Name: Duong Dinh Hung Exam code: 10(-01)
Student ID: BI10-073

INTRODUCTION TO CRYPTO GRAPHY

Ex 1:

+) X = (01100111 00110011 00011111)
+) Y = (11011101 11011101 11011101 1111)
+) Z = (11010001 10100011 01000111)

⊛ Iteration 1:

+) $x_8 = 0$
+) $y_{10} = 0$
+) $z_{10} = 1$
⇒ $m = major(0,0,1) = 0$

+) $x_8 = m$
⇒ $t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18}$
$= 1 \oplus 0 \oplus 1 \oplus 1$
$= 1$

⇒ Shift X to the right 1 step and $x_0 = t = 1$:
X = (10110011 00110011 00110011)

+) $y_{10} = m$
⇒ $t = y_{20} \oplus y_{21}$
$= 1 \oplus 1$
$= 0$

⇒ Shift Y to the right 1 step & $y_0 = t = 0$:
Y = (01101110 11101110 11101110 1111)

+) $z_{10} \neq m$ ⇒ No action

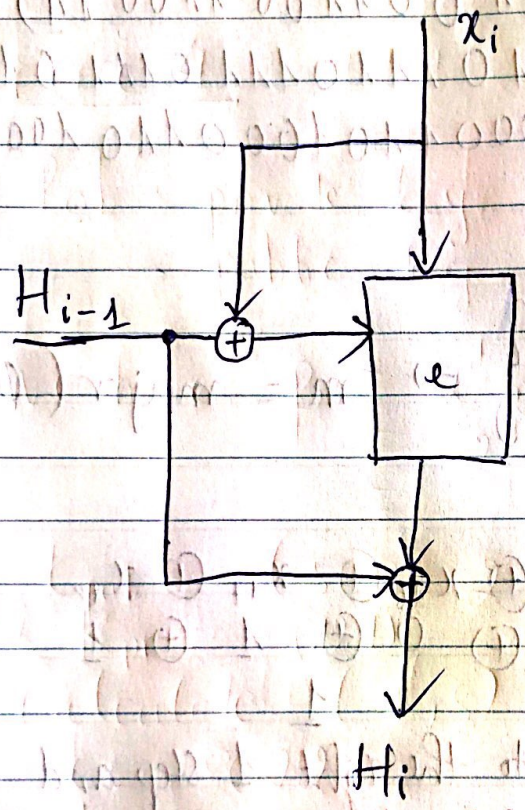
⇒ Key stream bit = $x_{18} \oplus y_{21} \oplus z_{22}$
$= 1 \oplus 1 \oplus 1 = 1$

⊛ Do the same process with iteration 2 and 3.

⇒ ~~Final~~ Next 3 keystream bits are : 1 1 1

Exercise 2:

→ Block diagram :



$$H_i = e(x_i \oplus H_{i-1}, x_i) \oplus H_{i-1}$$

Exercise 3:

1) Describe RSA :

⊛ Key generation :

- Select p and q (large prime)
- Calculate $N = p \cdot q$
- Compute $\phi(N) = (p-1)(q-1)$

+) Select e co-prime to $\phi(N)$

$\Rightarrow$ (N, e) : public key

+) Compute d such that $e.d \equiv 1 \pmod{\phi(N)}$

$\Rightarrow$ d : private key.

⊛ Encryption :

+) Suppose we have M - plain text.

$\Rightarrow$ Cipher text : $C = M^e \pmod{N}$

⊛ Decryption.

+) From the ciphertext C achieved.

$\Rightarrow$ Plaintext : $M = C^d \pmod{N}$

2) +) p = 211

+) q = 97

$\Rightarrow \begin{cases} N = p.q = 20467 \\ \phi(N) = (p-1)(q-1) = 20160. \end{cases}$

+) As we can see, $e_2 = 89$ and $\phi(N) = 20160$ are co-prime, while ~~e_1 is~~ $e_1 = 91$ is not (common divisor = 7)

$\Rightarrow$ $e_2 = 89$ is valid.

3) +) Public key : (N, e) = (20467, 89)

+) Find d such that :

$e.d \equiv 1 \pmod{20160}$

$(=) \quad 89d \equiv 1 \pmod{20160}$

$(=) \quad d \equiv 6569 \pmod{20160}$

$\Rightarrow$ Private key : ⊛ d = 6569

+) M = 5022

⇒ { Encrypt: $C \equiv M^e \pmod N$

⇔ $C \equiv 5022^{89} \pmod{20467}$

$\equiv 1142 \pmod{20467}$

Decrypt: $M \equiv C^d \pmod N$

$\equiv 1142^{6569} \pmod{20467}$

$\equiv 5022 \pmod{20467}$

Exercise 4:

+) Bob's private key: $K_{pr} = (d) = (127)$

public key: $K_{pub} = (p, \alpha, \beta)$

$= (509, 2, \beta)$.

+) We have: $\beta \equiv \alpha^d \pmod p$

$\equiv 2^{127} \pmod{509}$

$\equiv 301 \pmod{509}$

⇒ { $K_{pub} = (509, 2, 301)$

$K_{pr} = (127)$

1) Calculate (r, s)

+) $x = 8022$

+) $k_E = 215$

+) $r \equiv \alpha^{k_E} \pmod p$

$\equiv 2^{215} \pmod{509}$

$\equiv 249 \pmod{509}$

+) $s \equiv (x - dr) \cdot k_E^{-1} \pmod{p-1}$

$\equiv (8022 - 127.249) \cdot 215^{-1} \pmod{508}$

$\equiv -23601 \cdot 267 \pmod{508}$

$\equiv 273 \pmod{508}$

⇒ Elgamal signature : $(r, s) = (249, 273)$

2) + $(x_1, r_1, s_1) = (22, 249, 413)$.

+) We have:

$$t_1 \equiv \beta^{r_1} \cdot r_1^{s_1} \bmod p$$

$$\equiv 301^{249} \cdot 249^{413} \bmod 509$$

$$\equiv 301 \cdot 430 \bmod 509$$

$$\equiv 144$$

+) $\alpha^{x_1} \bmod p \equiv 2^{22} \pmod{509}$

$$\equiv 144 \pmod{509}.$$

⇒ Message (x_1, r_1, s_1) from Bob.

+) $(x_2, r_2, s_2) = (82, 249, 342)$

⇒ $t_2 \equiv 301^{249} \cdot 249^{342} \pmod{509}$

$$\equiv 301 \cdot 26 \pmod{509}$$

$$\equiv 194$$

+) $\alpha^{x_2} \bmod p \equiv 2^{82} \bmod 509$

$$\equiv 173$$

⇒ Message (x_2, r_2, s_2) not from Bob.

3) → $ID(A) = 1$; $ID(B) = 2$

+) $k_E = 213$ (A)

$k_E = 215$ (B)

+) $x_A = 4b_A + ID(A) = 4 \cdot 2022 + 1$

$$= 8089$$

+) $x_b = 4 \cdot 2602 + 2 = 10410$.

(8) For A:

$x = 8089$

$k_E = 213$

$$\begin{cases} r = \alpha^{k_E} \pmod p \\ \quad = 2^{213} \bmod 509 \\ \quad = 449 \\ s = (x - dr)\, k_E^{-1} \pmod{p-1} \\ \quad = (8089 - 127 \cdot 449) \cdot 213^{-1} \pmod{508} \\ \quad = -48299 \cdot 477 \pmod{508} \\ \quad = 193 \end{cases}$$

(8) For B:

$x = 10410$

$k_E = 215$

$$\begin{cases} r = \alpha^{k_E} \pmod p \\ \quad = 2^{215} \pmod{509} \\ \quad = 249 \\ s = (x - dr) \cdot k_E^{-1} \pmod{p-1} \\ \quad = -2213 \cdot 215^{-1} \pmod{508} \end{cases}$$

⇒ Elgamal signature : $(r, s) = (249, 273)$

2) + $(x_1, r_1, s_1) = (22, 249, 413)$.

+) We have:

$$t_1 \equiv \beta^{r_1} \cdot r_1^{s_1} \bmod p$$

$$\equiv 301^{249} \cdot 249^{413} \bmod 509$$

$$\equiv 301 \cdot 430 \bmod 509$$

$$\equiv 144$$

+) $\alpha^{x_1} \bmod p \equiv 2^{22} \pmod{509}$

$$\equiv 144 \pmod{509}.$$

⇒ <u>Message (x_1, r_1, s_1) from Bob.</u>

&

+) $(x_2, r_2, s_2) = (82, 249, 342)$

⇒ $t_2 \equiv 301^{249} \cdot 249^{342} \pmod{509}$

$$\equiv 301 \cdot 26 \pmod{509}$$

$$\equiv 194$$

+) $\alpha^{x_2} \bmod p \equiv 2^{82} \bmod 509$

$$\equiv 173$$

⇒ <u>Message (x_2, r_2, s_2) not from Bob</u>.

3) → $ID(A) = 1$; $ID(B) = 2$

+) $k_E = 213$ (A)

$k_E = 215$ (B)

+) $x_A = 4b_A + ID(A) = 4 \cdot 2022 + 1$

$$= 8089$$

+) $x_B = 4 \cdot 2602 + 2 = 10410$.

(a) For A:

$x = 8089$

$k_E = 213$

$$\begin{cases} r = \alpha^{k_E} \pmod p \\ \quad = 2^{213} \bmod 509 \\ \quad = 444 \\ s = (x - dr)\, k_E^{-1} \pmod{p-1} \\ \quad = (8089 - 127 \cdot 444) \cdot 213^{-1} \pmod{508} \\ \quad = 48299 \cdot 477 \pmod{508} \\ \quad = 193 \end{cases}$$

(b) For B:

$x = 10410$

$k_E = 215$

$$\begin{cases} r = \alpha^{k_E} \pmod p \\ \quad = 2^{215} \pmod{509} \\ \quad = 249 \\ s = (x - dr) \cdot k_E^{-1} \pmod{p-1} \\ \quad = 21213 \cdot 215^{-1} \pmod{508} \end{cases}$$