* Cryptography *

Topics:

- RSA
- diffie hellmen
- El Gamal

[I] RSA

(You need to do 3 steps to encrypt & decrypt)

① Key generation

1- choose two prime numbers

$p, q = (3, 7)$

2- Compute n

$n = p * q = 3 * 7 = \boxed{21}$

3- Compute ϕ euler

$\phi = (p-1)(q-1) = 2 * 6 = \boxed{12}$

4- choose "e" $\Rightarrow 1 < e < \phi$

+ coprime with ϕ

(يعني تشوف رقم بين 12 → 1 بشرط
ميقبلش القسمة على $\phi = 12$)

~~∴ e 5, 7, 8, 9, 10, 11 ممكن تكون e ∴~~

وميكونش في عامل مشترك بينهم غير الواحد

$12 \rightarrow 8, 4, 2, 1$

$\boxed{e = 7}$ (5, 7, 11) ممكن تكون

② Encryption

$\boxed{C = M^e \bmod n}$

Message = 'H' = 4

$\therefore C = 4^7 \bmod 21$

$= 16384 \bmod 21$

$16384 \div 21 = 780{,}19$

$780 * 21 = 16380$

$16384 - 16380 = \textcircled{4}$

③ Decription

$\boxed{M = C^d \bmod n}$

$\boxed{d = e^{-1} \bmod \phi}$

$d = 7^{-1} \bmod 12$

$= 7 * d \bmod 12 = 1$

$\boxed{d = 7}$

$\therefore M = 4^7 \bmod 21$

$= 4$

[2] Diffie Hellman

- a, b → Secret keys of Alice / Bob → private
- p → Big prime number
- g → Smaller than 'p' → Public

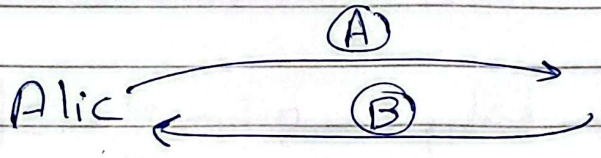
① Alice calculate A:

$A = g^a \bmod p$

② Bob Calaclate B

$B = g^b \bmod p$

بعتكده Alice لـ A الـ بعت Bob وكمان Bob لـ B بعت



② Alic Calc key:

$K = B^a \bmod p$

② Bob Calc key:

$K = A^b \bmod p$

* علشان تتأكد أن حلك صح لازم الـ keys تكون متساوية.

3 El-Gamal

Encryption

inputs: M or C, x_A, q, k, a

Decryption

① $Y_A = a^{x_A} \bmod q$

② $K = (Y_A)^{k} \bmod q$

③ $C_2 = K \cdot M \bmod q$

① $C_1 = a^{k} \bmod q$

② $K = (C_1)^{x_A} \bmod q$

③ $M = C \cdot K^{-1} \bmod q$ (message, cipher, key)

EX 1) Encrypt this message:
$M = 17$, $x_A = 5$, $q = 19$, $k = 6$, $a = 10$

① $Y_A = a^{x_A} \bmod q = 10^{5} \bmod 19 = 3$

② $K = (Y_A)^{k} \bmod q = (3)^{6} \bmod 19 = 7$

③ $C_2 = K \cdot M \bmod q = 7 * 17 \bmod 19 = 5$

if $K = 7$

$K^{-1} = ?$

$7^{-1} = ?$

$7 * N \bmod 19 = 1$

(Try until the res = 1)

$7 * 1 \bmod 19 = 7$ X

$7 * 2 \bmod 19 = 14$ X

⋮

$7 * 11 \bmod 19 = 1$

EX 2) Decrypt this cipher: $C = 5$

① $C_1 = a^{k} \bmod q = 10^{6} \bmod 19 = 11$

② $K = (C_1)^{x_A} \bmod q = (11)^{5} \bmod 19 = 7$

③ $M = C \cdot K^{-1} \bmod q = 5 * 11 \bmod 19 = 17$

How?

Quiz (2)

Q1) RSA

M=3, (P,Q) = (13,7)

Solution

- $n = p * q = 91$
- $\phi = (p-1)(q-1) = 12 * 6 = 72$
- $1 < e < 72$ but she want $1 < e < 10$

(Try numbers from 1 → 10)

$72 \div 2 = 36$ X
$72 \div 3 = 24$ X
$72 \div 4 = 18$ X
$72 \div 5 = 14.4$ ✓
$72 \div 6 = 12$ X
$72 \div 7 = 10.2$ ✓
$72 \div 8 = 9$ X
$72 \div 9 = 8$ X

∴ "e" can be (5) or (7) both are True.

- Let $e = 5$

$$\text{Cipher} = M^e \bmod n$$
$$= 3^5 \bmod 91$$
$$243 \bmod 91$$
$$243 \div 91 = 2.6$$
$$2 * 91 = 182$$
$$243 - 182 = 61$$

∴ Cipher = 61 ⟹ #

Q3) El-Gamal

Message (M) = 14
Alice's private key (X_A) = 5
prime number (q) = 23
Generator (α) = 4
Random number (K) = 3

- Engrypt this Message

Solution

unknown

$$\text{Cipher} = K.M \bmod q$$

- Alice's public key $(Y_A) = \alpha^{X_A} \bmod q$

$= 4^5 \bmod 23$

$1024 \div 23 = 44.5$

$44 * 23 = 1012$

$1024 - 1012 = 12$

$\therefore Y_A = 12$

- Key $(K) = (Y_A)^K \bmod q$

$= (12)^3 \bmod 23$

$1728 \div 23 = 75.13$

$75 * 23 = 1725$

$1728 - 1725 = 3$

$\therefore K = 3$

$\therefore$ Cipher $= K.M \bmod q = 3 * 14 \bmod 23 = 19$

#

Q2) Diffie-Hellman

$p = 23$
$g = 5$
Alice's private key (a) = 4
Bob's private key (b) = 3
Mallory's private key used with Alice (m_1) = 6
Mallory's " " " " Bob (m_2) = 7

Solution

Private key used with Alice ← $m_1 = 6$
Used with Bob ← $m_2 = 7$

private key ← $a = 4$

Bob's private key ← $b = 3$

Alice | **Mallory** | **Bob**

Alice: $A = g^a \bmod p$
$= 5^4 \bmod 23$
(public key)

Mallory (public key used for Alice): $M_1 = g^{m_1} \bmod p$
$= 5^6 \bmod 23$

$\therefore A = 4$ ⟷ $\therefore M_1 = 8$

Alice: $Key = M_1^a \bmod p$
$= 8^4 \bmod 23$

Bob: $Key = A^{m_1} \bmod p$
$= 4^6 \bmod 23$

$\therefore Key = 2$ (same) $\therefore Key = 2$

Mallory: $M_2 = g^{m_2} \bmod p$
$= 5^7 \bmod 23$

Bob: $B = g^b \bmod p$
$= 5^3 \bmod 23$

$\therefore M_2 = 17$ ⟷ $\therefore B = 10$

Mallory: $Key = B^{m_2} \bmod p$
$= 10^7 \bmod 23$

Bob: $Key = M_2^b \bmod p$
$= 17^3 \bmod 23$

$\therefore Key = 14$ (same) $\therefore Key = 14$