$\sqrt{N} = 2^{k/2} = 2^{\frac{\log_2 N}{2}}$ | Cryptography → Bit ... multiplication ... which is there in instruction set

Date........ Page........

RSA Algorithm

1. Select Primes p, q — $O(\text{MR Prime} t)$
2. Calculate $n = p \times q$ — $O(\log_2^2 n)$
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 $ed \equiv 1 \bmod \phi(n)$ or $d = e^{-1} \bmod \phi(n)$
6. Public Key $PU = \{e, n\}$
7. Private Key $PR = \{d, n\}$

$O(\log^3 n) \Rightarrow \log n \times \log n \times \log n$

$O(\log^3 n)$ Message $M < n$ Encrypt :- $C = M^e \bmod n$ — $O((e-1)\log^2 n)$

$M = C^d \bmod n$ — $O((d-1)\log^2 n)$

Correctness of RSA

$e, d \Rightarrow \log n$ bits size

$M = C^d \bmod n$

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

Proof: $ed \equiv 1 \bmod \phi(n) \Rightarrow \phi(n) \mid ed - 1$

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

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

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

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

Case 1:- $\gcd(M, p) \neq 1$. $p \mid M$ (p is prime so p must divide M)

$M \bmod p = 0$

$M^{k\phi(n)+1} \bmod p = 0$ — LHS = RHS

Case 2: $\gcd(M, P) = 1 \Rightarrow M^{\phi(P)} \equiv 1 \bmod P$ (Euler's Theorem)

$(M^{\phi(P)})^{\phi(q)} \equiv 1 \bmod p$ | if $x \bmod n = 1$, $x^y \bmod n = 1$

$M^{k\phi(n)} \equiv 1 \bmod p \Rightarrow M^{k\phi(n)} \equiv 1 \bmod p$) multiply M both side

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

$\underline{M < n} \Rightarrow$ if $M > n$ many msg will map to same CipherText.

Crypto

Date 3/4/18 Page

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

Exponential complexity ~~to~~

Eg $M^{13} \bmod n$ $m < n$, $M^8 \times M^4 \times M^1$ {use Square & Multiply}

5 multiplications are needed now.

$(M^2, M^4, M^8 \quad M^8 \times M^4 \times M^1)$
 1 2 3 4 5

$x^k \bmod n$

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

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

Decryption ⇒ $M = C^d \bmod n$

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

$X_p = q \times q^{-1} \bmod p \qquad X_q = p \times p^{-1} \bmod q.$

$M = (V_p X_p + V_q X_q) \bmod n$

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

$C = M^e \bmod n$, $X = C \times 2^e \bmod n$ X: Chosen cipherText

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

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

Crypto

Date 5/4/18 Page

Diffie-Hellman Key Exchange

Privacy – Public Key · Authentication – Private key

Global Parameters ⇒

1) Prime :- q 2) primitive root of q : α

	A	B
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.

$K_A = (Y_B)^{X_A} \bmod q \Rightarrow (\alpha^{X_B} \bmod q)^{X_A} \bmod q.$

$= (\alpha^{X_B X_A}) \bmod q \Rightarrow (\alpha^{X_A} \bmod q)^{X_B} \bmod q.$

$= (Y_A)^{X_B} \bmod q \Rightarrow K_B$

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

A	B
$X_A = 97$	$X_B = 253$
$Y_A = \alpha^{X_A} \bmod q = 3^{97} \bmod 353$	$Y_B = \alpha^{X_B} \bmod q = 3^{253} \bmod 353$
$= 40$ ⇄	$= 248$
$K_A = (Y_B)^{X_A} \bmod q$	$K_B = (Y_A)^{X_B} \bmod q$
$= (248)^{97} \bmod 353 = 160$	$= (40)^{253} \bmod q = 160$

1 -- n (users) user i wants to communicate user J then

$i \longrightarrow j$

$Y_J^{X_i} \bmod q$ $= k$ | $Y_I^{X_J} \bmod q$ $= k$

- Directory must be trusted
- Replay Attack is possible.

$i \rightleftarrows j$

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

- Man in the middle Attack-

3rd

Man in the middle Attack –

$K_{D_2} = (Y_A)^{X_{D2}} \bmod q$

X_{D2}, Y_{D2} D X_{D1}, Y_{D1}

Key generated at B

$K_B = (Y_{D_1})^{X_B} \bmod q$

$K_{D_2} = K_A$

A X_A, Y_A

X_B, Y_B B

Key generated at ~~B~~ D

$= K_{D_1} = (Y_B)^{X_{D1}} \bmod q$

$K_A = (Y_{D_2})^{X_A} \bmod q$

$K_D = K_B$.

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.

$Y_A = \alpha^{X_A} \bmod q$ → This can be done in polynomial time

Q. given Y_A, α, q, how ~~diffitt~~ difficult/easy to compute X_A?

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

It is also a hard problem.
Here computation depends on size of X_A.
d log problem. ~~increase~~ Exponential Complexity.

ELGamal CryptoSystem →

Global Parameters – 1) Prime q 2) Primitive root of q : α

Key Generation.

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

} A

Scanned by CamScanner

Crypto

Date 6/4/18 Page

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 $C_2 = k.M \bmod q$

Cipher Text $C = (C_1, C_2)$

Every Msg is Randomized.
For same msg
in RSA :- same Ciphertext
in Elgamal - diff. Ciphertext

A Decrypts.

Cipher Text $C = (C_1, C_2)$

Calculate $K = (C_1)^{X_A} \bmod q$

Calculate $M = (C_2 K^{-1}) \bmod q$

$$k = (\alpha^r \bmod q)^{X_A} \bmod q$$
$$= (\alpha^{X_A} \bmod q)^r \bmod q = (Y_A)^r \bmod q = K_{(B)}$$

Example

$q = 19$
$\alpha = 10$

$X_A = 5$ (Private)
$Y_A = 10^5 \bmod 19 = 3$ $\quad PK_{(A)} = \{19, 10, 3\}$

B Encrypts

$Msg = 17$, $r = 6$, $k = 3^6 \bmod 19 = 7$

$C_1 = 10^6 \bmod 19 = 11$ $\quad C_2 = 7 \times 17 \bmod 19 = 5$

A Decrypts

$C = (11, 5) \Rightarrow K = 11^5 \bmod 19 = 7$

$K^{-1} \bmod q = 7^{-1} \bmod 19 = 11$

$M = 5 \times 11 \bmod 19 = \underline{17}$ ✓

Security

- depends on dlog Problem (X_A is not known)
  Computing X_A is np hard, Breaking this Crypto System is also infeasible
- $(M_1 \| M_2 \| M_3 \| M_4)$