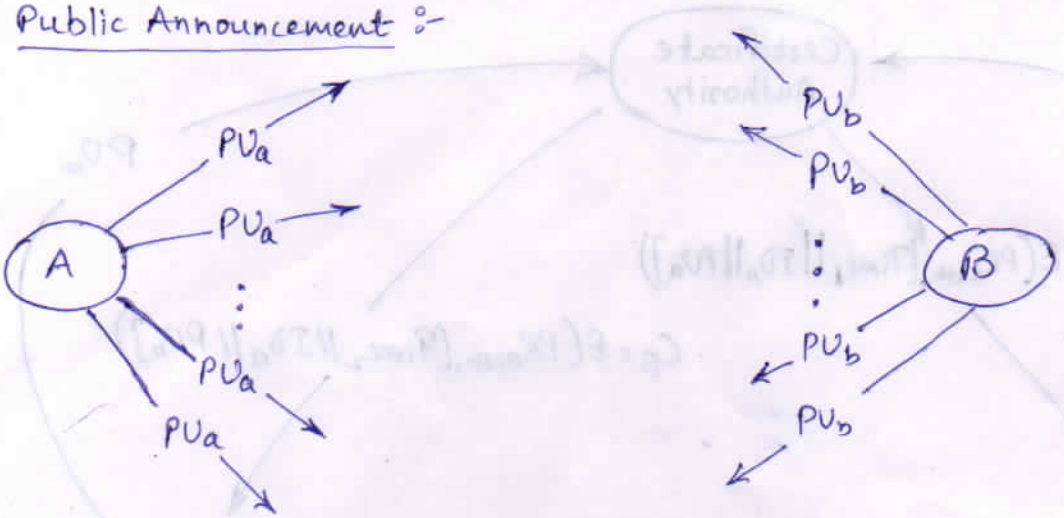
KEY MANAGEMENT :-

(I) DISTRIBUTION OF PUBLIC KEYS :-

1) Public Announcement :-



Weakness

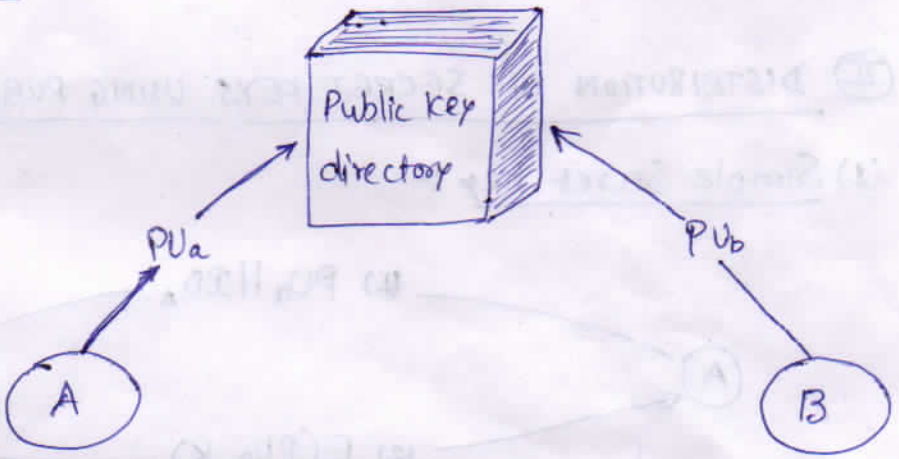
Anyone can forge such a public announcement.

2) Publicly Available Directory :-

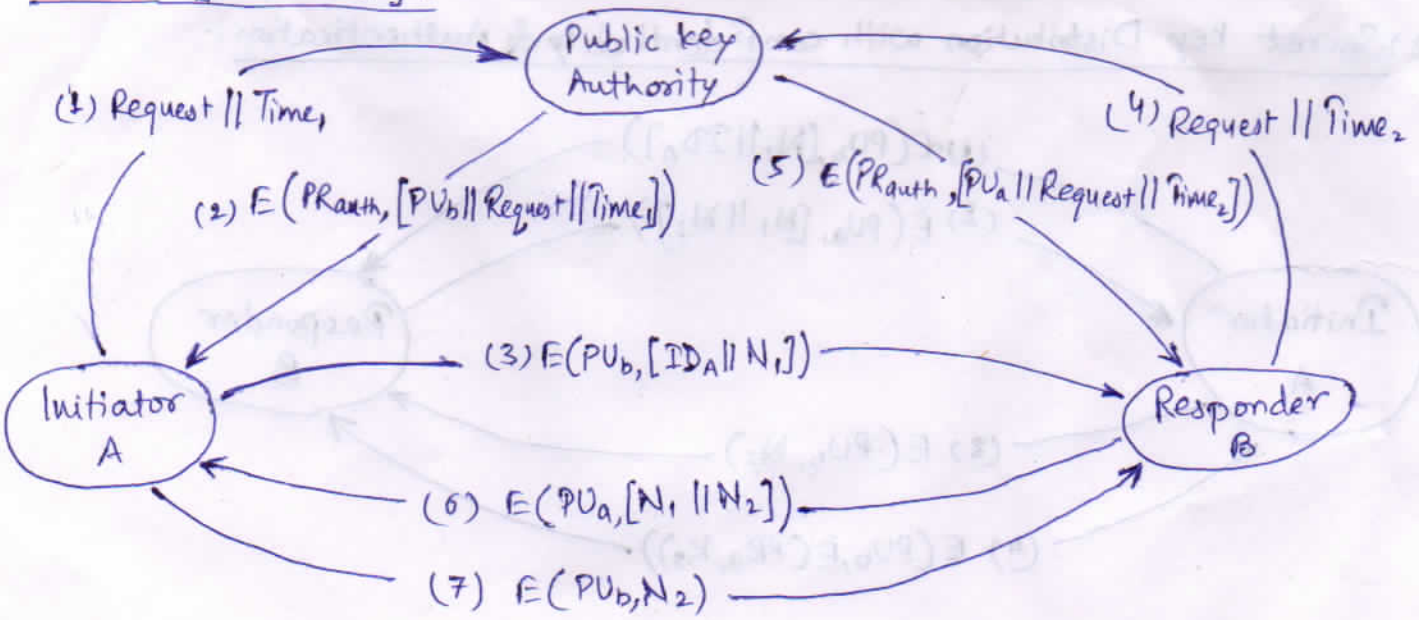
→ Authority maintains a directory with a {name, public key} entry for each participant.

Weakness

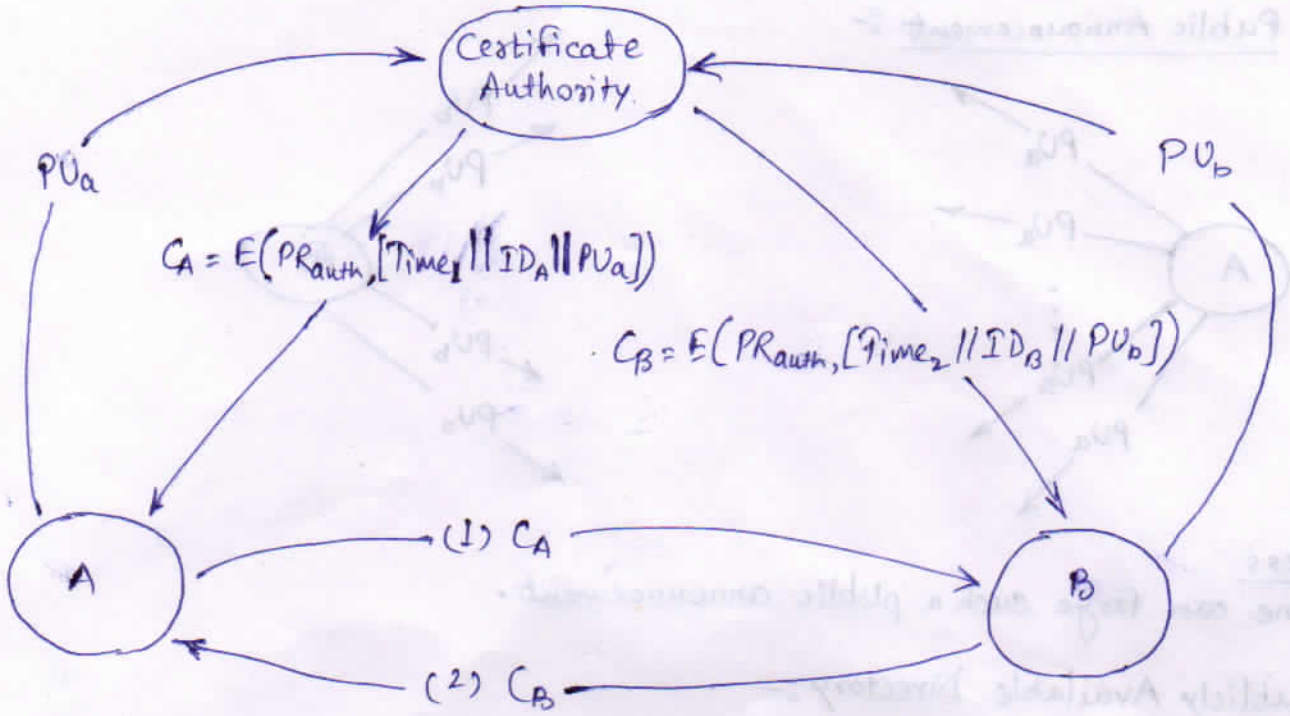
If an adversary succeeds in obtaining the private key of the directory authority, he could misuse public keys.



3) Public key Authority :-

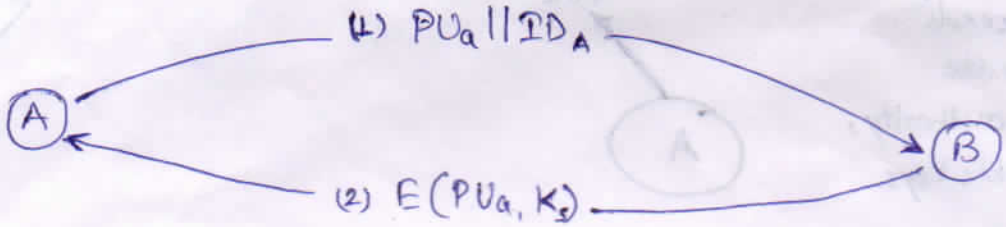


(4) Public key Certificates :-

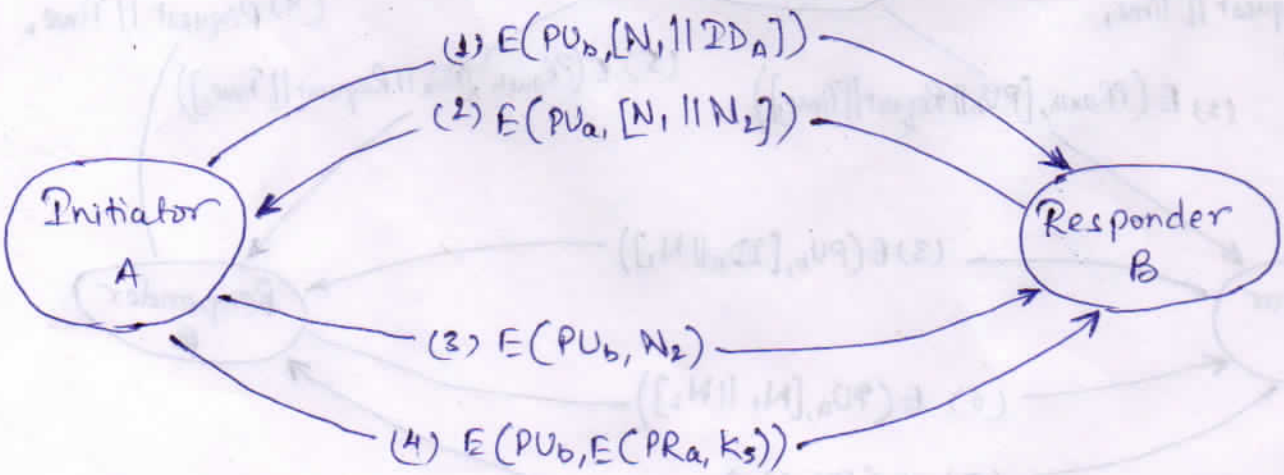


(II) DISTRIBUTION OF SECRET KEYS USING PUBLIC-KEY CRYPTOGRAPHY :-

(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 q

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.

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

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

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

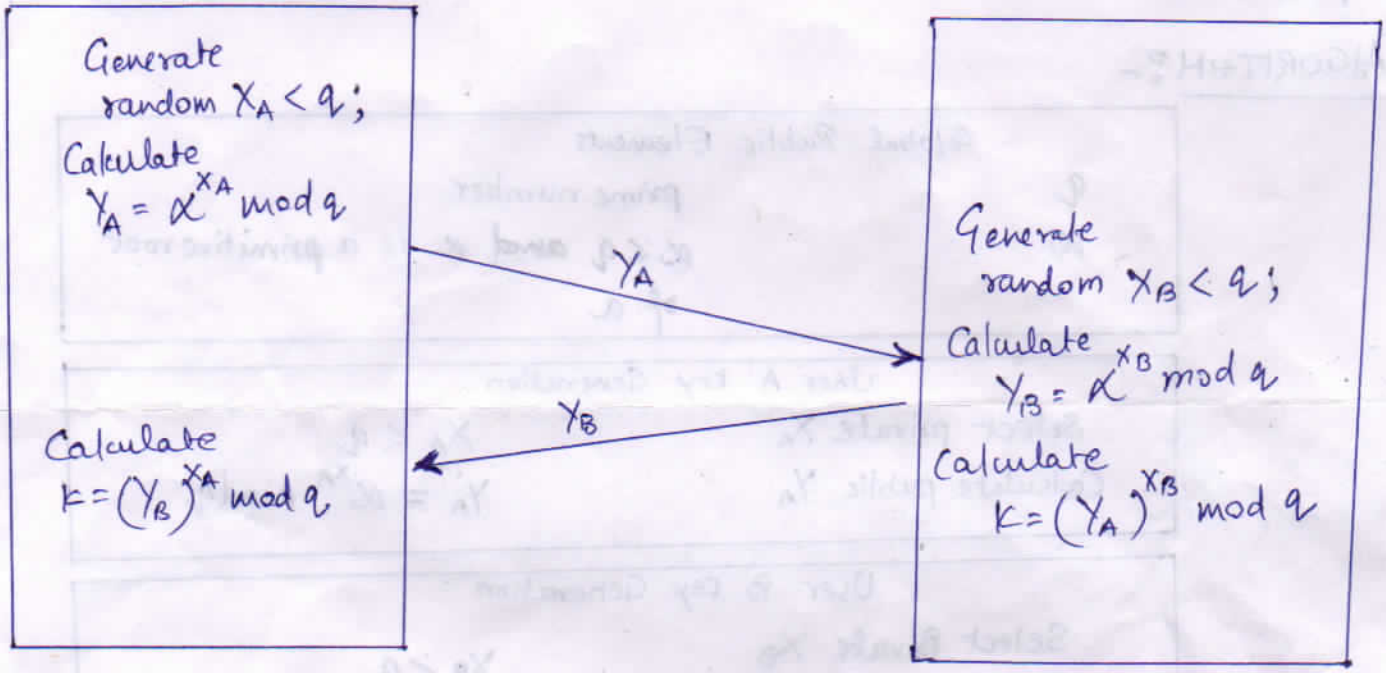
$$= (\alpha^{X_B})^{X_A} \bmod q = \alpha^{X_B X_A} \bmod q$$

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

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

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

by the rule of modular arithmetic



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

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.