classmate
Date
Page

Asymmetric Key Cryptography

★ **Diffie Hellman key exchange:** method to exchange key

$\alpha \rightarrow$ primitive root

$X \rightarrow$ private

$Y \rightarrow$ public

$Y_a = \alpha^{X_A} \bmod q$ i.e. $\boxed{\underset{\text{(public A)}}{Y_A} = \text{root}^{\text{private B}} \bmod q}$

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

$K_1 = X_B^{X_A} \bmod q$

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

$K_1 = K_2$ } if true the DHKE successful

Q1) $X_A = 3,\ X_B = 4\ \ \alpha = 5\ \ q = 7$

Ans $Y_A = 5^3 \bmod 7 = 6$

$Y_B = 5^4 \bmod 7 = 2$

$K_1 = 2^3 \bmod 7 = 1$

$K_2 = 6^4 = 1$ i.e. successfull

RSA - 2048

RSA-2048 is most common with AES-256

$p, q \rightarrow$ prime no

$n = p \times q$

$\phi(n) = (p-1) \times (q-1)$ $\rightarrow$ Totient factor

check $e \Rightarrow \gcd(e, \phi(n)) = 1$ } public

$d \equiv e^{-1} \bmod (\phi(n))$ } private

public $= (e, n)$

private (d, n)

$C = P^e \bmod n$

$P = C^d \bmod n$

P.T.O

Q) $P = 13$, $q = 11$, $e = 13$, $P_T = 13$

Ans

$n = 13 \times 11 = 143$

$\phi n = (12 \times 10) = 120$

$gcd(e, n) = 1$ i.e ✓

$$\boxed{d = \frac{(\phi(n) \times i) + 1}{e} \rightarrow i = 1 \ldots n}$$

↳ do this 'till you get a whole no

↳ $d = \frac{120 + 1}{13} = 9.3$ ✗

⋮

$d = \frac{120 \times 4 + 1}{13} = 37$ ✓

i.e whole no

$\therefore d = 37$

$CT = P^{e} \bmod n$

$= 13^{13} \bmod 143$

Method — fast exponentiation method

$52^{37} \bmod 143 \rightarrow b^{e} \bmod n$

$37 = (100101)_2$

Rules →

Binary digit $= 0 \Rightarrow rem^2 \bmod n \rightarrow F$

$1 \rightarrow rem^2 \bmod n$
$= ans$
$ans \times base \bmod n \rightarrow F$

1	0	0	1	0	1
52	$52^2 \bmod 143$ 130	$130^2 \bmod 143$ 26	$26^2 \bmod 143$ 104 ↓ base $104 \times 52 \bmod 143$ $= 117$	$117^2 \bmod 143$ 104	$104^2 \bmod 143$ 91 $91 \times 52 \bmod$ 13

redo

1	0	0	1	0	1
52	$52^2 \bmod 143$ 130				

Elgamal

public = e_1 e_2 p

private d

$e2 = e_1^d \bmod p$

$C1 = e_1^r \bmod p$

$C2 = (msg \times e_2^r) \bmod p$

$msg = C_2 \, C_1^{-d} \bmod p$

$\boxed{\text{Fermat}}$

$msg = C_2 \, C_1^{p-1-d} \bmod p$

Ans $p = 11$ $d = 5$ $e_1 = 2$ $r = 4$

$msg = 7$

Ans $e_2 = e_1^d \bmod p$

$= 2^5 \bmod 11$

$= 10$

* Rabin Cryptosystem :-

$C_T = Msg^2 \mod n$

$Msg = C_T^{\frac{1}{2}} \mod n$

a, b, mp, mq

$p = 23$, $q = 7$

$msg = 24$

$p \,\&\, q \equiv 3 \mod 4$

congruent

$23 \mod 4 = 3$ ✓

$7 \mod 4 = 3$ ✓

$n = p \times q = 161$

$C_T = 24^2 \mod 161$

$= 93$

* $m_p = C_T^{(p+1)/4} \mod p$

* $m_p = C_p^{\frac{(p+1)}{4}} \bmod p$

$\therefore m_p = 93^{\frac{(23+1)}{4}} \bmod 23$

$= 1$

* $m_q = 93^{\frac{23+1}{4}} \bmod 7$

$= 4$

* $a \times p + b \times q = 1$ } check this

by extended euclidean algo with modifications

$s = s_1 - q s_2$

$t = t_1 - q t_2$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
3	23	7	2	1	0	1	0	1	−3
3	7	2	1	0	1	calc $\boxed{-3}$	1	−3	calc $\boxed{10}$
2	2	1	0	1	−3	7	−3	10	−23
	1	0		−3	7		10	−23	

$\boxed{\begin{aligned} s_1 &= a = -3 \\ t_1 &= b = 10 \end{aligned}}$

check

$-3(23) + 10(7) = 1$ ✓

$P_{T1} = (a \times r_q \times p + b \times r_p \times q) \bmod n$

$P_{T2} = n - P_{T1}$

$P_{T3} = a \times r_q \times p - b \times r_p \times q$

$P_{T4} = n - P_{T3}$

we will get these 4 as the PT and users will send a hashed value of the message :-

P_T's :-

116

45

127

24