143, Private exponent d=103, Symmetric secret key: "WORD".

Entity A intends to transmit the plaintext message "WORLD" to Entity B. Knowing that key letters are encoded using their respective positions in the alphabet (modulo 26). The symmetric encryption algorithm employed is the BELLASO-PORTA (**See Part 2: Poly-Alphabetic Substitution: D-Bellaso/Porta**) cipher.

1. Outline the step-by-step communication protocol that Entity A and Entity B must follow.

**Entity A encryption: (04 pts)**

a.Sign the secret key WORD using its private key d = 103 (letter by letter)

WORD = (22, 14, 17, 3) mod 26 **(0.5 pt)**

**Encryption using d = 103 (01 pt)**

$S(W) = 22^{103} \pmod{143} = 22$, $S(O) = 14^{103} \pmod{143} = 27$, $S(R) = 17^{103} \pmod{143} = 95$, $S(D) = 3^{103} \pmod{143} = 16$

b.Send the signed secret key to B: **(22, 27, 95, 16) to B (0.5 pt)**

c.Encrypt the message WORLD using BELLASO-PORTA (BELLASO table **(01 pt)**)


**Encryption : (01 pt)**

| Plaintext | W | O | R | L | D |
|---|---|---|---|---|---|
| Key | W | O | R | D | W |
| Ciphertext | H | I | M | X | S |

**Encrypted message = HIMXS**

d.Send the encrypted message **HIMXS** to B

**Entity B decryption: (02 pts)**

a. Decrypt the signed encrypted secret key (22, 27, 95, 16) using A public key (e = 7, n = 143) **(1.25 pt)**

P(22) = $22^7$ (mod 143) = 22, P(27) = $27^7$ (mod 143) = 14, P(95) = $95^7$ (mod 143) = 17, P(16) = $16^7$ (mod 143) = 3 (1 pt)

Decrypted secret key (22, 14, 17, 3) mod 26 = WORD (0.25 pt)

b. Decrypt the encrypted message HIMXS using BELLASO-PORTA **(0.75 pt)**

| Ciphertext | H | I | M | X | S |
|---|---|---|---|---|---|
| Key | W | O | R | D | W |
| Plaintext | W | O | R | L | D |

**Plaintext message = WORLD**

**Now,** Entity A transmits a second encrypted message to Entity B, this time using Arabic script (right-to-left reasoning). The following information is communicated to Entity B:

- Secret key: (141,113,130,0,123,63)
- Encrypted message: ك، ش، ق، ر، غ، ر، ب، ب، س، ف، غ، ش

2. Provide a detailed explanation of the decryption procedure followed by Entity B in order to retrieve the original plaintext message from the encrypted Arabic text.

**Arabic script decryption procedure: (06 pts)**

a.B decrypts signed Secret key using A public key (e = 7, n = 143)**:**

P(141) = $141^7$ (mod 143) = 15, P(113) = $113^7$ (mod 143) = 9, P(130) = $130^7$ (mod 143) = 26, P(0) = $0^7$ (mod 143) = 0, P(123) = $123^7$ (mod 143) = 7, P(63) = $63^7$ (mod 143) = 2 **(1.5 pt)**

Decrypted secret key (15, 9, 26, 0, 7, 2) mod 28 = طروادة **(0.5 pt)**

b.BELLASO-PORTA decryption **(**Arabic BELLASO Table **(02 pts))**

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ص | ش | س | ز | ر | ذ | د | خ | ح | ج | ث | ت | ب | أ | أ ب |
| ي | و | ه | ن | م | ل | ك | ق | ف | غ | ع | ظ | ط | ض | |
| ص | ش | س | ز | ر | ذ | د | خ | ح | ج | ث | ت | ب | أ | ت ث |
| و | ه | ن | م | ل | ك | ق | ف | غ | ع | ظ | ط | ض | ي | |
| ص | ش | س | ز | ر | ذ | د | خ | ح | ج | ث | ت | ب | أ | ج ح |
| ه | ن | م | ل | ك | ق | ف | غ | ع | ظ | ط | ض | ي | و | |
| ص | ش | س | ز | ر | ذ | د | خ | ح | ج | ث | ت | ب | أ | خ د |
| ن | م | ل | ك | ق | ف | غ | ع | ظ | ط | ض | ي | و | ه | |
| ص | ش | س | ز | ر | ذ | د | خ | ح | ج | ث | ت | ب | أ | ذ ر |
| م | ل | ك | ق | ف | غ | ع | ظ | ط | ض | ي | و | ه | ن | |
| ص | ش | س | ز | ر | ذ | د | خ | ح | ج | ث | ت | ب | أ | ز س |
| ل | ك | ق | ف | غ | ع | ظ | ط | ض | ي | و | ه | ن | م | |
| ص | ش | س | ز | ر | ذ | د | خ | ح | ج | ث | ت | ب | أ | ش ص |
| ك | ق | ف | غ | ع | ظ | ط | ض | ي | و | ه | ن | م | ل | |
| ص | ش | س | ز | ر | ذ | د | خ | ح | ج | ث | ت | ب | أ | ض ط |
| ق | ف | غ | ع | ظ | ط | ض | ي | و | ه | ن | م | ل | ك | |
| ص | ش | س | ز | ر | ذ | د | خ | ح | ج | ث | ت | ب | أ | ظ ع |

| | ق | ك | ل | م | ه | و | ي | ض | ط | ظ | ع | غ | ف |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| غ ف | أ | ب | ت | ث | ج | ح | خ | د | ذ | ر | ز | س | ش | ص |
| | ف | ق | ك | ل | م | ن | ه | و | ي | ض | ط | ظ | ع | غ |
| ق ك | أ | ب | ت | ث | ج | ح | خ | د | ذ | ر | ز | س | ش | ص |
| | غ | ف | ق | ك | ل | م | ن | ه | و | ي | ض | ط | ظ | ع |
| ل م | أ | ب | ت | ث | ج | ح | خ | د | ذ | ر | ز | س | ش | ص |
| | ع | غ | ف | ق | ك | ل | م | ن | ه | و | ي | ض | ط | ظ |
| ن ه | أ | ب | ت | ث | ج | ح | خ | د | ذ | ر | ز | س | ش | ص |
| | ظ | ع | غ | ف | ق | ك | ل | م | ن | ه | و | ي | ض | ط |
| و ي | أ | ب | ت | ث | ج | ح | خ | د | ذ | ر | ز | س | ش | ص |
| | ط | ظ | ع | غ | ف | ق | ك | ل | م | ن | ه | و | ي | ض |

**Decryption : (1.5 pt)**

| Ciphertext | ك | ش | ق | ر | غ | ر | ب | ب | س | ف | غ | ش |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key | ط | ر | و | ا | د | ة | ط | ر | و | ا | د | ة |
| Plaintext | ا | ل | ح | م | د | ل | ل | ه | و | ح | د | ه |

**Decrypted message = الحمد لله وحده (0.5 pt)**

**Exercise n°2 (8 pts):** Consider two entities, denoted as A (the sender) and B (the recipient). Sender A possesses the cryptographic parameters: n=143, e=7, and d=103, whereas recipient B is associated with the cryptographic parameters: n=85, e=5, and d=13. To ensure both the **authenticity** and **integrity** of the messages exchanged, the two entities agree to utilize a cryptographic hash function in conjunction with public-key encryption mechanisms (**See Part 4: Combination of Hash function with Public Key Encryption**).

Assume that sender A wishes to transmit the plaintext password "ZYXWV" to recipient B. Furthermore, assume that the sender generates the hash by converting the password into its corresponding alphabetic positions (mod 26) and expressing the result in hexadecimal format.

1) List with details the different steps that the two entities should follow.

**Sender A procedure: (2.75 pts)**

a. Sender A sends its Public key (n=143, e=7) and plaintext password "ZYXWV" to Recipient B **(0.25 pt)**

b. Sender A generates password Hash **(01 pt)**

ZYXWV = (25, 24, 23, 22, 21) mod 26 = (19, 18, 17, 16, 15) HEX

Hash = (19, 18, 17, 16, 15)

c. Sender A encrypts Hash using his private key d = 103 **(1.25 pt)**

$S(19) = 19^{103} \pmod{143} = 72$, $S(18) = 18^{103} \pmod{143} = 112$, $S(17) = 17^{103} \pmod{143} = 95$, $S(D) = 16^{103} \pmod{143} = 81$, $S(15) = 15^{103} \pmod{143} = 141$

Encrypted Hash = (72, 112, 95, 81, 141)

d. Sender A sends encrypted Hash **(0.25 pt)**

**Recipient B procedure: (2.75 pts)**

e. Recipient B generates Hash of plaintext password **(01 pt)**

ZYXWV = (25, 24, 23, 22, 21) mod 26 = (19, 18, 17, 16, 15) HEX

Hash = (19, 18, 17, 16, 15)……(Hash 1)

f. Recipient B decrypts received encrypted Hash using Sender A public key n = 143, e = 7 **(1.25 pt)**

Encrypted Hash = (72, 112, 95, 81, 141)

P(72) =$72^7$ (mod 143) = 19, P(112) =$112^7$ (mod 143) = 18, P(95) =$95^7$ (mod 143) = 17, P(81) =$81^7$ (mod 143) = 16,

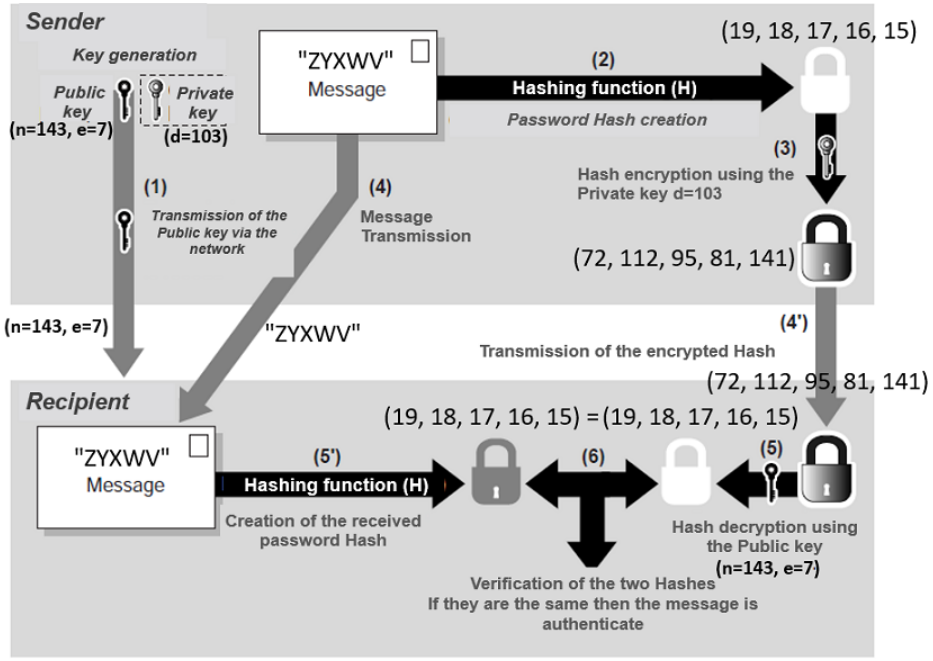
P(141) =$141^7$ (mod 143) = 15

Decrypted Hash = (19, 18, 17, 16, 15)……(Hash 2) **(0.25)**

Compare Hash 1 with Hash 2 **(0.25 pt)**

**(Hash 1) = (Hash 2)**

2) Diagram the security protocol **(2.5 pts)**




**Combination of Hash function with Public-Key Encryption**