SENG 460

Practice of Information Security and Privacy

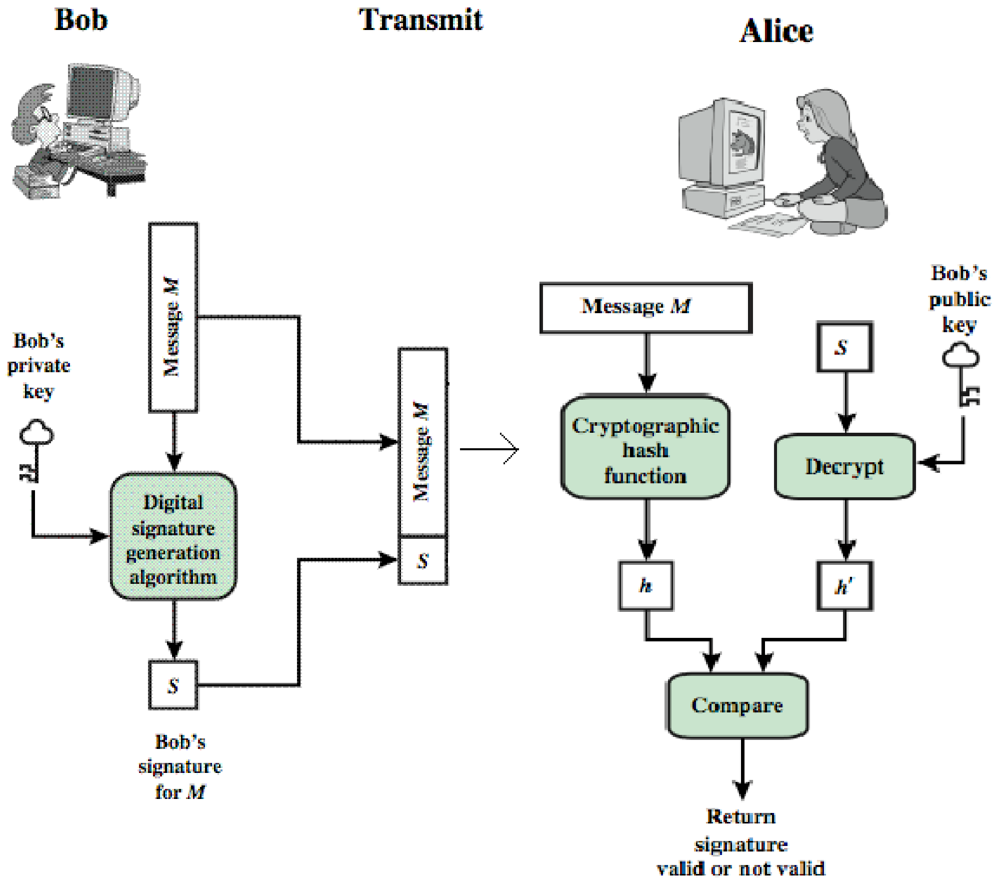
Cryptography II

Cryptographic Applications/Systems

- Digital Signatures

A digital signature is a hash value encrypted with the sender's private key.

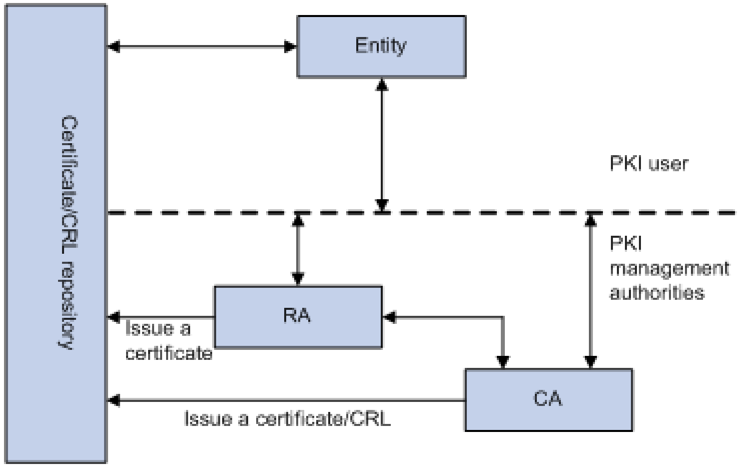
- A digital signature provides authentication, nonrepudiation, and integrity.
- US Federal government requires digital signature to be generated by SHA and Digital Security Algorithm (DSA), RSA, or ECDSA.



Cryptographic Applications/Systems

- Public Key Infrastructure (PKI)

- A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke **digital certificates**.
  - A PKI provides confidentiality, message integrity, authentication, and nonrepudiation.
  - The main components of a PKI includes
    - Certificate Authorities (CA)
    - Certificates (Cert) & Certificate Revocation lists (CRL) Repository
    - Registration Authorities (RA)

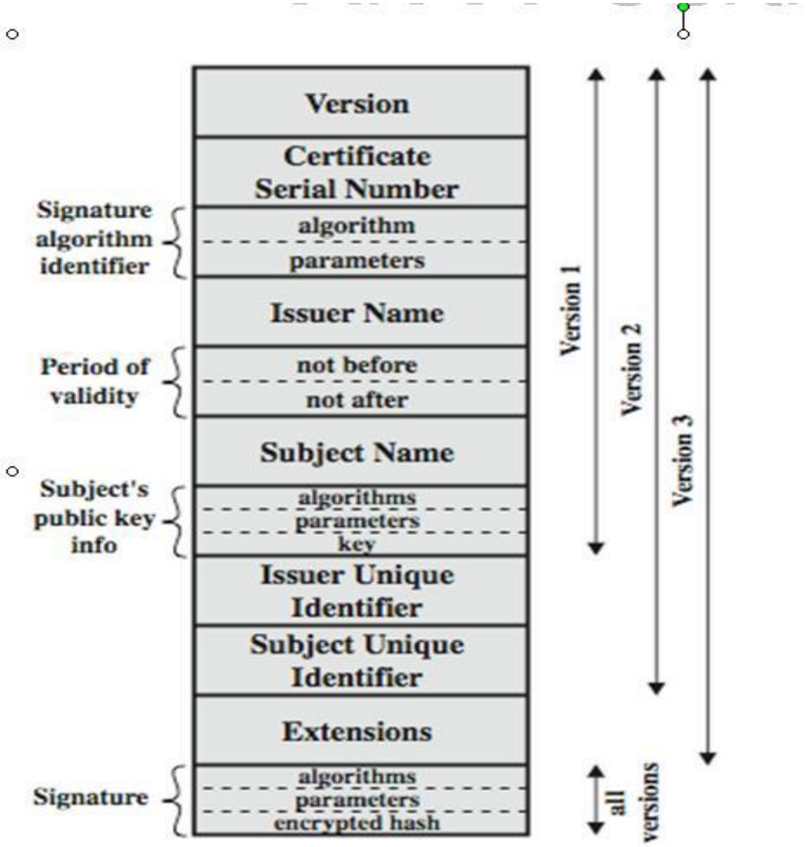


Cryptographic Applications/Systems

- PKI Certificate

- A ***certificate*** is the mechanism used to associate a public key with a collection of components in a manner that is sufficient to uniquely identify the claimed owner.

The standard for how the CA creates the certificate is X.509, which dictates the different fields used in the certificate and the valid values that can populate those fields.



(a) X.509 Certificate

Cryptographic Applications/Systems

- PKI Steps

- Certificate Request
  1. A user request a digital certificate from RA
  2. RA verifies and validates the user's identity information
  3. RA forwards the certificate request to CA
  4. CA creates the certificate for the user, and publish the certificate in the repository if necessary.
  5. User receives his certificate (which contains the public key) and private key.

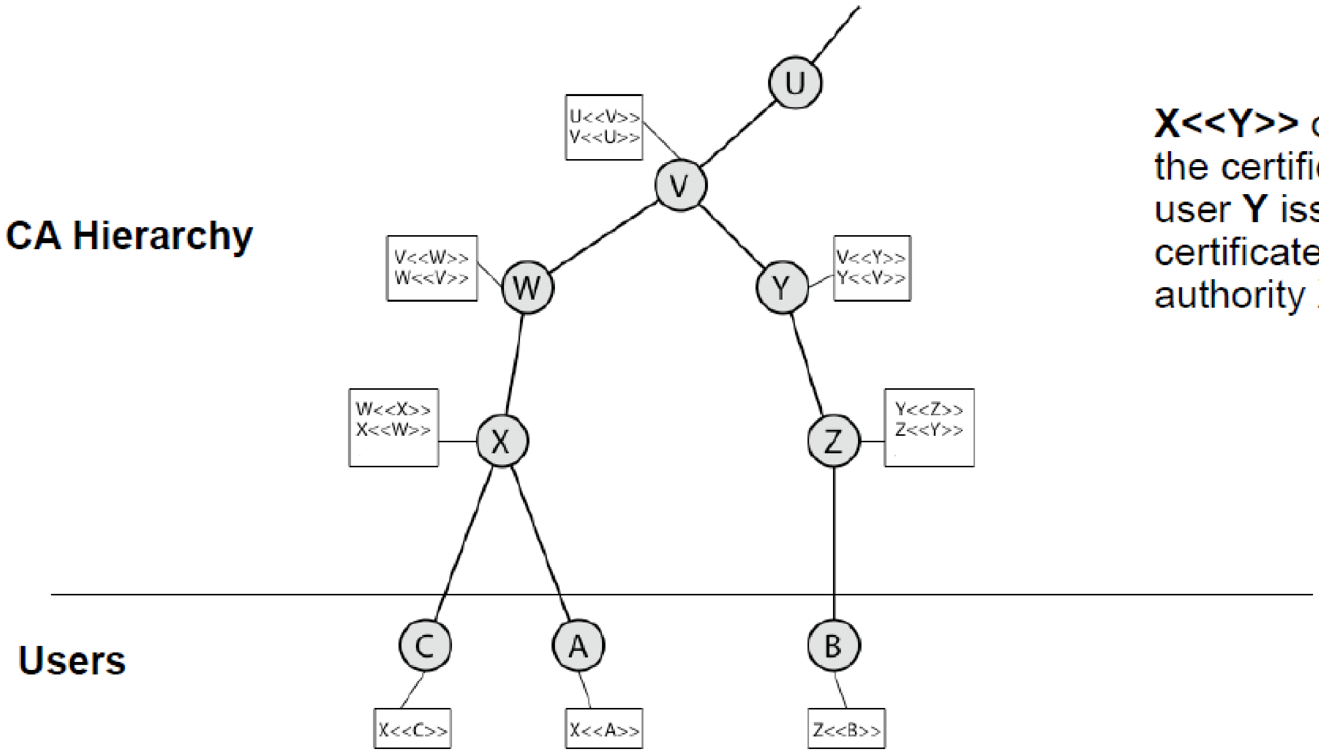
- Secure Communication (2-way authentication)
  1. User 1 request user 2's certificate either from user 2 directly or from a repository
  2. User 1 validates user 2's certificate by verifying the certificate signature
  3. User 1 encrypts a secret with user 2's public key and sends the encrypted secret to user 2 with user1's certificate.
  4. User 2 decrypt the secret using his private key, verify user1's certificate, generate his own secret, encrypt the secret with user 1's public key and sends the encrypted secret to user 1.
  5. User 1 descripts user2's secret using his own private key.

At this point, a common secret can be established by combing both user 1 and use 2's secrets. And this common secret can be used as a symmetric key for secure communication.

Cryptographic Applications/Systems

- PKI Cross-Certification

- Two CAs are **cross-certificated** if they issue certificates to each other.



X<<Y>> denotes the certificate of user **Y** issued by certificate authority **X**

Users can validate a certificate from any CA using a chain of certificates obtained from the CAs hierarchy (Cross-certification)

Cryptographic Applications/Systems

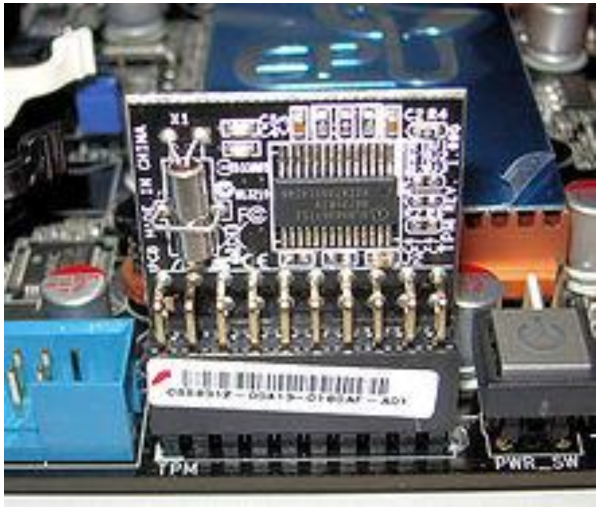
- Key Management

- Key management involves the entire process of ensuring that keys are protected during creation, distribution, transmission, storage, and destruction.
  - Because keys can be lost, backup copies should be made and stored in a secure location.
  - The key recovery process should require more than one operator to ensure that only valid key recovery requests are completed.
  - Key recovery personnel should span across the entire organization and not just be members of the IT department.
  - Keys should always be stored in ciphertext when stored on a noncryptographic device.

Cryptographic Applications/Systems

- Trusted Platform Module (TPM)

- Trusted Platform Module (TPM) is a security chip installed on computer motherboards that is responsible for managing symmetric and asymmetric keys, hashes, and digital certificates. TPM usually communicates with the rest of the system by using a hardware bus. Two particularly popular uses of TPM are binding and sealing.
  - **Binding:** encrypts data using TPM bind key
  - **Sealing**: encrypts data in a similar manner to binding, but in addition specifies a state in which TPM must be in order for the data to be decrypted.



Cryptographic Applications/Systems

- E-Mail Security

- Pretty Good Privacy (PGP) provides secure e-mail communication over the Internet.
  - PGP uses encryption to provide confidentiality, hashing to provide integrity, public key certificates to provide authentication, and message digests to provide nonrepudiation.
  - Certificates in PGP are usually self-signed, No CAs involved.

- Multipurpose Internet Mail Extension (MIME) is an Internet standard that allows e-mail to include non-text attachments, non-ASCII character sets, multiple-part message bodies, and non-ASCII header information. Secure MIME (S/MIME) allows MIME to encrypt and digitally sign e-mail messages and encrypt attachments.
  - S/MIME uses encryption to provide confidentiality, hashing to provide integrity, public key certificates to provide authentication, and message digests to provide nonrepudiation.

Cryptographic Applications/Systems

- Internet Security

- Secure Sockets Layer (SSL/TLS) is a transport-layer protocol that provides encryption, server and client authentication, and message integrity.
- Secure Electronic Transaction (SET) a communication protocol that secures credit card transaction information over the Internet and was based on X.509 certificates and asymmetric keys.
- Internet Protocol Security (IPsec) is a suite of protocols that establishes a secure channel at network layer.
- Secure Shell (SSH) is an application and protocol that is used to remotely log in to another computer using a secure tunnel.

Cryptography Attacks
- Attack Types

The common attack vectors in cryptography are key, algorithm, implementation, data, and people.

Ciphertext-only attack: In this type of attack, the attacker has the ciphertext of several messages.

Known plaintext attack: the attacker has the plaintext and corresponding ciphertext of one or more messages.

Chosen plaintext attack: the attacker has the plaintext and ciphertext, he can choose the plaintext that gets encrypted to see the corresponding ciphertext.

Chosen ciphertext attack: the attacker can choose the ciphertext to be decrypted and has access to the resulting decrypted plaintext.

Cryptography Attacks

- Techniques

Frequency Analysis: Study the frequency of letters or groups of letters in a ciphertext. The method is effectiveto breaking classical ciphers.

Cover-channel Attack: gather “outside” information with the goal of uncovering the encryption key.

Replay attack: capture some type of data and resubmits it with the hopes of fooling the receiving device into thinking it is legitimate information.

Reverse engineering: obtain a particular cryptographic product and attempt to reverse the product to discover vulnerabilities. (One of the most popular and effective attacks)