Cryptography - Introduction

Mridul Sankar Barik

Jadavpur University

2023

Security Requirements

- **Confidentiality**: Requires that data only be accessible by authorized parties. This type of access includes printing, displaying, and other forms of disclosure, including simply revealing the existence of an object.
- **Integrity**: Requires that only authorized parties can modify data. Modification includes writing, changing, changing status, deleting, and creating.
- **Availability**: Requires that data are available to authorized parties.
- **Authenticity**: Requires that a host or service be able to verify the identity of a user.

Security Attacks

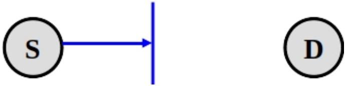
- **Passive attacks**: A passive attack attempts to learn or make use of information from the system but does not affect system resources.
  - Release of message contents
  - Traffic analysis
- **Active attacks**: An active attack attempts to alter system resources or affect their operation.
  - Masquerade
  - Replay
  - Modification of messages
  - Denial of service

Security Attacks I

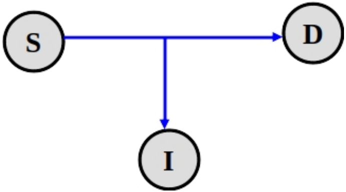
- Any action that compromises the security of information
- Four types of attack
  - Interruption
  - Interception
  - Modification
  - Fabrication

Security Attacks II

- Interruption
  - Attack on availability

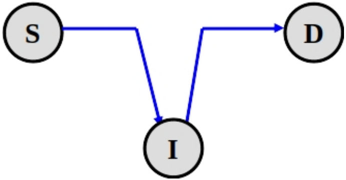


- Interception
  - Attack on confidentiality

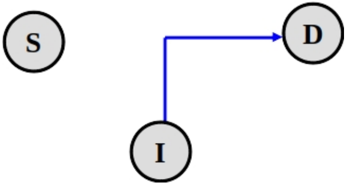


Security Attacks III

- Modification
  - Attack on integrity



- Fabrication
  - Attack on authenticity



Security Mechanism

- A mechanism that is designed to detect, prevent, or recover from a security attack
- Example
  - Cryptography
  - Software Controls (access limitations in a data base, in operating system protect each user from other users)
  - Hardware Controls (smart card)
  - Policies (frequent changes of passwords)
  - Physical Controls

Cryptography

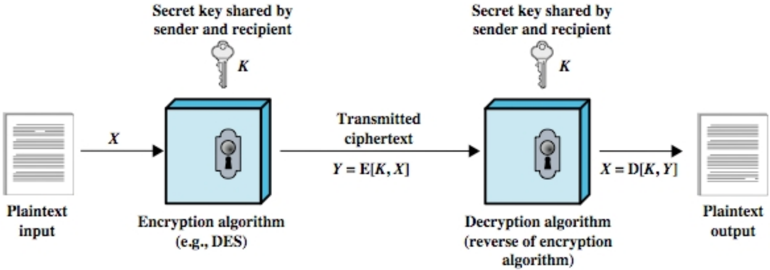
Classified along three independent dimensions:

- The type of operations used for transforming plaintext to ciphertext
  - Substitution
  - Transposition
- The number of keys used
  - Symmetric (single key)
  - Asymmetric (two-keys, or public-key encryption)
- The way in which the plaintext is processed
  - Block cipher processes input one block at a time
  - Stream cipher processes input elements continuously

Secret Key Cryptography Principles I

- Basic ingredients:
  - Plaintext (X)
    - Message to be encrypted
  - Secret Key (K)
    - Shared among the two parties
  - Encryption algorithm (E)
    - Uses X and K
  - Ciphertext (Y)
    - Message after encryption
  - Decryption algorithm (D)
    - Uses Y and K

Secret Key Cryptography Principles II



Secret Key Cryptography Principles III

- Security of the scheme
  - Depends on the secrecy of the key
  - Does not depend on the secrecy of the algorithm
- Assumption
  - Algorithms for encryption/decryption are known to the public
  - Keys used are kept secret

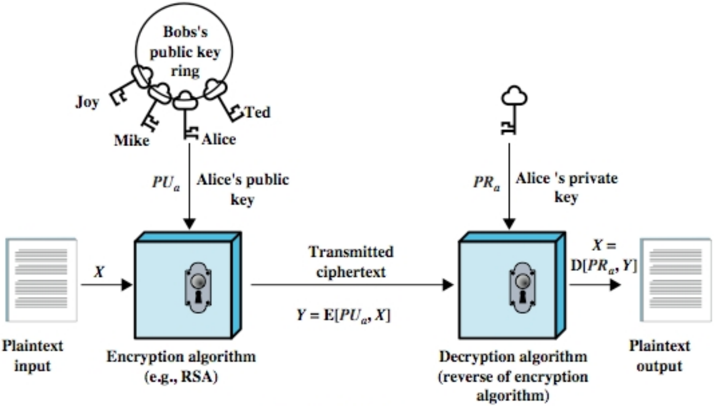
Secret Key Cryptography Algorithms

- Data Encryption Standard (DES): 56 bit key, 64-bit block size
- Advanced Encryption Standard (AES): block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits

Public Key Cryptography Principles I

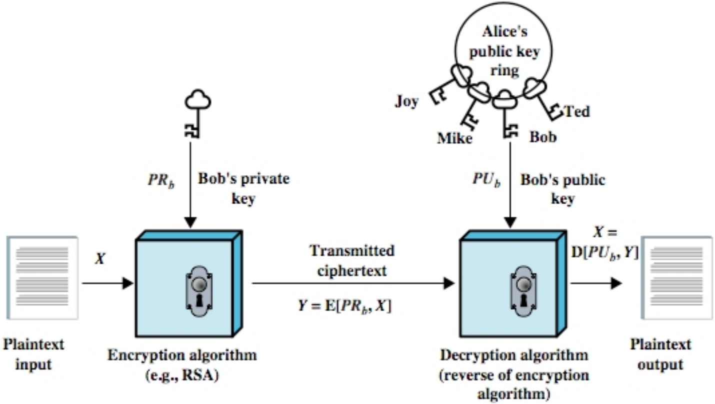
- Basic ingredients:
  - Plaintext (X)
    - Message to be encrypted
  - Public Key (K_{pub}) and Private Key (K_{pri})
    -
  - Encryption algorithm (E)
    - Uses X and either K_{pub} or K_{pri}
  - Ciphertext (Y)
    - Message after encryption
  - Decryption algorithm (D)
    - Uses Y and K_{pri} if K_{pub} was used for encryption / K_{pub} if K_{pri} was used for encryption

Public Key Cryptography Principles II



(a) Confidentiality

Public Key Cryptography Principles III



(b) Authentication

Public Key Cryptography - Requirements

- Computationally easy to create key pairs
- Computationally easy for sender knowing public key to encrypt messages
- Computationally easy for receiver knowing private key to decrypt ciphertext
- Computationally infeasible for opponent to determine private key from public key
- Computationally infeasible for opponent to otherwise recover original message
- Useful if either key can be used for each role

Public Key Cryptography Algorithm: RSA

- A block cipher in which the plaintext and ciphertext are integers between 0 and $n-1$ for some n
- For some plaintext block M and ciphertext block C
  - $C = M^e \bmod n$
  - $M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$
- Public key of $PU = \{e, n\}$, Private key $PR = \{d, n\}$
- Requirements
  - It is possible to find values of e, d, n such that $M^{ed} \bmod n = M$ for all $M < n$.
  - It is relatively easy to calculate M^e and C^d for all values of $M < n$.
  - It is infeasible to determine d given e and n.

Public Key Cryptography Algorithm: RSA

Key Generation

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

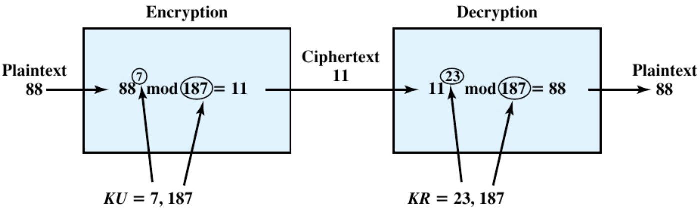
Public Key Cryptography Algorithm: RSA

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

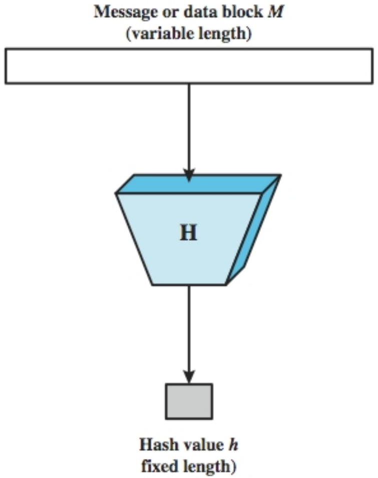
Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod{n}$

Public Key Cryptography Algorithm: RSA Example

1. Select two prime numbers, $p = 17$ and $q = 11$.
2. Calculate $n = pq = 17 \times 11 = 187$.
3. Calculate $\Phi(n) = (p-1)(q-1) = 16 \times 10 = 160$.
4. Select e such that e is relatively prime to $\Phi(n) = 160$ and less than $\Phi(n)$; we choose e $= 7$.
5. Determine d such that de mod $160 = 1$ and $d < 160$. The correct value is $d = 23$, because $23 \times 7 = 161 = 10 \times 160 + 1$.
6. The resulting keys are public key $PU = \{7, 187\}$ and private key $PR = \{23, 187\}$.



Secure Hash Functions



Secure Hash Function Requirements

- Applied to any size data
- H produces a fixed-length output
- $H(x)$ is relatively easy to compute for any given x
- One-way property
  - Given h, it is computationally infeasible to find x such that $H(x) = h$
- Weak collision resistance
  - Given x, it is computationally infeasible to find $y \neq x$ such that $H(y) = H(x)$
- Strong collision resistance
  - It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$

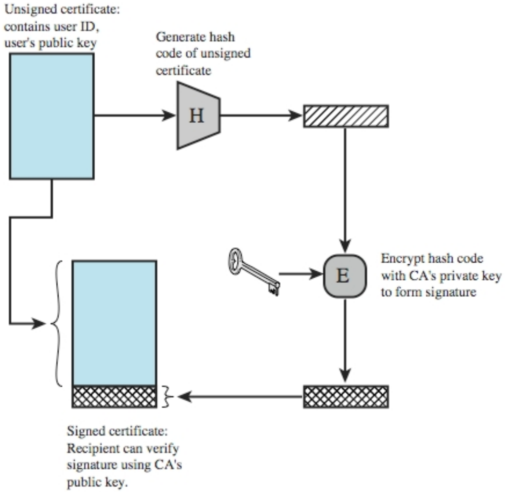
Secure Hash Function Algorithms

- Secure Hash Algorithm-1 (SHA-1),
- Secure Hashing Algorithm-2 family (SHA-2 and SHA-256)
- Message Digest 5 (MD5)

Digital Signature

- An authenticator (a function of the document.) is encrypted with the sender's private key
- It is infeasible to change the document without changing the authenticator
- A secure hash code such as SHA-1 can serve this function
- It is impossible to alter the message without access to Bob's private key
- Digital signature does not provide confidentiality.

Public Key Certificates



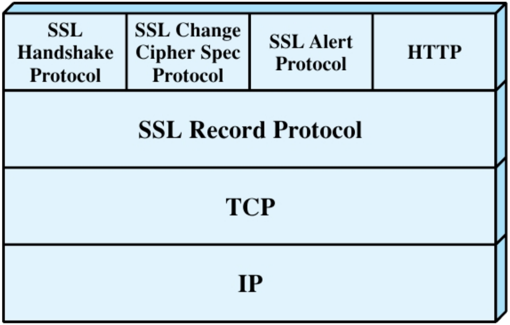
Certification Authority

- A CA is a trusted third party that validates a person's identity and either generates a public/private key pair on their behalf or associates an existing public key provided by the person to that person.
- Once a CA validates someone's identity, they issue a digital certificate that is digitally signed by the CA. The digital certificate can then be used to verify a person associated with a public key when requested.

Secure Sockets Layer (SSL)

- Follow-on Internet standard known as Transport Layer Security (TLS)
- TLS v1.0 RFC 2246
- TLS v1.3: RFC 8446

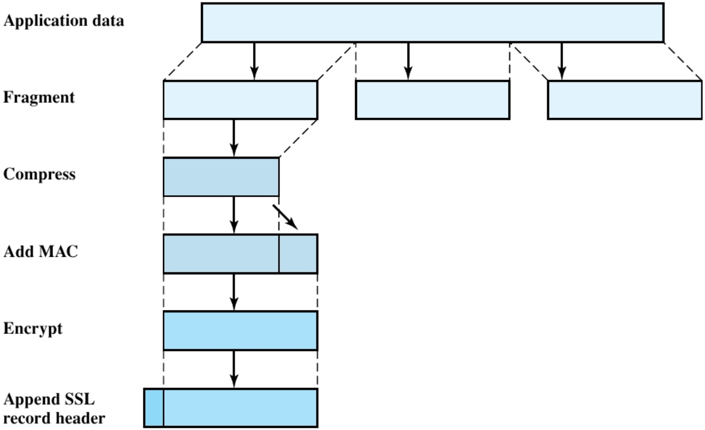
SSL Architecture I



SSL Architecture II

- **Connection**: A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session.
- **Session**: An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

SSL Record Protocol I



SSL Record Protocol II

- Each upper-layer message is fragmented into blocks of 2^{14} bytes (16,384 bytes) or less.
- Next, compression is optionally applied. The next step in processing is to compute a message authentication code over the compressed data.
- Next, the compressed message plus the MAC are encrypted using symmetric encryption.
- Prepend a header, consisting of the following fields:
  - Content Type (8 bits): The higher-layer protocol used to process the enclosed fragment.
  - Major Version (8 bits): Indicates major version of SSL in use. For SSLv3, the value is 3.
  - Minor Version (8 bits): Indicates minor version in use. For SSLv3, the value is 0.
  - Compressed Length (16 bits): The length in bytes of the plaintext fragment (or compressed fragment if compression is used). The maximum value is $2^14 + 2048$.

SSL Change Cipher Spec Protocol

- A single message, which consists of a single byte with the value 1.
- The sole purpose of this message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.

SSL Alert Protocol

- used to convey SSL-related alerts to the peer entity
- alert messages are compressed and encrypted
- Two bytes messages
  - first byte takes the value warning(1) or fatal(2) to convey the severity of the message
  - If the level is fatal, SSL immediately terminates the connection. Other connections on the same session may continue, but no new connections on this session may be established.
  - second byte contains a code that indicates the specific alert
  - example of a fatal alert is an incorrect MAC
  - example of a nonfatal alert is a `close_notify` message, which notifies the recipient that the sender will not send any more messages on this connection

SSL Handshake Protocol