

$$\sqrt{N} = 2^{\frac{k/2}{2}} = 2^{\frac{\log_2 N}{2}}$$

Cryptography

Bitwise multiplication which is more in instruction set
Date..... Page.....

RSA Algorithm

- ① Select Primes p, q $O(\log p \log q)$
- ② Calculate $n = p \times q$ $O(\log^2 n)$
- ③ Calculate $\phi(n) = (p-1) \times (q-1)$ $O(\log^2 n)$
- ④ Select integer 'e' such that $\gcd(e, \phi(n)) = 1$
- ⑤ Calculate d st $ed \equiv 1 \pmod{\phi(n)}$ or $d = e^{-1} \pmod{\phi(n)}$
- ⑥ Public Key $PU = \{e, n\}$
- ⑦ Private Key $PK = \{d, n\}$

$O(\log^3 n)$

Message $M < n$ Encrypt:- $C = M^e \pmod n$ $O((e+1)\log^2 n)$
 $M = C^d \pmod n$ $O((d+1)\log^2 n)$

Correctness of RSA

$$M = C^d \pmod n$$

$$= (M^e)^d \pmod n \Rightarrow \text{To prove } M = M^{ed} \pmod n$$

Proof

$$ed \equiv 1 \pmod{\phi(n)} \Rightarrow \phi(n) \mid ed - 1$$

$$ed - 1 = k \cdot \phi(n) \Rightarrow ed = 1 + k \cdot \phi(n)$$

Using Result $\Rightarrow M^{k\phi(n)+1} \pmod p = M \pmod p$ | $M^{k\phi(n)+1} \pmod q = M \pmod q$

$$\Rightarrow p \mid M^{k\phi(n)+1} - M \quad \& \quad q \mid M^{k\phi(n)+1} - M \Rightarrow pq \mid M^{k\phi(n)+1} - M$$

$$M^{k\phi(n)+1} - M \pmod n = 0 \Rightarrow \boxed{M^{k\phi(n)+1} \pmod n = M}$$

Case 1:-

$$\gcd(M, p) \neq 1 \quad p \mid M \quad (p \text{ is prime so } p \text{ must divide } M)$$

$$M \pmod p = 0$$

$$M^{k\phi(n)+1} \pmod p = 0$$

LHS = RHS

Case 2:-

$$\gcd(M, p) = 1 \Rightarrow M^{\phi(p)} \equiv 1 \pmod p \quad (\text{Euler's Theorem})$$

$$(M^{\phi(p)})^{\phi(q)} \equiv 1 \pmod p$$

$$M^{\phi(n)} \equiv 1 \pmod p \Rightarrow M^{k\phi(n)} \equiv 1 \pmod p$$

$$\Rightarrow M^{k\phi(n)+1} \equiv M \pmod p$$

if $x \pmod n = 1$
 $x^y \pmod n = 1$

multiply both sides

$M < n$ \Rightarrow if $M > n$ many msg will map to same ciphertext.

RSA :-

$$C = M^e \text{ mod } n = \underbrace{m \times m \times \dots \times m}_{(e-1) \text{ times}} \text{ (mod } n)$$

Exponential Complexity to

Eg

$M^{13} \text{ mod } n$ $m < n$, $M^8 \times M^4 \times M^1$ {use Square & Multiply}
 5 multiplications are needed ~~now~~ now.
 (M^2 \oplus M^4 \oplus M^8 \oplus $M^8 \times M^4 \times M^1$)

$x^k \text{ mod } n$

$O(\log k) \times \log^2 n = O(\log^3 n)$ bit wise operation

- If binary no. containing less no. '1' bits, then multiplication required will be less (eg 3, 17,

Decryption $\Rightarrow M = C^d \text{ mod } n$

$V_p = C^d \text{ mod } p$ $V_q = C^d \text{ mod } q \Rightarrow O(\log^3 \sqrt{n})$

$x_p = q \times q^{-1} \text{ mod } p$ $x_q = p \times p^{-1} \text{ mod } q$

$M = (V_p \times x_p + V_q \times x_q) \text{ mod } n$

$E(PU, M_1) \times E(PU, M_2) = E(PU, m_1 \times m_2)$

$C = M^e \text{ mod } n$, $X = C \times 2^e \text{ mod } n$ x : Chosen ciphertext

$Y = X^d \text{ mod } n \Rightarrow (C \times 2^e)^d \text{ mod } n \Rightarrow C^d \times 2^{ed} \text{ mod } n$
 $= M \times 2 \text{ mod } n$

$M = Y \times 2^{-1} \text{ mod } n$

Diffie-Hellman Key Exchange

Privacy - Public Key Authentication - Private Key

Global Parameters \Rightarrow

- 1) Prime $:- q$
- 2) primitive root of $q: \alpha$

	<u>A</u>	<u>B</u>
Private	$x_A < q$	Private $x_B < q$
Public	$Y_A = \alpha^{x_A} \bmod q$	Public $Y_B = \alpha^{x_B} \bmod q$
Secret key (K_A)	$(Y_B)^{x_A} \bmod q$	Secret key $= K_B = (Y_A)^{x_B} \bmod q$

Claim: $- K_A = K_B$

Proof

$$\begin{aligned}
 K_A &= (Y_B)^{x_A} \bmod q \Rightarrow (\alpha^{x_B} \bmod q)^{x_A} \bmod q \\
 &= (\alpha^{x_B x_A}) \bmod q \Rightarrow (\alpha^{x_A x_B}) \bmod q \\
 &= (Y_A)^{x_B} \bmod q \Rightarrow K_B
 \end{aligned}$$

Example $q = 353$ $\alpha = 3$

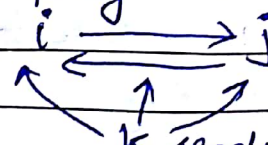
<u>A</u>	<u>B</u>
$x_A = 97$	$x_B = 253$
$Y_A = \alpha^{x_A} \bmod q = 3^{97} \bmod 353$	$Y_B = \alpha^{x_B} \bmod q = 3^{253} \bmod 353$
$= 40$	$= 248$
$K_A = (Y_B)^{x_A} \bmod q$	$K_B = (Y_A)^{x_B} \bmod q$
$= (248)^{97} \bmod 353 = 160$	$= (40)^{253} \bmod 353 = 160$

1..n (users) User i wants to communicate User j then

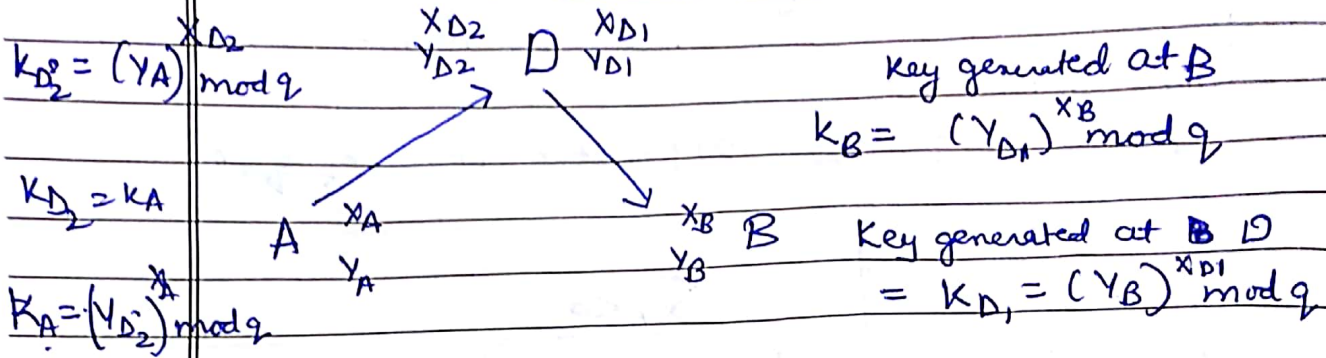
$i \rightarrow j$ $\frac{x_i}{Y_j \bmod q}$ $= k$	$\frac{x_j}{Y_i \bmod q}$ $= k$
---	------------------------------------

• Man in the middle Attack -

- Directory must be trusted
- Replay Attack is possible.



K sends the previous old msg. i & j cannot detect that it is old. Since genuine key is used

Man in the middle Attack -

D is B for A } This attack is possible bcoz there is no authentication of Public key.
 D is A for B }

Digital Certificate issued by trusted authority - so that above attack cannot be done.

$Y_A = \alpha^{X_A} \mod q$ → This can be done in polynomial time
 Q. Given Y_A, α, q , how difficult/easy to compute X_A ?

X_A no. of multiplication needed $\alpha^1, \alpha^2, \dots, \alpha^{X_A}$

It is also a hard problem.

Here computation depends on size of X_A .

d log problem - increase Exponential Complexity.

ElGamal Crypto System →

Global Parameters - 1) Prime q 2) Primitive root of $q = \alpha$

Key Generation

1. Select Private Key $X_A < q-1$
2. Calculate ~~Public Key~~ $Y_A = \alpha^{X_A} \mod q$
3. Public key $PU = \{q, \alpha, Y_A\}$

} (A)

B
Encrypts

Plaintext $M < q$
 Select Random Integer $r < q$
 Calculate $k = (Y_A)^r \bmod q$
 Calculate $C_1 = (\alpha)^r \bmod q$
 Calculate $C_2 = kM \bmod q$
 Cipher Text $C = (C_1, C_2)$

Every msg is
 Randomized.
 For same msg
 in RSA:- same CipherText
 in ElGamal - diff. CipherText

A
Decrypts

CipherText $C = (C_1, C_2)$
 Calculate $K = (C_1)^{X_A} \bmod q$
 Calculate $M = (C_2 K^{-1}) \bmod q$

$$K = (\alpha^r \bmod q)^{X_A} \bmod q$$

$$= (\alpha^{rX_A} \bmod q) \bmod q = (Y_A)^r \bmod q = K(B)$$

Example

$q = 19$
 $\alpha = 10$
 $X_A = 5$ (Private)
 $Y_A = 10^5 \bmod 19 = 3$
 $P_K = \{19, 10, 3\}$

(B)
Encrypts

Msg = ~~16~~ 7, $r = 6$, $k = 3^6 \bmod 19 = 7$
 $C_1 = 10^6 \bmod 19 = 11$ $C_2 = 7 \times 7 \bmod 19 = 5$

(A)
Decrypts

$C = (11, 5) \Rightarrow K = 11^5 \bmod 19 = 7$
 $K^{-1} \bmod q = 7^{-1} \bmod 19 = 11$
 $M = 5 \times 11 \bmod 19 = 17$

Security

- depends on discrete log Problem (X_A is not known)
 Computing X_A is nphard, Breaking this Crypto System is also infeasible
- $(M_1 || M_2 || M_3 || M_4)$