Unit :- II

__/__/____

→ Principle's of Asymmetric Key :-
→ RSA algorithm.
→ Key Management / Exchange
→ Deffie Hellman Algorithm.

PT → Encryption → { } → Decryption → PT

PT → Sender Side

Encryption Algo → Key-1 → Public Key / Private Key

{ } → CT

Decryption Algo → Key-2 → Private Key / Public Key

PT → Receiver Side

RSA :- Rivest Shamir Adleman., developed in 1978.

→ choose p, q , 2 prime numbers.
→ calculate $n = p * q$.
→ calculate $\phi(n) = (p-1)(q-1)$ ≡ totient f^n.
→ choose 'e' such that $1 < e < \phi(n)$; and gcd $((\phi(n)), e) = 1$.
→ choose 'd' such that $ed \bmod \phi(n) = 1$.
→ The Private key is {d, n} and
Public key is {e, n}
* e should be co-prime to $\phi(n)$.
→ to encrypt the msg M, ⇒ $C = M^e \bmod n$. ($M = M$)
→ to decrypt the msg C, ⇒ $M = C^d \bmod n$.

$M^e \bmod n = C$.

Formula to calculate value of d {other than hit & trial}

→ $ed = 1 \bmod \phi(n)$

$d = \frac{(\phi(n) * i) + 1}{e}$ $\quad i = 1, 2, 3, - - - - -$

Put i's value 1 then 2, - -
upto when (d ∈ Z), not any decimal value.

Qu:- $p = 3$, $q = 11$

$n = p * q = 3 \times 11 = 33$

$\phi(n) = (3-1)(11-1) = 2 \times 10 = 20$

Now, choose e.

$1 \leq e < \phi(n)$ $\quad \gcd(\phi(n), e) = 1$.

let $e = 3$. $\quad \gcd(20, 3) = 1$.

Calculation of d:

$e\,d \bmod \phi(n) = 1$

$3 \cdot d \bmod 20 = 1 \Rightarrow \underline{d = 7}$

Same thing $\left\{ d = e^{-1} \bmod \phi(n) \right\}$ $\left\{ e\,d = 1 \bmod \phi(n) \right\}$

Private Key :- $\{7, 33\}$ Public Key :- $\{3, 33\}$

Encrypt :- $C = M^e \bmod n \Rightarrow$ {in question M (Plain text) let, $M = 31$; $M = (4)$ for ez solution will be either given or we have to assume}.

$C = 31^3 \bmod 33$

$C = 4^3 \bmod 33 = 64 \bmod 33 = 31$

Decrypt :- $M = C^d \bmod n$

$= 31^7 \bmod 33$

$= 4$.

Diffie.

Deffie Hellman Key Exchange Algo :-

→ It is not an encryption algo.

→ Deffie Hellman is used to exchange secret key b/w 2 users.

→ Here asymmetric encryption is used to exchange secret key b/w users — Public Key + Private Key.

'a' is primitive root of q if :-

$a^1 \bmod q$

$a^2 \bmod q$

$a^3 \bmod q$ - - - - $a^{q-1} \bmod q$.

gives result :- $\{1, 2, 3, 4, - - - q-1\}$

eg :- if $q = 7$ $\quad a = ?$ $\quad a = 3$; $\underline{\text{Ans.}}$

$3^1 \bmod 7 = 3$

3^2 " $= 2$

3^3 " $= 6$ $\quad \{1, 2, 3, 4, 5, 6\}$

3^4 " $= 4$

3^5 " $= 5$

3^6 " $= 1$

Algo :-

(i) Consider a Prime no. 'q'

(ii) Select α such that it must be the primitive root of q and $\boxed{\alpha < q}$

eg :- 'a' is a primitive root of q if $a^1 \bmod q =$

$a^2 \bmod q$

$a^3 \bmod q$

$a^{q-1} \bmod q$

gives result $\{1, 2, 3, - - - q-1\}$

q > 1

eg:- If $q = 7$ suppose $a = 5$.

$5^1 \bmod 7 = 5$
$5^2 \bmod 7 = 4$
$5^3 \bmod 7 = 6$
$5^4 \bmod 7 = 2$
$5^5 \bmod 7 = 3$
$5^6 \bmod 7 = 1$

$\{1, 2, 3, 4, 5, 6\}$ = Result.

No two remainder should be equal if not then discard that value of a.

X → Private Key Y → Public Key

(iii) Assume X_A (Private key of A) and $X_A < q$
Calculate $Y_A = \alpha^{X_A} \bmod q$.
Public key of A.

(iv) Assume X_B (Private key of B) and $X_B < q$
Calculate $Y_B = \alpha^{X_B} \bmod q$
Public key of B.

Calculate Secret Key:- For this, both sender and receiver will use their Public Keys.

User A:
$K_A = (Y_B)^{X_A} \bmod q$

User B:
$K_B = (Y_A)^{X_B} \bmod q$

If $K_A = K_B$ successful exchange.

eg:- If $q = 7$ (Prime no)
$\alpha < q$ (Primitive root)
Both α and q are public elements (Known to everyone)
$X \rightarrow$ private key
$Y \rightarrow$ public key

→ Key generation of A:-
Private key, $X_A = 3$ $(\because X_A < q)$

→ Calculate Public Key of A:
$Y_A = \alpha^{X_A} \bmod q$
$Y_A = 5^3 \bmod 7 = 125 \bmod 7$
$= 7 \times 17 = 6$.

Key generation of B:
Let private key of B,
$X_B = 4$ $(X_B < q)$
~~$X_B = $~~
$Y_B = \alpha^{X_B} \bmod q$
$= 5^4 \bmod 7 = 2$

Calculate secret key of both A and B:-
User A:-
$K_A = (Y_B)^{X_A} \bmod q$
$= 2^3 \bmod 7 = 1$

User B: $K_B = (Y_A)^{X_B} \bmod q$
$= 6^4 \bmod 7 = 1$

$\therefore K_A = K_B$ (Keys are exchanged successfully)

eg:- Let Sender = A
Receiver = B
Private key = X
Public key = Y
Private key of A :- X_A
Public key of A :- Y_A
Private key of B :- X_B
Public key of B :- Y_B

Key is exchanged with steps:-

Step 1:- (i) One of the party choose two numbers 'q' and 'α'. and exchange with other party.
(ii) 'α' is a primitive root of prime number 'q'.
(iii) Now, both parties know value of 'q' and 'α'.

Step-2 : (iv) Both parties know their own private keys.
(v) Both parties calculate the value of their public key and exchange with each other.
⇒ Private key of A ⇒ X_A
Calculate Public key of A ⇒ $Y_A = (\alpha)^{X_A} \bmod q$.
⇒ Private key of B ⇒ X_B
Calculate Public key of B ⇒ $Y_B = (\alpha)^{X_B} \bmod q$.

Step-3 :- (vi) Both parties receive Public key of each other.
(vii) Now, both can calculate the value of Secret key.
User A: Calculate Secret key
$K_A = (Y_B)^{X_A} \bmod q$.
User B: Calculate Secret key
$K_B = (Y_A)^{X_B} \bmod q$.

$K_A = K_B$ {Key exchange successful}

Qui:- Suppose two parties A and B wish to setup a common secret key b/w themselves using Diffie Hellman key they agree on 7 as modulus and 3 as primitive root. Party A choose 2 and B choose 5 as their resp. secrets. Their diffie Hellman key is :

Sty -
$q = 7 \quad \alpha = 3$
$X_A = 2 \quad X_B = 5$

$Y_A = (3)^2 \bmod 7 = 2$
$Y_B = (3)^5 \bmod 7 = 243 \bmod 7 = 5$

$K_A = (2)^2 \bmod 7 = 4$
$K_B = (5)^5 \bmod 7 = 15625 \bmod 7 = 1$.

$K_A \neq K_B$

$K_A = (5)^2 \bmod 7 = 4$
$K_B = (2)^5 \bmod 7 = 4$

$K_A = K_B$.

Authentication Requirement :-
→ Disclosure
→ Traffic analysis
→ Masquerade
→ Content Modification
→ Sequence Modification
→ Timing Modification
→ Sequence of messages
→ Repudiation.

Authentication function :-
→ Message encryption
→ Message Authentication Code (MAC)
→ Hash function.

Qui:- In RSA algorithm if $p=7$, $q=11$ and $e=13$, what will be value of d.

Sty -
$n = p*q = 7 \times 11 = 77$
$\phi(n) = (7-1)(11-1) = 6 \times 10 = 60$
Now, choose e (these value is given)
$\gcd(\phi(n), e) = 1$.

$e \cdot d \bmod \phi(n) = 1$.
$13 \cdot d \bmod 60 = 1$
$d = 37$.
Encryption = $C = M^e \bmod n$
$= -$

Qui:- In an RSA ; a participant uses 2 prime no. $p=3$, $q=11$ to generate public & private. If private key is 7 then how will text COMPUTER will be encrypted using Public key.

Sty -
$n = p*q = 3 \times 11 = 33$
$\phi(n) = (p-1) \times (q-1) = 2 \times 10 = 20$

e = 3, d = 7

Public Key = (3, 20)

Encrypt: (i) $C = M^e \bmod n$. let m = 3

$C = 3^3 \bmod 20 = 7$

(ii) $C = M^e \bmod n$

$= 15^3 \bmod 20 = 3375 \bmod 20 = (15)$

$C = 13^3 \bmod 20$

$= 169 \times 13 \bmod 20 = 2197 \bmod 20$

$= 17$

$C = 16^3 \bmod 20 = 4096 \bmod 20 = 16$

$C = 21^3 \bmod 20$

A - 2
Z - 26

225 x 15
3375

Message Authentication Code (MAC) :- Cryptographic Checksum

Secret key is used to generate MAC.
MAC is fixed size block of code.
MAC is appended with the message.
The communication parties will share a common secret key used to create MAC.

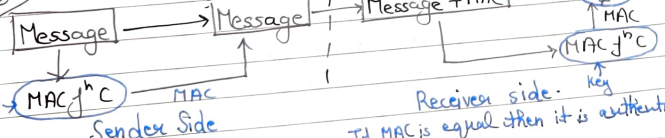
Suppose :- A → Sender B → receiver

A sends mssg. to B it calculates MAC as,

MAC = C(K, M)

MAC function, K: shared secret key, M: Input mssg.

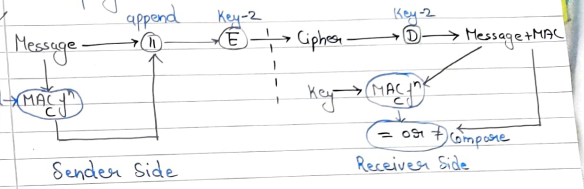
Only authentication - NO confidentiality -



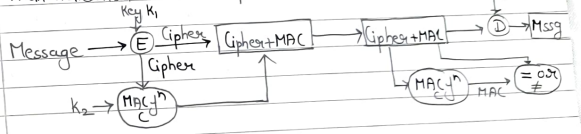
If MAC is equal then it is authentic.

Both Auth. & Confi.

Confidentiality is provided when authentication as well as encryption is also performed.

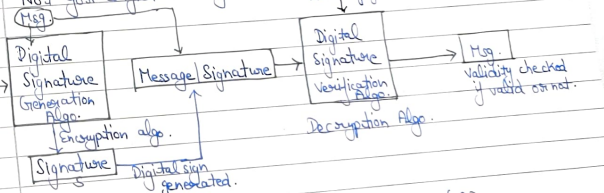


Authentication tied to Cipher Text :-



Digital Signature :- To verify the msg comes from a authenticated user.

→ Plays role in E-commerce, transaction etc.
→ Based on asymmetric key cryptography.
Encryption :- Private key
Decryption :- Public key
→ Used for authentication of msg, non repudiation & msg integrity.
→ Not for confidentiality.



in with DS:

Confidentiality :- achieved through Encryption & Decryption:-

Sender :- Msg → P_{RA} → Signing Algo → Sign → Public Key B → Encryption → Decryption ← Pr.(B) → P_{UA} Message → Verifying algo ← Receiver

El-Gamel Digital Signature :-

Encryption :- Public Key (Y)

Decryption :- Private Key (X)

(i) Select a Prime number q.

(ii) Select a Primitive root α of q.

(iii) Generate a random integer : (Private key of A) : X_A
Such that, $1 < X_A < q-1$

(iv) Compute $Y_A = (\alpha)^{X_A} \bmod q$. {Public Key of A = Y_A}

(v) Generate keys for user (A).
Private key = X_A
Public Key = (q, α, Y_A)

(vi) Generate hash code (m) for message (M):
$m = H(M)$
such that : $0 \le m \le q-1$

(vii) Generate a random integer (K) such that:
$1 \le K \le q-1$ and $\gcd(K, q-1) = 1$.

(viii) Now, Calculate S_1 and S_2.
$S_1 = (\alpha)^K \bmod q$.
$S_2 = K^{-1}(m - X_A S_1) \bmod (q-1)$.

Any other user can verify signature as follows :-

① Compute $V_1 = \alpha^m \bmod q$.

② Compute $V_2 = (Y_A)^{S_1} (S_1)^{S_2} \bmod q$.

Signature valid if $V_1 = V_2$.

Numerical of Hash function, HMAC, CMAC, Schnorr Digital Signature.

El-Gamal Digital Signature :-

Let prime no. $q = 19$.

Select primitive root (α) of q.
$\alpha = 10$.

Now generate a random integer (X_A) such that $(1 < X_A < q-1)$
$\therefore X_A = 16 \Leftarrow (1 < X_A < 18)$

Calculate $Y_A = (\alpha)^{X_A} \bmod q = (10)^{16} \bmod 19 = 4$.

Generation of keys for user (A):
Private Key $\Rightarrow X_A = 16$.
A's public key $\Rightarrow (q, \alpha, Y_A) = (19, 10, 4)$

Generate hash code (m) for plain text (M)
$m = H(M)$ such that $0 \le m \le q-1$.
$(m = 14) \Leftarrow 0 \le m \le 18$

Generate a random integer (K) such that $(1 \le K \le q-1)$ and $\gcd(K, q-1) = 1$ (Relatively Prime)

So K is : $0 \le K \le 18$ and $\gcd(K, 18) = 1$ $\therefore K = 5$.

Calculate S_1 and S_2 :- $S_1 = \alpha^K \bmod q$.
$= (10)^5 \bmod 19 = 3$.

$S_2 = K^{-1}(m - X_A S_1) \bmod (q-1)$
$K^{-1} \Rightarrow K^{-1} \bmod (q-1)$
$= 5^{-1} \bmod (18)(q-1)$
$\Rightarrow 5 \times (?) = 1 \bmod (q-1)$
$K^{-1} = 11$.
$S_2 = K^{-1}(m - X_A S_1) \bmod (q-1)$
$= 11(14 - 16 \times 3) \bmod 18 = 4$.

Verification :-
$V_1 = \alpha^m \bmod q = 10^{14} \bmod 19 = 16$.
$V_2 = (Y_A)^{S_1} (S_1)^{S_2} \bmod q$
$= 4^3 \times 3^4 \bmod 19$
$= 5184 \bmod 19 = 16$.

__/__/____

CMAC:- Cipher Based Message Authentication Code.

↳ Most used in government and industry.

↳ Message limitation.

↳ It is Block cipher based.

eg:- Message :- 101011

→ each block is encrypted.

Let $A_1, A_2, A_3, \ldots A_n$ are blocks of plain text.

CipherText : $C_1, C_2, \ldots C_{n-1}$

$$\text{Key} = K$$

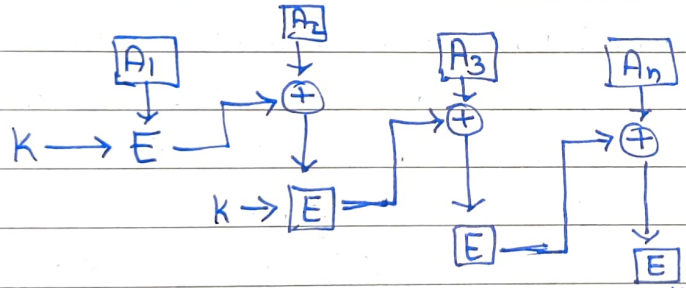
$$C_1 = E(K, A)$$

$$C_2 = E(K, A \oplus C_1)$$

$$C_3 = E(K, A \oplus C_2)$$

$$\vdots \qquad \vdots$$

$$C_n = E(K, A_n + C_{n-1} \oplus k_1)$$



final output.

HMAC:- Hash based message authentication code.

→ Key hash msg authentication code.

→ Cryptographic hash f^n & secret key used.