Q.3 & Q.4 – Explain four ways to distribute public key.

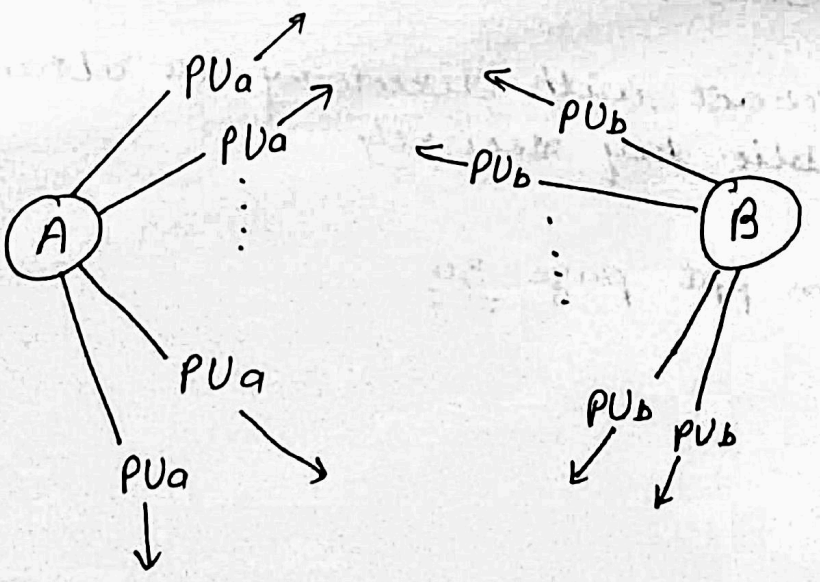
List four general categories of schemes for the distribution of public keys.

→ Distribution of public keys can be considered as using one of :-

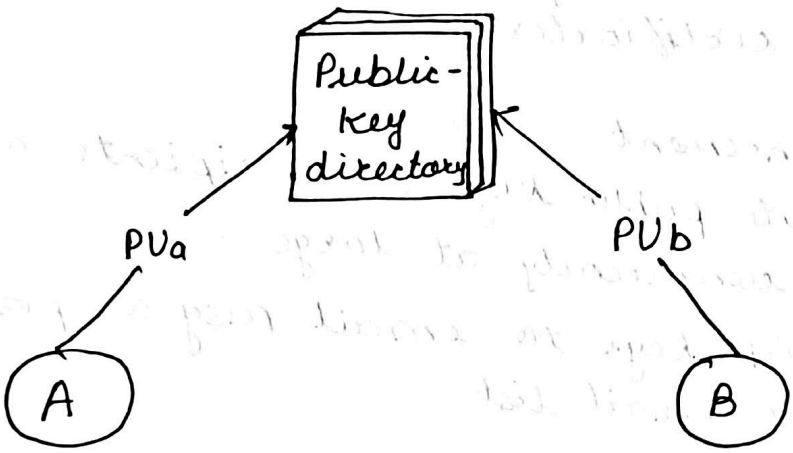
1] public announcement
2] public available directory
3] public – key authority
4] public – key certificates.

1] public announcement

- Users distribute public keys to recipients or broadcast to community at large
- Eg :- append PGP keys to email msg or post to news groups or email list
- Major weakness is forgery
  - Anyone can create a key claiming to be someone else and broadcasting it.
  - until forgery is discovered can masquerade as claimed user



2] publicly available directory
- can obtain greater security by registering keys with a public directory.
- directory must be trusted with properties:-
  - contains {name, public-key} entities
  - participants register securely with directory.
  - participants can replace key anytime
  - directory is periodically published
  - directory can be accessed electronically.



3] public-key authority
- improve security by tightening control over distribution of keys from directory.
- has properties of directory.
- and requires users to know public key for the directory.
- then users interact with directory to obtain any desired public key securely

fig from ppt page 36

4] public-key certificates

- certificates allow key exchange without real-time access to public-key authority
- a certificate binds identity to public key usually with other info such as period of validity, rights of use etc.
- with all contents signed by a trusted public key or certificate authority (CA).
- can be verified by anyone who knows the public-key authorities public-key.

fig from ppt page-38

Q.5. What is public-key certificate.

→ same as above.

Q.6. What are the requirements for the use of public key certificate scheme?

→ 1. Any participant can read a certificate to determine the name and public key of the certificate's owner.

2. Any participant can verify that the certificate originated from the certificate authority and is not counterfeit.

3. Only the certificate authority can create & update certificates.

4. Any participant can verify the currency of the certificate.

Q.7. Explain X.509 certificates format.

→ 1. Version :- Differentiate among successive versions of the certificate format. The default version is 1.

2. Serial number :- An integer value unique within the issuing CA, that is unambiguously associated with certificate.

3. Signature algorithm identifier :-
It is used to sign the certificate together with any associated parameters.

4. Issuer name -
X.500 is the name of the CA that created & signed this certificate.

5)

5. Period of validity -
consists of two dates: the first & last on which the certificate is valid.

6. subject name -
The name of the user to whom this certificate refers.

7. subject's public key info -
The public key of subject is used together with any associated parameters.

8. Issuer unique identifier -
An optional-bit string field used to identify uniquely issuing CA in event X.500

9. Extension -
A set of one or more extension field. It was added in version 3.

10. signature -
covers all of the other fields of the certificate

fig. from ppt [page 42]

Q.8. Explain X.509 version 3 certificate format.

→ - Following are the requirements not satisfied by version 2 but available in version 3:

1] The subject field inadequate to convey the identity of a key owner to a public key user. X.509 names may be relatively short & lacking in obvious identification details that may be needed for user.

2] The subject field is also inadequate for many applications, which recognise entities by an email, URL.

3] There is a need to indicate security policy info. This need security application such as IPsec to relate to an X.509 certificate to a given policy.

- Version 3 includes a number of optional extensions that may be added to version 2 format.
- Each extension consists of an extension identifier, a ~~critically~~ criticality indicator & an extension value.
- The certificate extensions fall into three main categories:-
  1) key & policy info.
  2) subject & issuer keys
  3) certification path constraints.

Q.9. Why an X.509 certificate is revoked?

→ - Certificates have a period of validity.

- May need to revoke before expiry

Eg 1. user's private key is compromised

2. user is no longer certified by this CA

3. CA's certificate is compromised

- CA's maintain list of revoked certificates
  - the certificate Revocation List (CRL)
- users ~~should~~ should check certificates with CA's CRL.

Q.10. Explain hierarchy of certificate authorities (CA) for distribution of other CA public key.

→ 1. For many users there have to be a number of CAs.

2. May not be practical for all users to subscribe to the same CA.

3. User must have a copy of the CA's public key to verify signatures.

4. A has a ~~cert~~ certificate from CA X1 & B has from CA X2.

5. If A does not securely know the public key of X2, then B's certificate, issued by X2, is useless to A.

6. A can read B's certificate, but A cannot verify the signature.

7. If the two CAs have securely exchanged their own public key, the following procedure will enable A to obtain B's public key.

Step 1 :- A obtains from the directory the certificate of X2 signed by X1. Because A securely knows X1's public key, A can obtain X2's public key from its certificate and verify it by means of X1's signature on the certificate

Step 2:- A then goes back to the directory and obtains the certificate of B signed by X2, because A now has a trusted copy of X2's public key, A can verify the signature & securely obtain B's public key.

8. A has used a chain of certificates to obtain B's public key. In the notation of X.509, this chain is expressed as

$X_1 << X_2 >> X_2 << B >>$

9. In the same fashion B can obtain A's public key with the reverse chain:

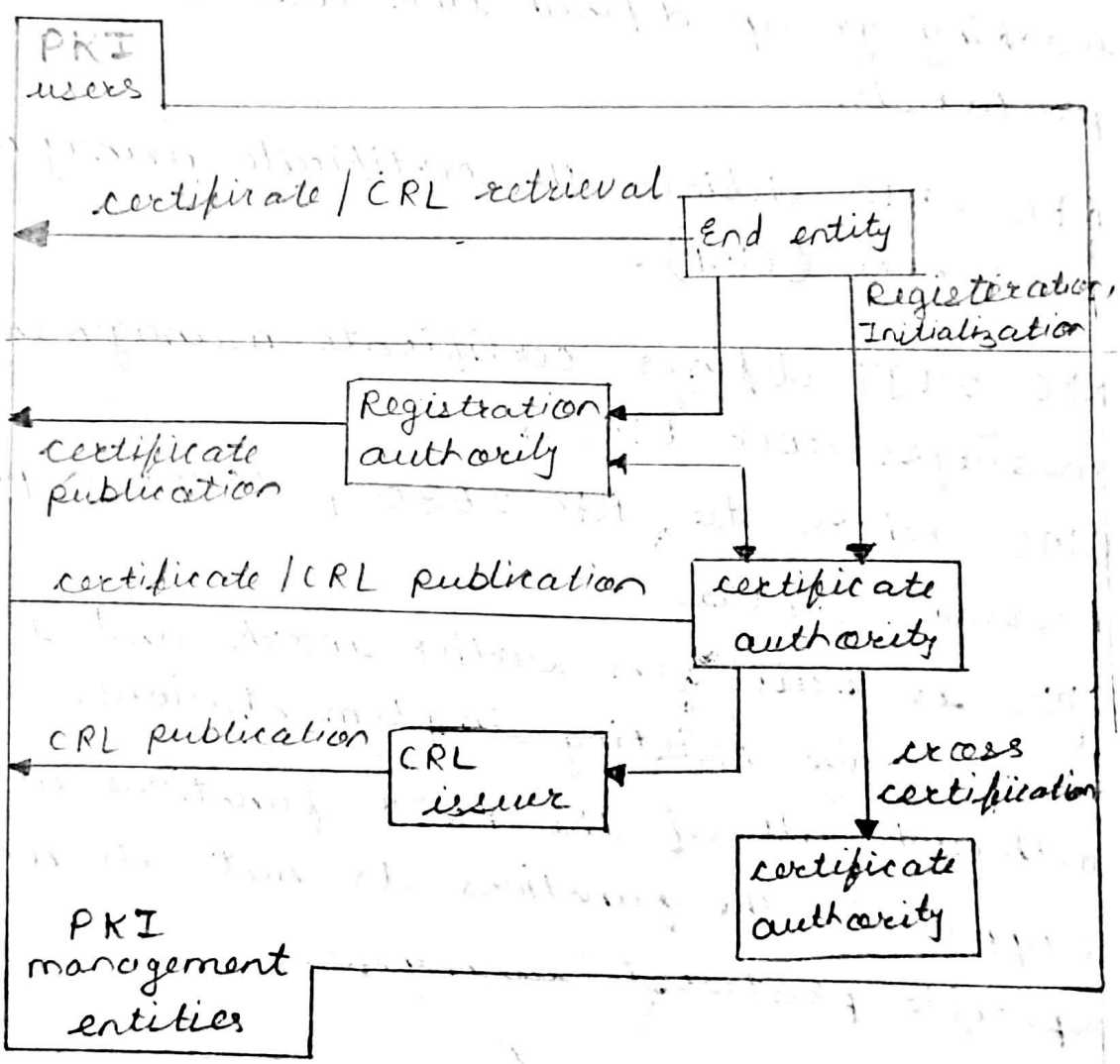
$X_2 << X_1 >> X_1 << A >>$

10. An arbitary long path of CAs can be followed to produce a chain:

$X_1 << X_2 >> X_2 << X_3 >> \ldots X_n << B >>$.

Q.11. Explain PKIX architectural model.

→ 1. Internet Engineering Task Force (IETF) public key infrastructure X.509 (PKIX) working group has been the driving force behind setting up a formal (and generic) model based on X.509.



2. Key points of PKIX model :-

① end entity

② certification authority (CA)

③ Registration authority (RA)

④ CRL issuer

⑤ Repository

3. PKIX management functions-

① registration
② initialization
③ certification
④ key pair recovery
⑤ key pair update
⑥ revocation request
⑦ cross certification.

4. To support the management functions PKIX working group defined two alternative management protocols.

5. RFC 2510 defines the certificate management protocols (CMP).

6. RFC 2797 defines certificate management messages over CMS.

7. CMS refers to RFC 2630, cryptographic message syntax.

8. CMS is built on earlier work and is intended to leverage existing implementations.

9. Although all of the PKIX functions are supported, the functions do not all map into specific protocol exchanges.