25/1/23 CSS

Page No.
Date

→ RSA

(I) Key Generation:

1. Select 2 prime nos p & q
2. Calculate $n = p \times q$
3. Calculate $\phi(n) = (p-1)(q-1)$
4. Choose the value of e, such that $1 < e < \phi(n)$ & $\gcd(\phi(n), e) = 1$
5. Calculate d
   $d = e^{-1} \bmod \phi(n)$
   $ed = \bmod \phi(n)$, $ed \bmod \phi(n) = 1$
6. Public key $= (e, n) \Rightarrow$ Encryption.
7. Private key $= (d, n) \Rightarrow$ Decryption.

(II) Encryption

$$\boxed{c = m^e \bmod n}$$

m = no of digit in msg (PT)
c = cipher text
Assume $(m < n)$

(III) Decryption

$$(PT) = c^d \bmod n$$

2-75

2 | 20
2 | 10
5 | 5
1

Page No.
Date

eg. $p = 3 \quad q = 11$ ① $n = 33$

② $\phi(n) = (p-1) \times (q-1) = 2 \times 10 = 20$

③ $e = ? \quad \ldots \quad 1 < e < \phi$

$\gcd(\phi n, e) = 1$

$d(n) = 20 = 2, 2, 5$

$e = 7$

4

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

~~$ed = \bmod \phi(n) = 1$~~

5

$ed = \bmod \phi(n)$

$ed \bmod \phi(n) = 1$

$7 \times d \bmod \phi(n) = 1$

$7 \times d \bmod (20) = 1$ mod 7

$7 \times 3 \bmod (20)$ $(21 - 21 \div 20 \times 20)$

$\boxed{d = 3}$

⑥ (e, n) public key ; (d, n) private key

$(7, 33)$ $(3, 33)$.

11. $c = m^e \bmod n$

$m = \text{message} = 31$

$= 31^7$

$[(31)^3 \bmod (33)]$. $(31^3) \bmod 33$. $31^1 \bmod 33$

$29791 \bmod 33$ $29791 \bmod 33$.

25 25 31

$$PT = C^d \bmod n$$
$$= 4^{(3)} \bmod 33$$
$$= 31$$

$p = 7, q = 13, M = 42$

→ $d = \frac{1 + k(\phi(n))}{e}$

$n = p * q = 7 \times 13$

$= 91$

$n = 91$

$(p-1)(q-1) = 12 \times 6 = 72$

$1 < e < \phi$

$e = 5$

$= \frac{1 + 2(72)}{5}$

$d = 29.$

public $(e, n) = (5, 91)$ private $(d, n) = (29, 91)$

$C = me \bmod n$

$= 42^5 \bmod 91$

$= 130691232 \bmod 91$

$= \boxed{35}$

$P.T. = C^d \bmod n$

$= 35^{29} \bmod 91$ —

6, 6, 6,

P.T = $35^{29} \bmod 91$

$= (35^6 \bmod 91) \cdot (35^6 \bmod 91) \cdot (35^6 \bmod 91)$
$(35^4 \bmod 91) \cdot (35^5 \bmod 91)$

$= 1838263625 \bmod 91$

$= 14 \times 14 \times 14 \times 14 \times 42$

$= 1613472 \bmod 91$

P.T = 42.

$35^{-5} = 52521875$

31/1/23

CSS

— Knapsack Algorithm.

(I.) Key Generation

1. Public Key
2. Private Key

select 2 no. n & m.

m > sum of all nos in sequence.

n = select no such that no common factor with m.

Find public key → $(Bi \times n) \bmod m$ (plaintext)

(II.) Encryption ⇒ $CT = (PTi \times Pubi) + (PTj \times Pubj) + (PTn \times Pubn)$

III Decryption : Calculate n^{-1} ⇒ get x

$(CT \times x) \bmod m$

eg) {1, 2, 4, 10, 20, 40} = wts.

D = {1, 2, 4, 9, 20, 40} = private key

sum = 787

m > sum

m = 110 n = 31

2, 5, 11

→ Public Key (Di × n) mod m

(1 × 31) mod 110 = 31

(2 × 31) mod 110 = 62

(4 × 31) mod 110 = 14

(9 × 31) mod 110 = 90

(20 × 31) mod 110 = 70

(40 × 31) mod 110 = 30

→ PT = 10010011110010110

C·T = (PTi × Pubi) + (PTj × Pubj) + .. (PTn × Pubj)

1st PT C1 = (1 × 31) + (0 × 62) + (0 × 14) + (1 × 90) + (0 × 70) + (0 × 30)

= 121

2nd PT C2 = (1 × 31) + (0 × 62) + (1 × 14) + (1 × 90) + (0 × 70) + (0 × 30)

= 197

3rd PT C3 = (1 × 31) + (0 × 62) + (1 × 14) + (1 × 90) + (1 × 70) + (0 × 30)

= 205

Page No.
Date

Decrypⁿ : $n^{-1} = 31^{-1}$

$31 \times x \bmod 110 = 1$

$31 \times 71 \bmod 110 = 1$

$1 = 1$

$\boxed{x = 71}$

$(CT \times x) \bmod m$

$CT = 121, 197, 205$

$D = \{1, 2, 4, 10, 20, 40\}$

$(121 \times 71) \bmod 110 = 11$

100100

$(197 \times 71) \bmod 110 = 17$

111100

$(205 \times 71) \bmod 110 = 35$

101110

Q2.) $b = \{1, 2, 4, 7, 12, 20, 33, 54\}$ → private key

$n = 147$, $m = 250$

P.T = 01100110

Q3.) $b = \{2, 3, 6, 13, 27, 52\}$ → private key

$m = 105$, $n = 31$

P.T = 110101

2/1/23

CSS

→ Diffie - Hellman key {Exchange Algo}

1.) Consider a prime no. 'q'
2.) select α .... $\boxed{\alpha < q}$ & α is primitive root of q
3.) X_A .... $\boxed{X_A < q}$ .... (X_A private key of A)

$$\boxed{Y_A = \alpha^{X_A} \bmod q}$$

X = pvt key
Y = pub " "

4.) X_B (Pvt key of B) & $X_B < q$

$$\boxed{Y_B = \alpha^{X_B} \bmod q}$$

$$K_1 = Y_B^{X_a} \bmod q$$

$$K_2 = Y_A^{X_b} \bmod q$$

Page No.
Date

1) $X_A = 3$; $X_B = 4$, $q = 7$, $\alpha = 5$

$$Y_A = \alpha^{X_A} \bmod q$$
$$= 5^3 \bmod 7$$
$$= 6$$

$$Y_B = \alpha^{X_B} \bmod q$$
$$= 5^4 \bmod 7$$
$$= 2$$

$$K_1 = Y_B^{X_a} \bmod q$$
$$= 2^3 \bmod 7$$
$$= 1$$

$$K_2 = Y_A^{X_b} \bmod q$$
$$= 6^4 \bmod 7$$
$$= 1$$

Q2) ELGamal Cryptography

I. Key Generation

1. select large prime no. P
2. select decrypⁿ key D
3. select encrypⁿ key or E_1
4. select $E_2 = E_1^D \bmod P$
5. Public key (E_1, E_2, D, P)

II. Encrypⁿ

1) select random integer

2)

$(C_1^D)^{-1} \rightarrow (C_1^D)x \bmod p = 1$

EL Gamal

Page No.
Date

Q.) P.T = 7

private key = 3, $E_1 = 2$, prime no = 11

Soln :

$E_2 = E_1^D \bmod p$

$= 2^3 \bmod 11$

$= 8$

public key (2, 8, 3, 11)

II Encryn

$R = 2$

$C_1 = E_1^R \bmod p$

$C_1 = 2^2 \bmod 11$

$C_1 = 4$

$C_2 = (PT \times E_2^R) \bmod p$.

$= 7 \times 8^2 \bmod 11$

$C_2 = 8$.

$CT = (4, 8)$

III Decrypn

$PT = [C_2 \times (C_1^D)^{-1}] \bmod p$

$= 8 \times (4^3)^{-1} \bmod 11$

$= 8 \times 5 \bmod 11$

$= 7$