RSA ALGORITHM :-

(Ron- Rivest, Adi Shamir, Len Adleman)

Key Generation	
Select p, q	p and q both prime $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption	
Plaintext	$M < n$
Cipher text	$C = M^e \bmod n$.

Decryption	
Cipher text	C
plaintext	$M = C^d \bmod n$.

Example :-

(i) $p = 17$ and $q = 11$

(ii) Calculate $n = pq$
$n = 17 \times 11 = 187$.

(iii) Calculate $\phi(n) = (p-1)(q-1)$
$\phi(n) = 160$.

(iv) Select e; e is relatively prime to $\phi(n)$ and less than $\phi(n)$.
so $e = 7$.

(v) select d:
$de \equiv 1 \pmod{160}$ and $d < 160$.

so $d = 23$. becoz
$23 \times 7 = 161 = 10 \times 16 + 1$

(vi) Publickey $PU = \{7, 187\}$
Private key $PR = \{23, 187\}$.

(vii) Plain text input $M = 88$.

cipher $C = 88^7 \bmod 187 = 11$

(viii) $M = 11^{23} \bmod 187 = 88$

Calculation

(i) $88^7 \bmod 187 = 11$.

$\Rightarrow 88^1 \bmod 187 = 88$

$88^2 \bmod 187 = 77$

$88^4 \bmod 187 = 132$

so. $88^7 \bmod 187 = (88 \times 77 \times 132) \bmod 187$
$= 11$.

(ii) $11^{23} \bmod 187 = 88$

$\Rightarrow 11 \bmod 187 = 11$

$11^2 \bmod 187 = 121$

$11^4 \bmod 187 = 55$

$11^8 \bmod 187 = 33$.

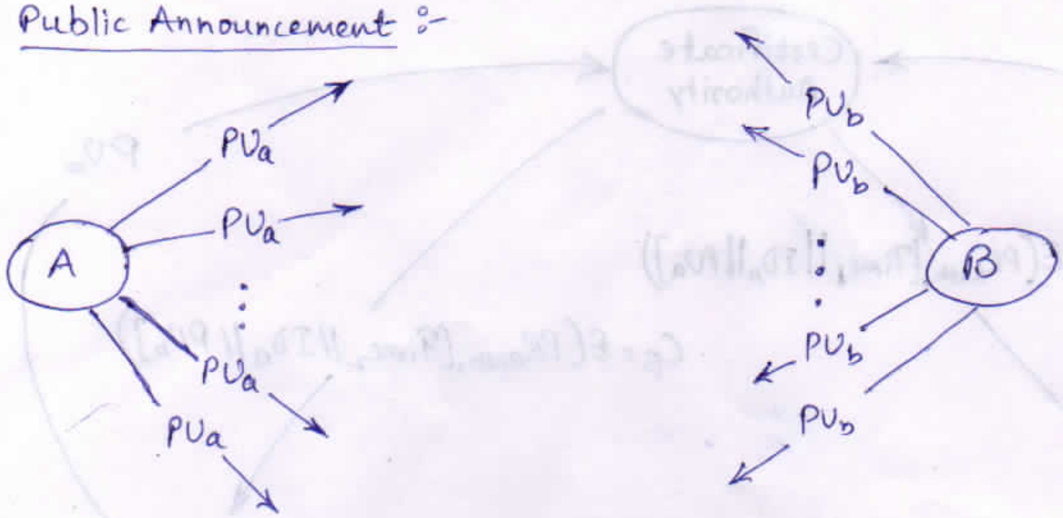
$11^{23} \bmod 187 = (11 \times 121 \times 55 \times 33 \times 33) \bmod 187$
$= 88$.

Example :-
(i) $p = 3;\ q = 11;\ e = 7;\ M = 5$ | $d = 3, C = 14$
(ii) $p = 5;\ q = 11;\ e = 3;\ M = 9$ | $d = 27, C = 14$
(iii) $p = 7;\ q = 11;\ e = 17;\ M = 8$ | $d = 53, C = 57$
(iv) $p = 11;\ q = 13;\ e = 11;\ M = 7$ | $d = 11, C = 106$
(v) $p = 17;\ q = 31;\ e = 7,\ M = 2$ | $d = 343, C = 128$

KEY MANAGEMENT :-

(I) DISTRIBUTION OF PUBLIC KEYS :-

1) Public Announcement :-



Weakness

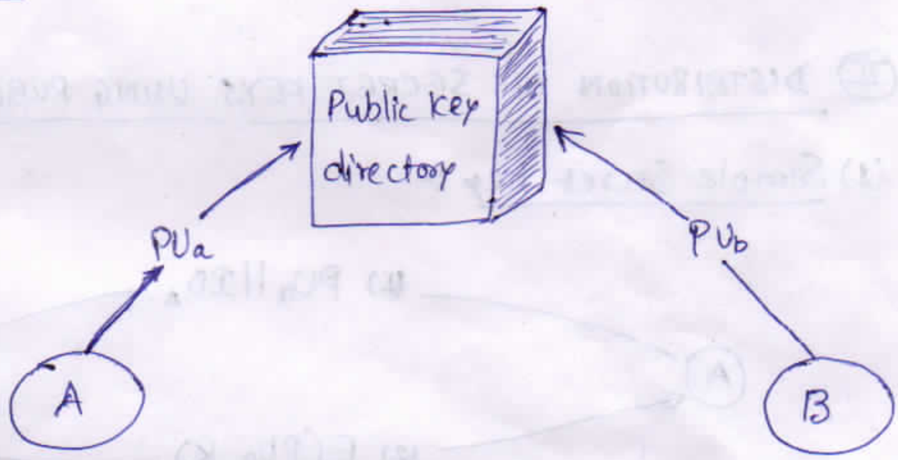
Anyone can forge such a public announcement.

2) Publicly Available Directory :-

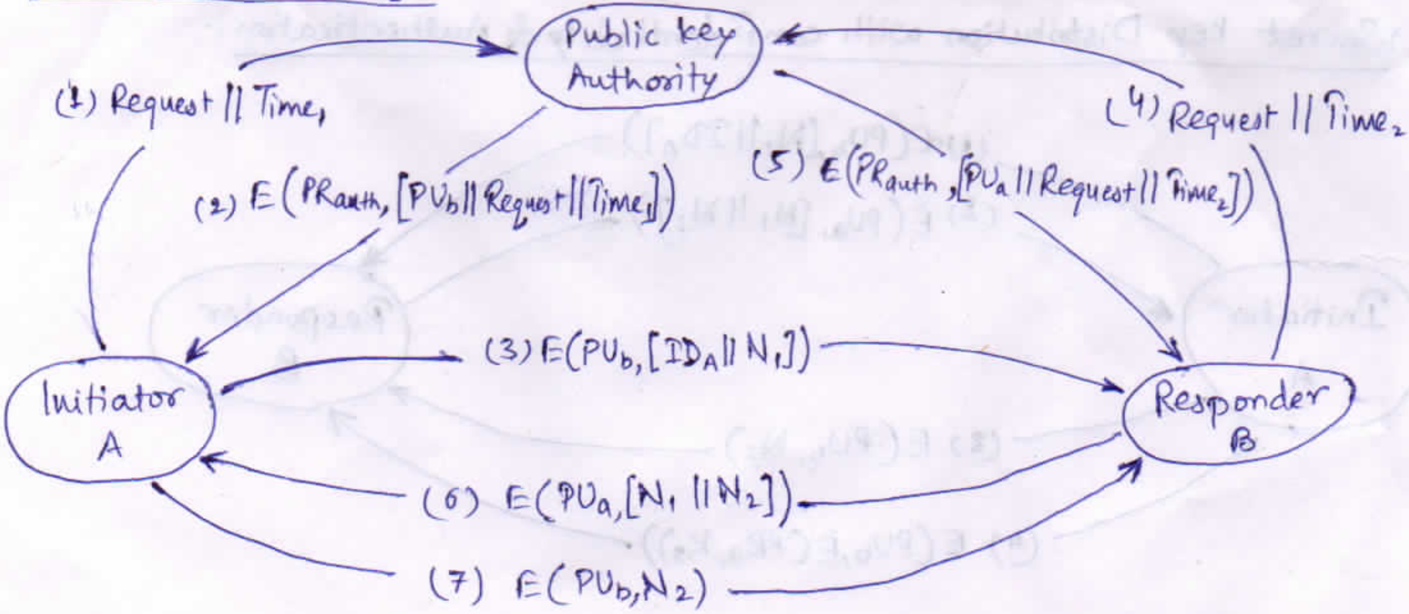
→ Authority maintains a directory with a {name, public key} entry for each participant.

Weakness

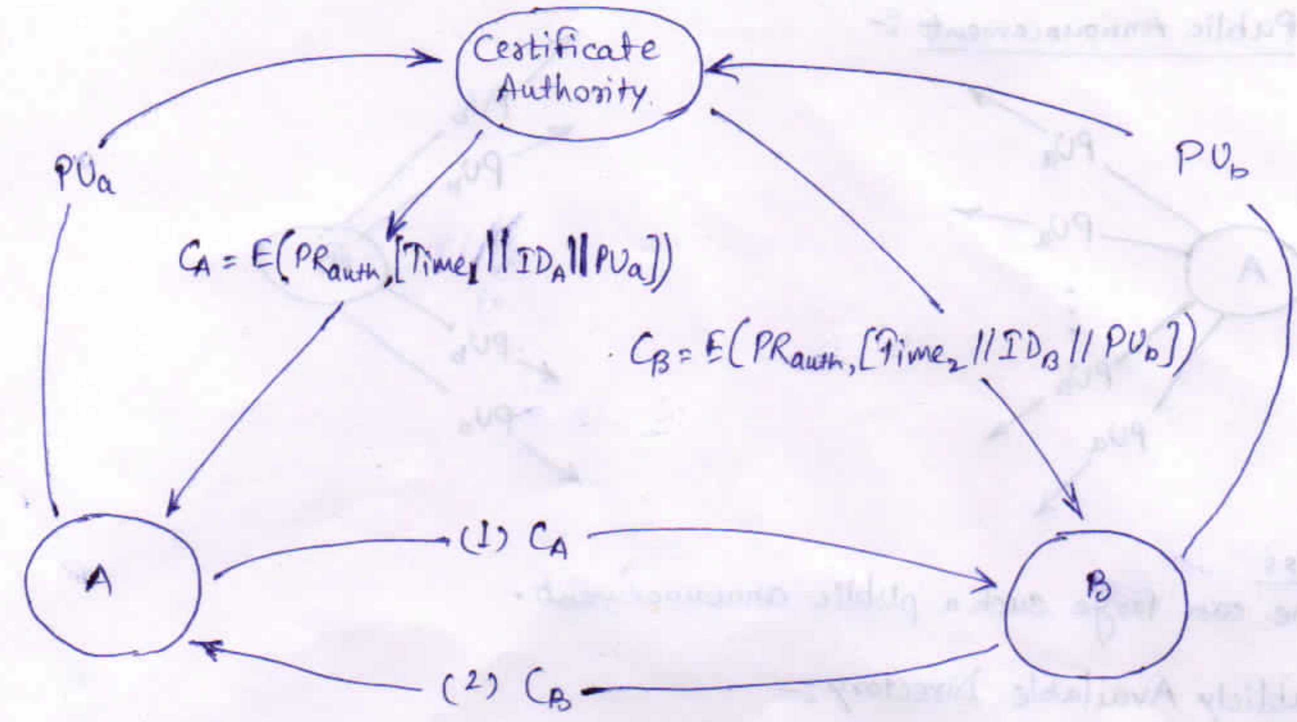
If an adversary succeeds in obtaining the private key of the directory authority, he could misuse public keys.



3) Public key Authority :-

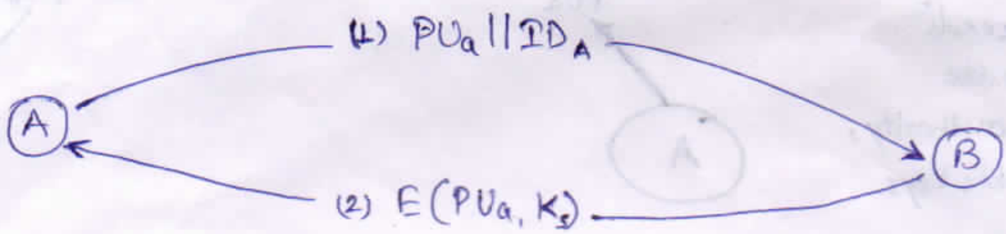


(4) Public Key Certificates :-

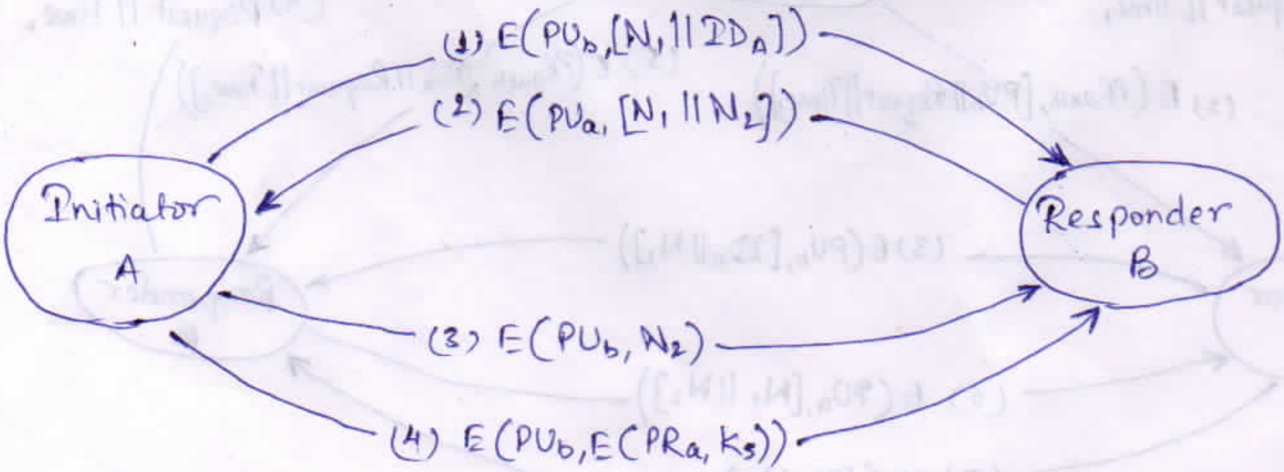


II DISTRIBUTION OF SECRET KEYS USING PUBLIC-KEY CRYPTOGRAPHY :-

(1) Simple Secret key :-



(2) Secret key Distribution with confidentiality & Authentication :-



DIFFIE-HELLMAN KEY EXCHANGE:-

(1) The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages.

Primitive root of a prime number p as one whose powers modulo p generate all the integers from 1 to p-1.

If a is a primitive root of the prime number p, then the numbers

$$a \bmod p,\ a^2 \bmod p,\ a^3 \bmod p,\ \ldots\ a^{p-1} \bmod p$$

are distinct and consists of the integers from 1 through p-1 in some permutation.

ALGORITHM:-

Global Public Elements

q prime number

α $\alpha < q$ and α is a primitive root of a

User A Key Generation.

Select private X_A $X_A < q$

Calculate public Y_A $Y_A = \alpha^{X_A} \bmod q$

User B Key Generation

Select Private X_B $X_B < q$

Calculate public Y_B $Y_B = \alpha^{X_B} \bmod q$

Calculation of Secret key by User A

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

Calculation of Secret key by User B.

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

$$\left[K = (Y_B)^{X_A} \bmod q \right]$$

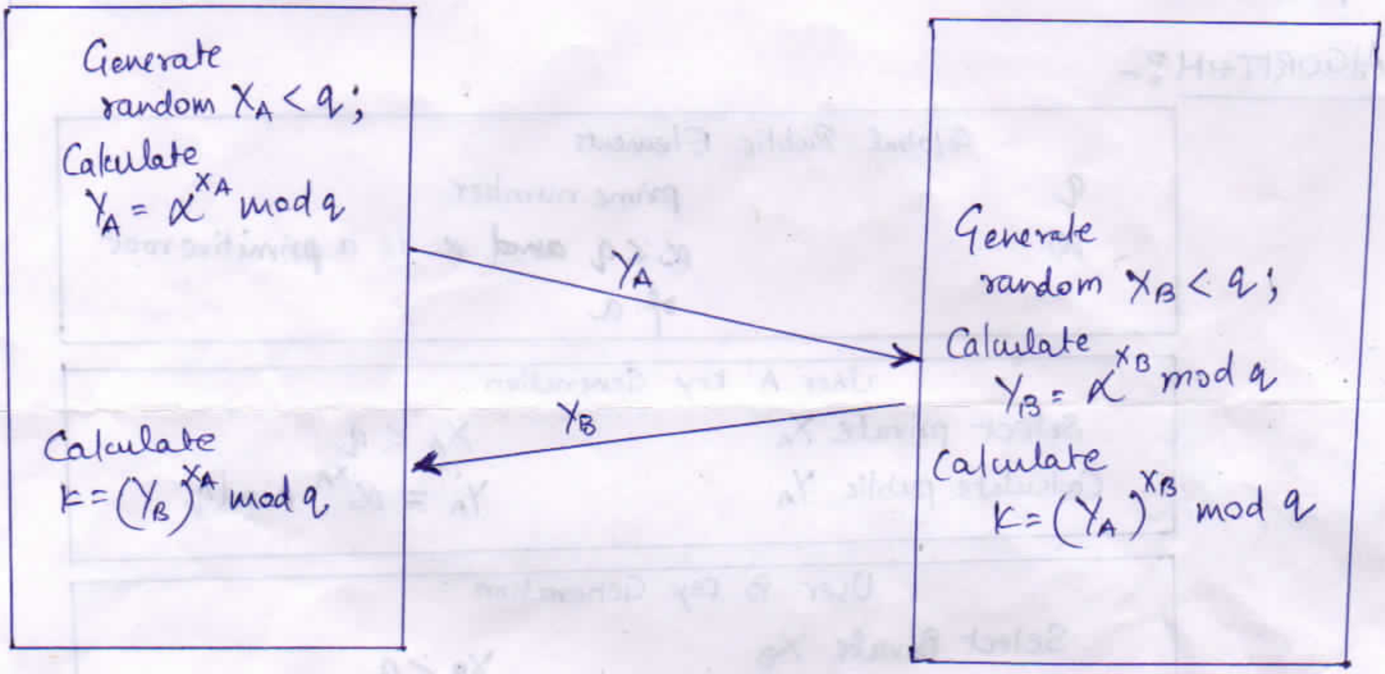
$$= (\alpha^{X_B} \bmod q)^{X_A} \bmod q \quad \text{by the rule of modular arithmetic}$$

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

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

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

$$\left[K = (Y_A)^{X_B} \bmod q \right]$$



Q.① $q = 71$, $\alpha = 7$, $X_A = 5$, $X_B = 12$
Calculate Y_A, Y_B and Secret key(K).

Q.② $q = 11$, $\alpha = 2$, $Y_A = 9$, $Y_B = 3$
(i) Calculate X_A, X_B and Secret key(K).
(ii) Show that 2 is a primitive root of 11.

Example:-

$q = 353$

a primitive root of 353 is $\alpha = 3$.

Let $X_A = 97$, $X_B = 233$.

A computes $Y_A = 3^{97} \bmod 353 = 40$

B computes $Y_B = 3^{233} \bmod 353 = 248$

After they exchange public keys, the common secret key is:

A computes $K = (Y_B)^{X_A} \bmod q = (248)^{97} \bmod 353 = 160$.

B computes $K = (Y_A)^{X_B} \bmod q = (40)^{233} \bmod 353 = 160$.