UNIT V:
MUTUAL TRUST AND KEY MANAGEMENT **AFTAB-1405**

01. EXPLAIN IN DETAILS DISTRIBUTION OF SECRET KEYS USING PUBLIC KEY ENCRYPTION.

Distributing Secret Keys Using Public-Key Encryption

Public-key cryptography, while ***not ideal for encrypting large amounts of data directly*** due to its ***computational cost,*** plays a vital role in ***securely distributing secret keys for symmetric encryption.*** Here's a detailed explanation of this process:

The Problem with Symmetric Key Distribution:

Traditionally, ***symmetric encryption relies on pre-shared secret keys between communicating parties.*** Distributing these keys securely can be challenging, especially when dealing with a large number of users.

The distribution of secret keys using public-key encryption involves ***securely exchanging secret keys between parties*** using asymmetric cryptography. This process is ***crucial for establishing secure communication channels between entities without relying on a pre-shared secret key.*** Here's a detailed explanation of how secret keys are distributed using public-key encryption:

1. **Simple Secret Key Distribution:**
    - One of the simplest methods was proposed by ***Merkle,*** which involves the following steps:
        1. ***'A' generates a public/private key pair*** and ***transmits the public key*** along with an identifier to 'B'.
        2. ***'B' generates a secret key*** and ***encrypts it using A's public key.***
        3. ***'A' decrypt the message using its private key*** to recover the secret key.
        4. 'A' and 'B' can now securely communicate using the ***session key.***
    - This method ensures ***minimal risk of key compromise as keys are generated and discarded for each session.*** However, it's vulnerable to ***man-in-the-middle*** attacks.
2. **Secret Key Distribution with Confidentiality and Authentication:**
    - This approach, based on a suggestion by ***Needham and Schroeder,*** provides protection against ***active and passive attacks:***
        1. A encrypts a message to B containing ***A's identifier and a nonce*** using B's public key.
        2. B responds with a message encrypted using A's public key, ***containing A's nonce and a new nonce generated by B.***
        3. ***A verifies B's identity*** and ***sends back B's nonce*** encrypted with B's public key.
        4. A selects a secret key, ***encrypts it first with A's private key*** and then with ***B's public key, and sends it to B.***

5. B decrypts the message using its private key and A's public key to recover the secret key.

- This scheme ensures both ***confidentiality and authentication*** in the exchange of the secret key.

3. **Hybrid Scheme:**

- In a hybrid approach, a ***Key Distribution Centre (KDC) shares a secret master key*** with each user and ***distributes session keys encrypted with the master key. Public-key encryption is used to distribute the master keys.***
- This scheme involves three levels: ***users, KDC, and session keys.***

In summary, distributing secret keys using public-key encryption involves leveraging asymmetric cryptography to securely exchange session keys between parties. Different protocols and schemes ensure ***confidentiality, authentication, and efficiency*** in key distribution processes, addressing various security threats such as ***eavesdropping and man-in-the-middle attacks.***

02. EXPLAIN THE FOLLOWING TECHNIQUES FOR THE DISTRIBUTION OF PUBLIC KEYS: 1. PUBLICLY AVAILABLE DIRECTORY 2. PUBLIC KEY CERTIFICATES

Public Key Distribution Techniques

Here's a breakdown of two common techniques for distributing public keys:

1. Publicly Available Directory:

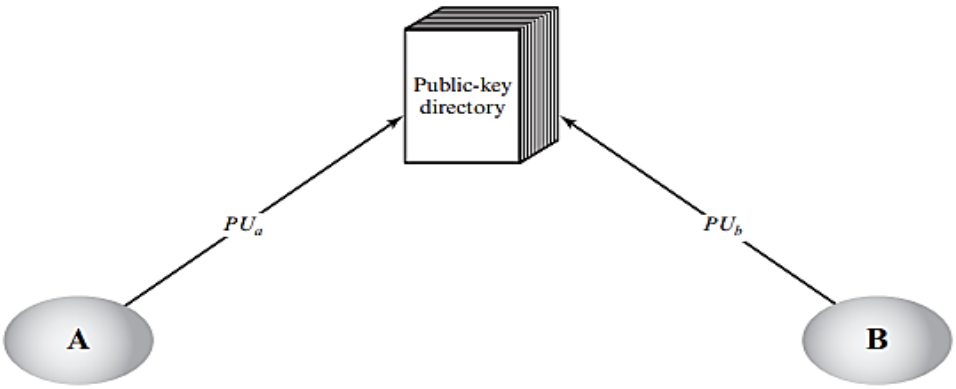


Figure 14.11 Public-Key Publication

This method involves maintaining a central repository of public keys accessible to everyone. Here's how it works:

- **Directory Authority:** A ***trusted entity or organization manages the directory,*** ensuring its ***accuracy and security.***
- **Registration:** Users ***register their public keys with the directory authority.*** This ***process may involve secure communication methods to prevent unauthorized registrations.***

- **Access:** Users can electronically access the directory to retrieve public keys of other participants. ***Secure communication between the directory and users is essential*** to ***prevent tampering with key information.***

Security Advantages over Public Announcement:

- **Reduced Risk of Forgery:** Anyone can't forge public key entries as the directory authority controls registration.
- **Centralized Management:** ***Simplifies updates and revocations*** of public keys.

Security Weaknesses:

- **Single Point of Failure:** If the directory authority is compromised, ***attackers could inject fake public keys or tamper with existing ones.***
- **Scalability Concerns:** ***Maintaining a large directory with efficient access*** for a vast user base can be challenging.

2. Public Key Certificates:

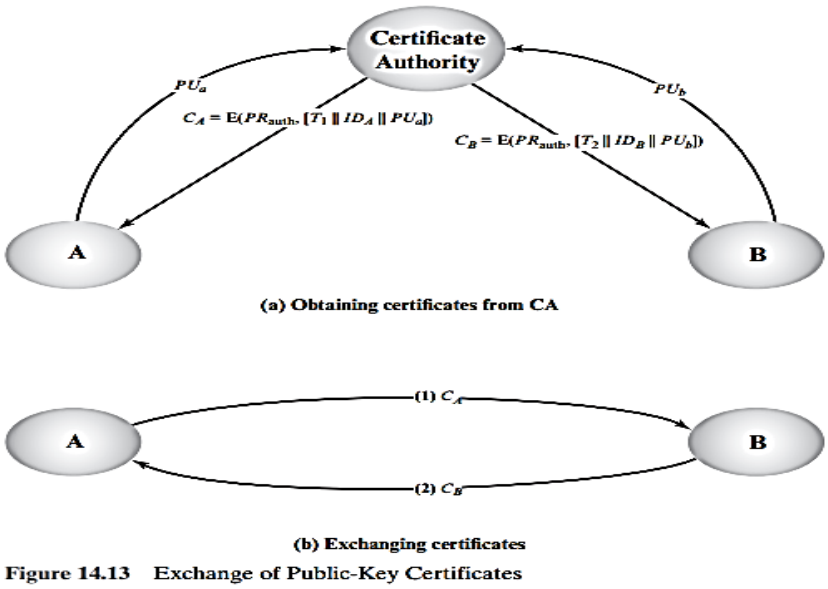


Figure 14.13 Exchange of Public-Key Certificates

This approach ***utilizes digital certificates*** issued by a trusted third party, called a ***Certificate Authority (CA),*** to verify the authenticity of public keys. Here's the process:

- **Certificate Structure:** A certificate contains:
  - Public key of the owner
  - Time of creation and validity period of certificate
  - Owner's identity information
  - ***Digital signature*** of the ***Certificate Authority***
- **Certificate Issuance:** ***Users apply to the CA with their public key for a certificate.*** The CA ***verifies the user's identity*** through secure communication and ***issues a signed certificate.***

- **Public Key Distribution:** Users can share their certificates with others electronically.

Security Advantages:

- **Authentication:** The CA's signature ensures the public key belongs to the claimed owner.
- **Integrity Protection:** Digital signatures prevent tampering with certificate contents.
- **Revocation Mechanism:** ***CAs can revoke compromised certificates*****,** mitigating security risks.

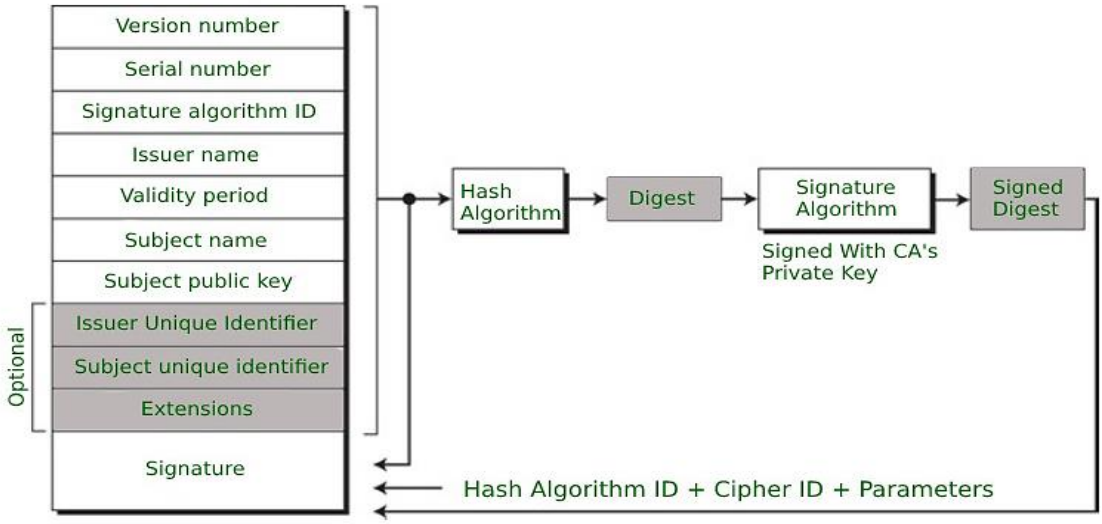
Requirements for a Secure Scheme:

- **Readability:** Anyone can access a certificate ***to obtain the owner's name and public key.***
- **Verification:** Anyone can verify the certificate's authenticity using the CA's public key.
- **Issuance Control:** ***Only the CA can create*** and ***update certificates.***
- **Time Validity:** ***Certificates have expiration dates to address compromised keys.*** (Added by Denning ***[DENN83]***)

X.509 is the universally accepted standard for formatting public key certificates. It plays a crucial role in various ***network security applications*** like ***IP security, Transport Layer Security (TLS), and S/MIME.***

In conclusion, both publicly available directories and public key certificates offer more secure methods for public key distribution compared to simple public announcement.

03. WHAT DO YOU MEAN BY X.509? EXPLAIN WITH NEAT DIAGRAM X.509 CERTIFICATE FORMAT/ STATE THE PURPOSE OF X.509 CERTIFICATE FORMAT. DISCUSS X.509 CERTIFICATE FORMAT.



An X.509 certificate is a digital document that ***binds a public key to an entity's identity,*** such as ***an individual, a computer system, or a service.*** It is an essential component of ***public key infrastructure (PKI)*** and is used to ***facilitate secure communications and transactions*** over networks.

UNIT V:

MUTUAL TRUST AND KEY MANAGEMENT **AFTAB-1405**

The ***purpose of the X.509 certificate format*** is to provide a ***standardized way to distribute and manage public keys*** in a ***secure and verifiable manner*** as part of a PKI. X.509 certificates bind an entity's public key to its identity, ***ensuring that the key truly belongs to the claimed entity.*** This ***binding is achieved through a digital signature applied by a trusted third party, known as a Certification Authority (CA).***

By ***validating the CA's signature on a certificate,*** relying parties can trust the association between the public key and the entity's identity. X.509 certificates serve several important functions:

1. **Authentication:** ***Enables authentication of entities*** in secure communications by ***verifying their identities.***
2. **Non-repudiation:** Digital signatures provide non-repudiation, ***preventing the signer from denying their involvement.***
3. **Key distribution:** ***Facilitates secure distribution of public keys,*** eliminating manual key exchange.
4. **Confidentiality:** Public keys can be used for ***key establishment*** and ***encryption for confidential communications.***

The X.509 certificate format has the following structure:

1. **Version:** Identifies the X.509 version (1, 2, or 3, with later versions having more extensions).
2. **Serial Number:** A ***unique integer assigned by the issuing CA***.
3. **Signature Algorithm:** The ***algorithm used by the CA to sign the certificate***.
4. **Issuer Name:** The X.500 name of the issuing CA.
5. **Validity Period:** The time period when the certificate is valid.
6. **Subject Name:** The ***name of the entity*** (user, device, service etc.) ***identified by the certificate***.
7. **Subject's Public Key:** The ***public key of the subject entity*** and ***associated algorithms/parameters***.
8. **Issuer Unique ID (optional):** Additional identifier for the issuing CA.
9. **Subject Unique ID (optional):** Additional identifier for the subject entity.
10. **Extensions (X.509 v3):** Additional attributes, e.g., ***Key Usage, Extended Key Usage, Subject Alternative Names***.
11. **Signature:** The CA's digital signature over the other fields, ***verifying the certificate's authenticity and integrity***.

The extensions in X.509 v3 certificates provide additional capabilities, such as specifying key usage constraints, alternative names for the subject, and policy information. Common extensions include Key Usage, Extended Key Usage, Subject Alternative Name, and Basic Constraints.