Chapter 5:
CRYPTOGRAPHY OVERVIEW

Content

- Intro
- Block Cipher
- Symmetric Encryption
- Public Key Encryption
- Combining Symmetric and Public Key Encryptions
- Key Management: Generation, Transportation, and Distribution
- Public Key Infrastructure
- Hash Function
- Digital Signatures

Content

- Intro
- Block Cipher
- Symmetric Encryption
- Public Key Encryption
- Combining Symmetric and Public Key Encryptions
- Key Management: Generation, Transportation, and Distribution
- Public Key Infrastructure
- Hash Function
- Digital Signatures

Intro

- Cryptography guarantees authorization, authentication, integrity, confidentiality, and nonrepudiation in all communications and data exchanges in the new information society.

Table 11.1 Modern cryptographic security services

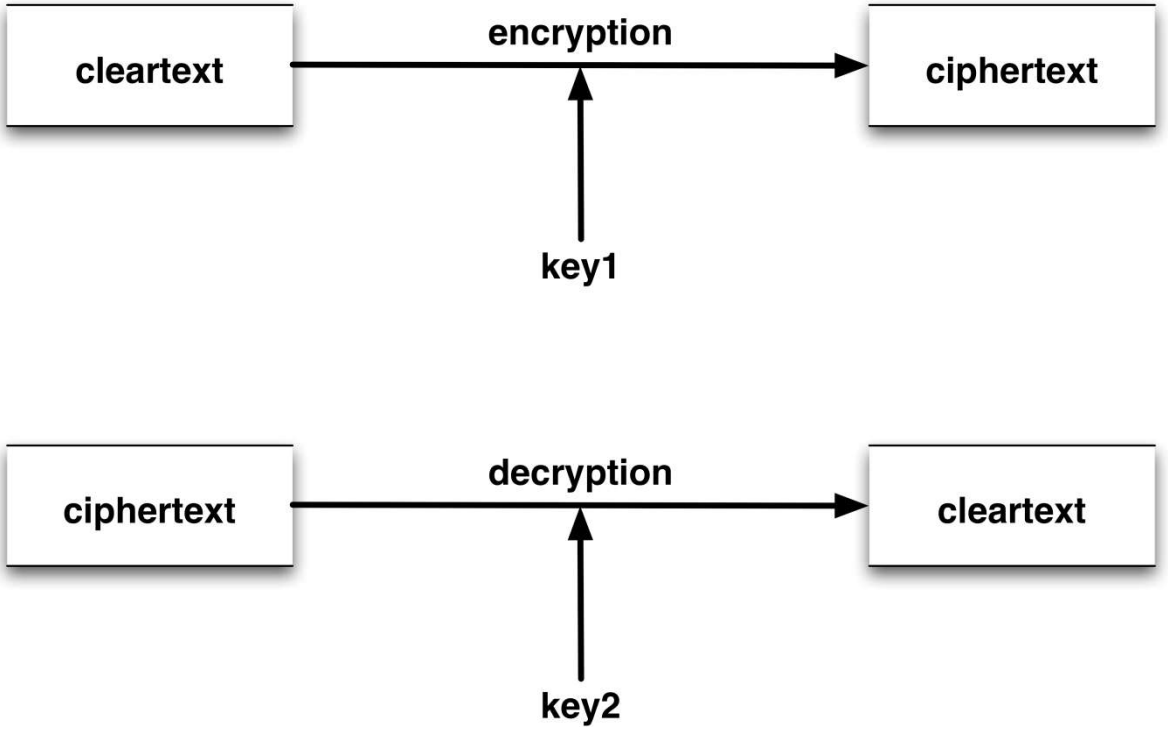
Security Services	Cryptographic Mechanism to Achieve the Service
Confidentiality	Symmetric encryption
Authentication	Digital signatures and digital certificates
Integrity	Decryption of digital signature with a public key to obtain the message digest. The message is hashed to create a second digest. If the digests are identical, the message is authentic and the signer's identity is proven.
Nonrepudiation	Digital signatures of a hashed message then encrypting the result with the private key of the sender, thus binding the digital signature to the message being sent.
Nonreplay	Encryption, hashing, and digital signature

Intro

- A cryptographic system consists of four essential components:
  - Plaintext – the original message to be sent.
  - Cryptographic system (cryptosystem) or a cipher – consisting of mathematical encryption and decryption algorithms.
  - Ciphertext – the result of applying an encryption algorithm to the original message before it is sent to the recipient.
  - Key – a string of bits used by the two mathematical algorithms in encrypting and decrypting processes.

Intro

- The encryption process uses the cryptographic algorithm, known as the encryption algorithm, and a selected key to transform the plaintext data into an encrypted form called ciphertext. The ciphertext can then be transmitted across the communication channels to the intended destination.



Intro

- A cipher can either be a :
  - stream cipher: partition the text into small (e.g. 1 bit) blocks and let the encoding of each block depend on many previous blocks, for each block, a different “key” is generated.
  - block cipher: partition the text into relatively large (e.g. 128 bits) blocks and encode each block separately. The encoding of each block generally depends on at most one of the previous blocks, the same “key” is used at each block.

Content

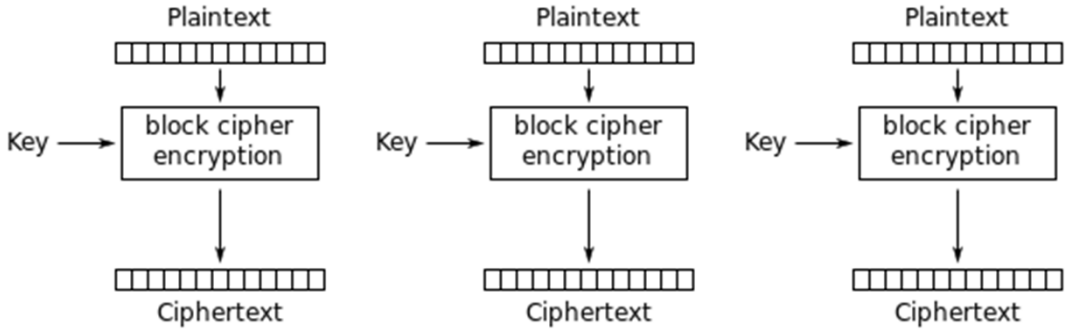
- Intro
- Block Cipher
- Symmetric Encryption
- Public Key Encryption
- Combining Symmetric and Public Key Encryptions
- Key Management: Generation, Transportation, and Distribution
- Public Key Infrastructure
- Hash Function
- Digital Signatures

Block Cipher

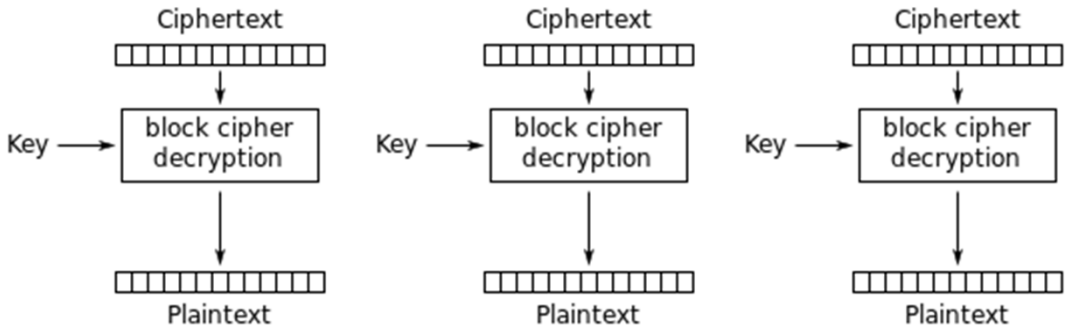
- Block ciphers operate on combinations of blocks (usually 64 bits) of plaintext and ciphertext , may be vulnerable to simple cryptanalysis attacks (the same plaintext always produces the same ciphertext).
- Solution: applying the ciphertext from the previous encrypted block to the next block in a sequence into a combination resulting into a final ciphertext stream.
- To prevent identical messages encrypted on the same day from producing identical ciphertext, an *initialization vector* derived from a *random number generator* is combined with the text in the first block and the key.

Block Cipher

- Several block cipher combination modes of operation:
  - Electronic Codebook (ECB) mode: the message is divided into blocks, and each block is encrypted separately.



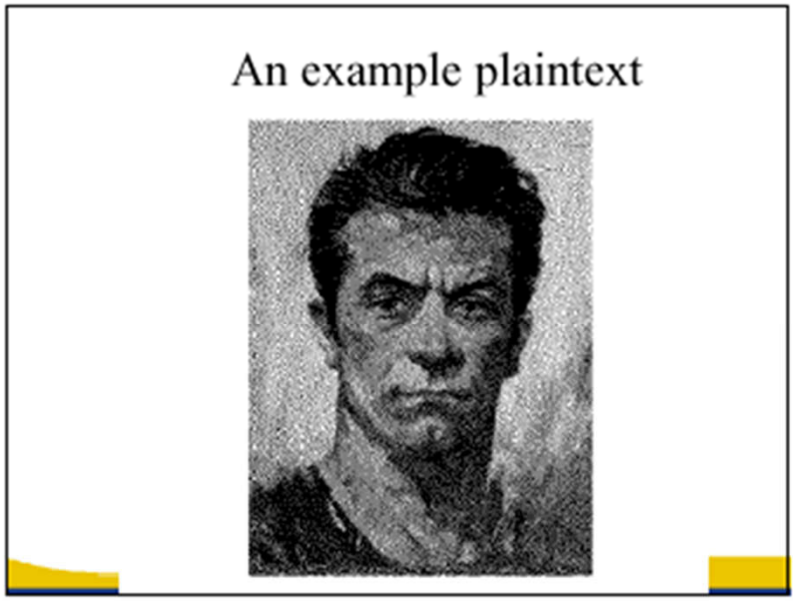
Electronic Codebook (ECB) mode encryption

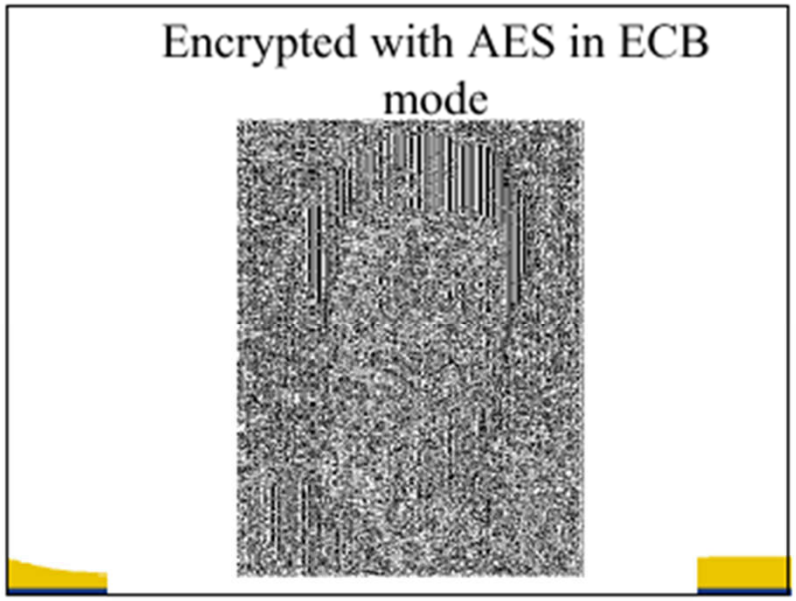


Electronic Codebook (ECB) mode decryption

Block Cipher

- Several block cipher combination modes of operation:
  - Electronic Codebook (ECB) mode: the message is divided into blocks, and each block is encrypted separately.

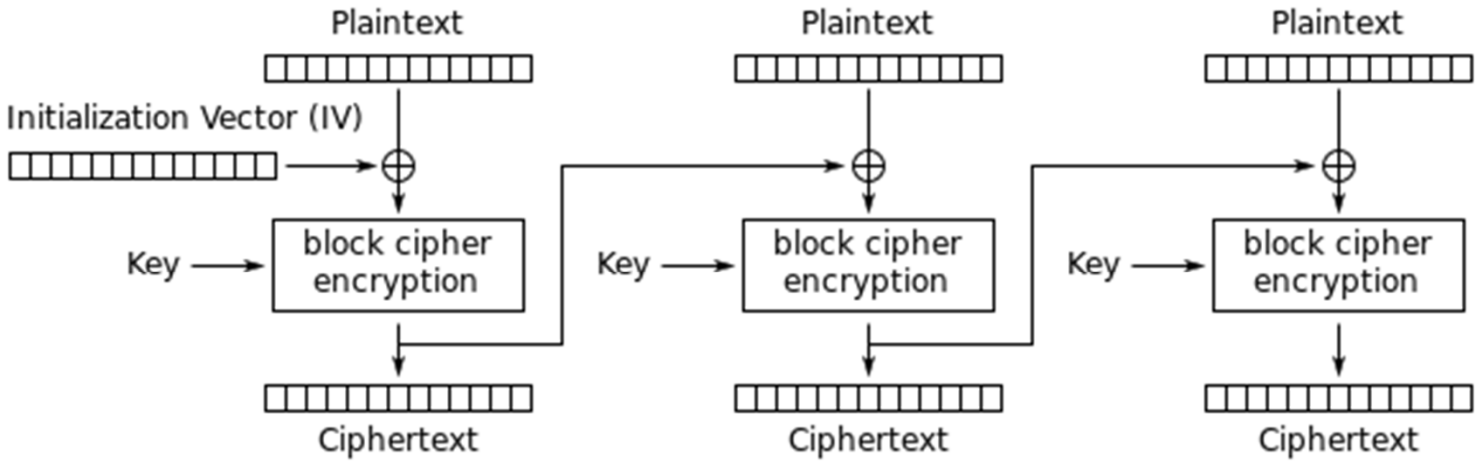




The disadvantage of this method is that identical plaintext blocks are encrypted into identical ciphertext blocks

Block Cipher

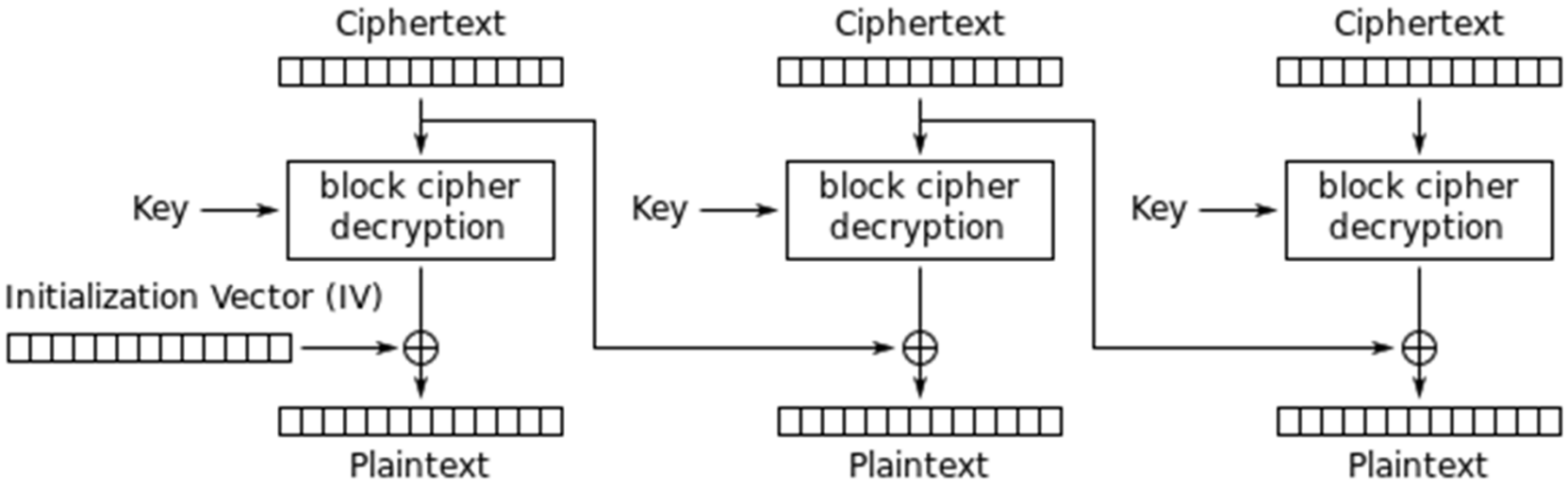
- Several block cipher combination modes of operation:
  - Block Chaining (CBC) mode: each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.



Cipher Block Chaining (CBC) mode encryption

Block Cipher

- Several block cipher combination modes of operation:
  - Block Chaining (CBC) mode



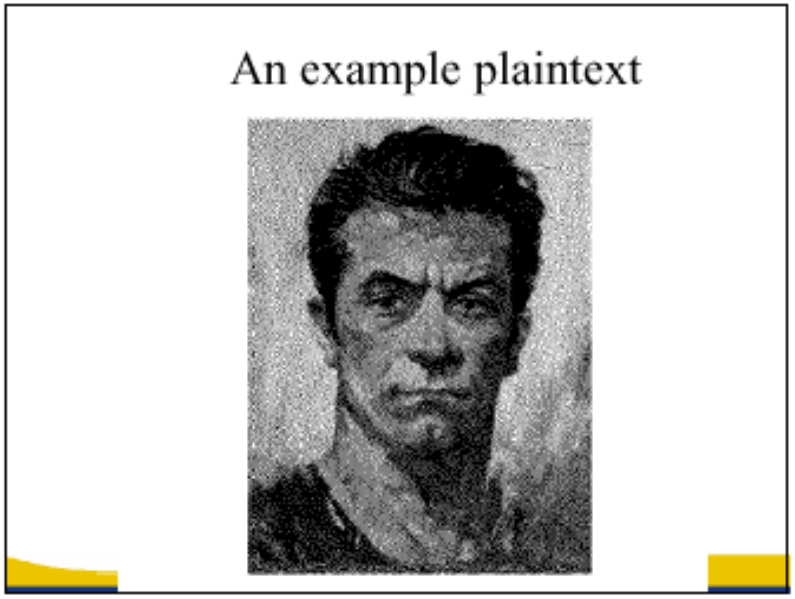
Cipher Block Chaining (CBC) mode decryption

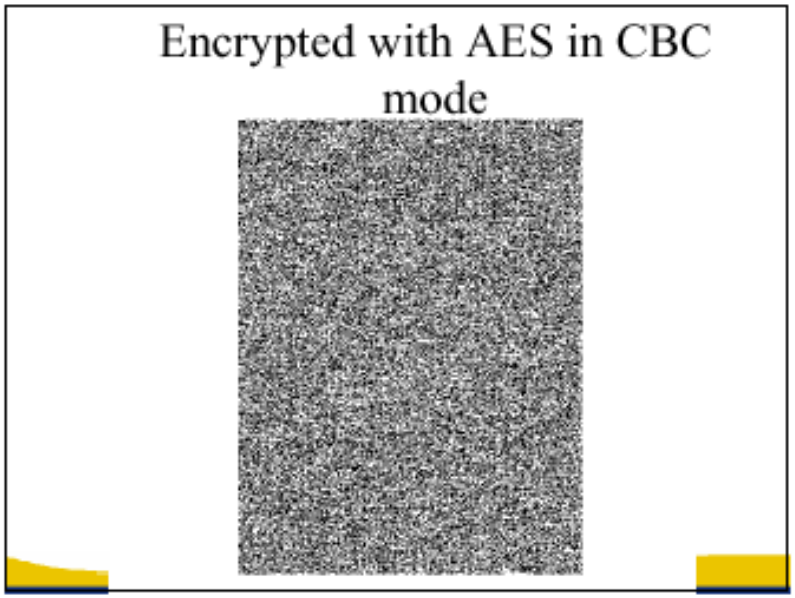
$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$$

$$P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV.$$

Block Cipher

- Several block cipher combination modes of operation:
  - Block Chaining (CBC) mode



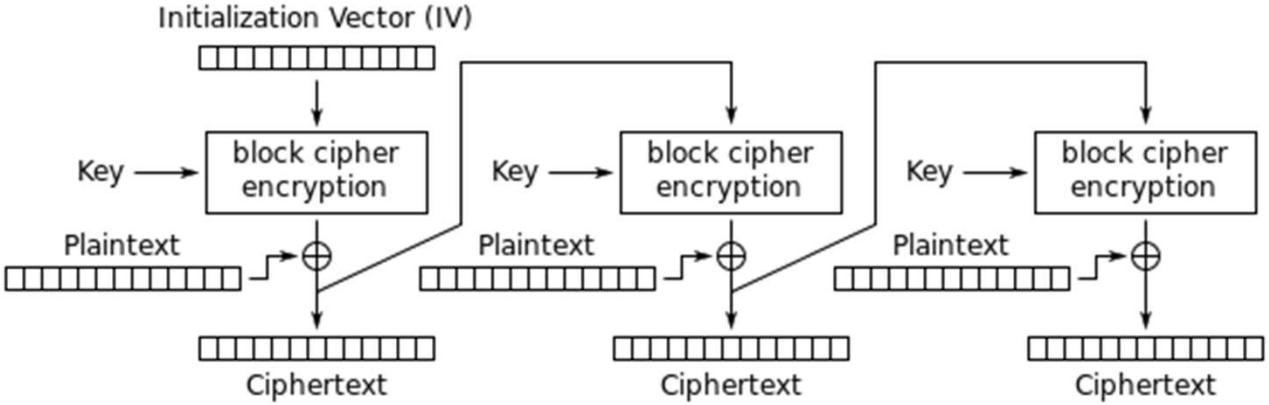


Block Cipher

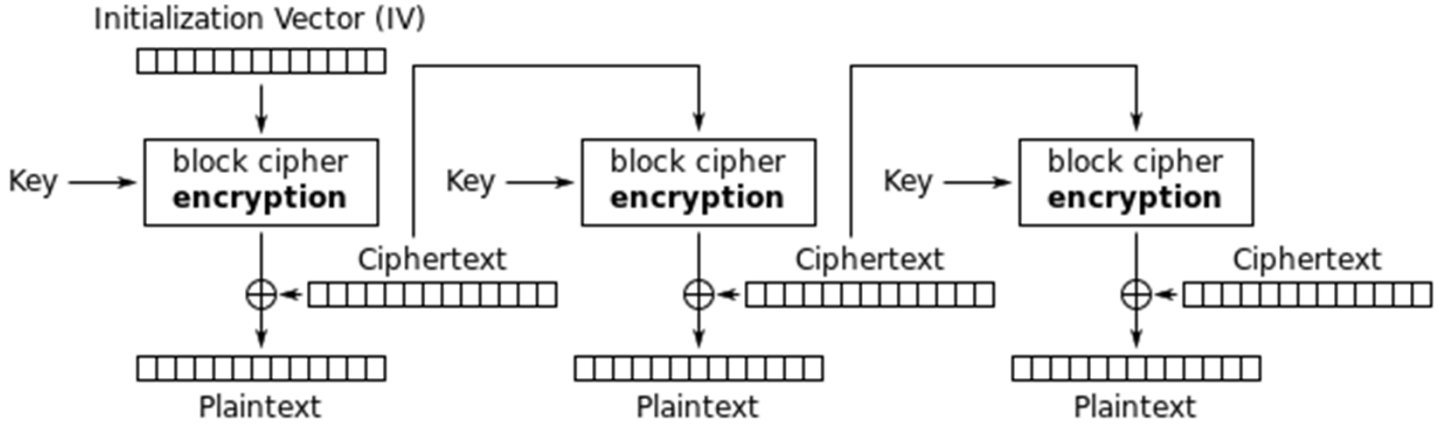
- Several block cipher combination modes of operation:
  - Cipher Feedback (CFB) mode: is similar to the previous CBC in that the following data is combined with previous data, the difference between CBC and CFB is that in CFB data is encrypted a byte at a time and each byte is encrypted along with the previous 7 bytes of ciphertext.

Block Cipher

- Several block cipher combination modes of operation:
  - Cipher Feedback (CFB) mode



Cipher Feedback (CFB) mode encryption



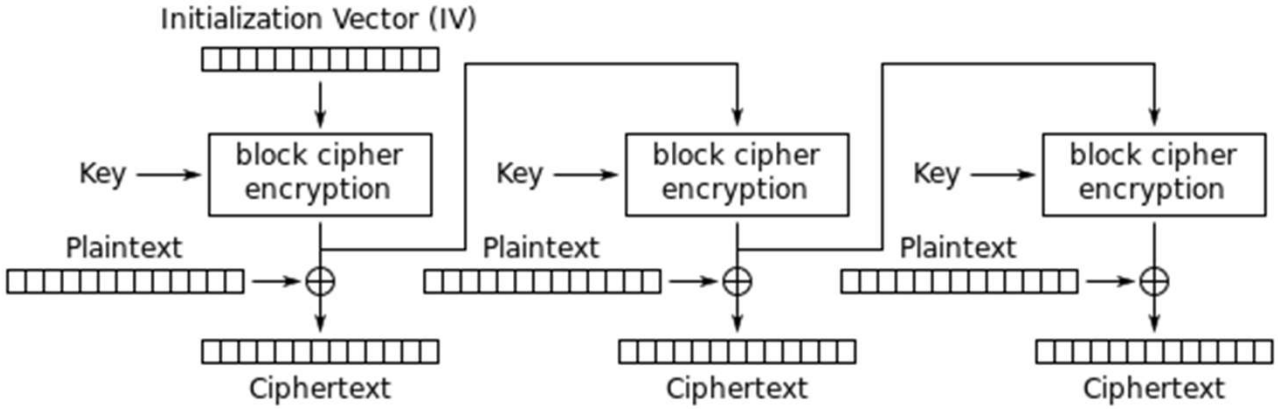
Cipher Feedback (CFB) mode decryption

Block Cipher

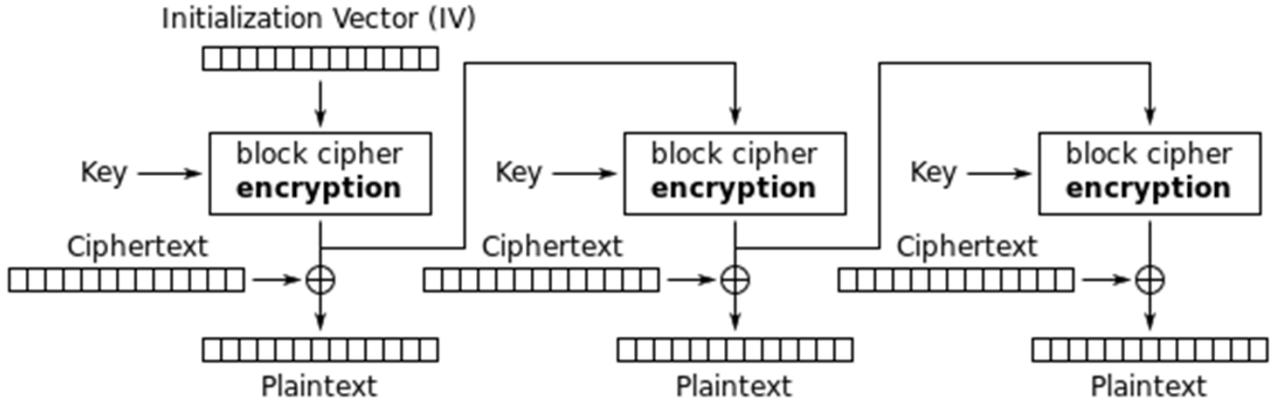
- Several block cipher combination modes of operation:
  - Output Feedback (OFB) mode: is a mode similar to the CFB (permits encryption of differing block sizes), the key difference that the output of the encryption block function is the feedback, not the ciphertext.
    - The XOR value of each plaintext block is created independently of both the plaintext and ciphertext

Block Cipher

- Several block cipher combination modes of operation:
  - Output Feedback (OFB) mode:



Output Feedback (OFB) mode encryption



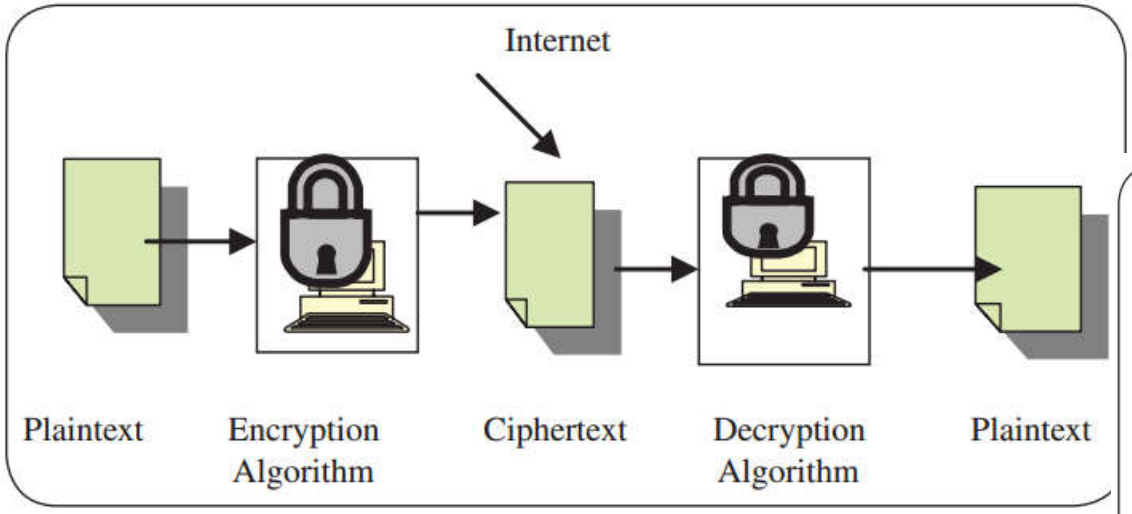
Output Feedback (OFB) mode decryption

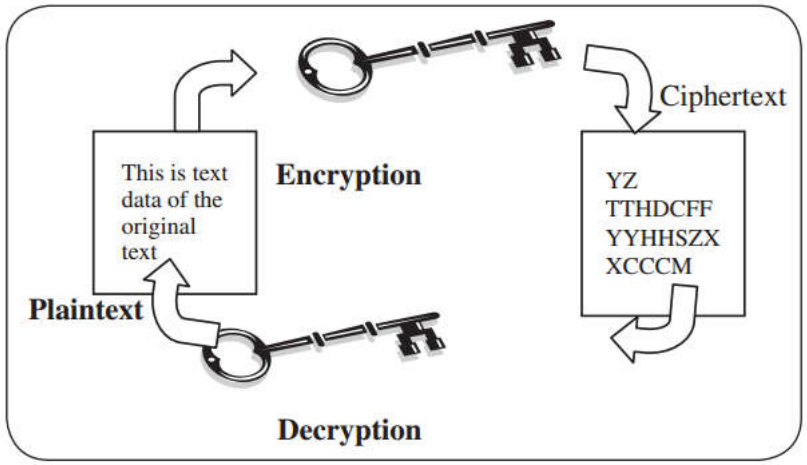
Content

- Intro
- Block Cipher
- Symmetric Encryption
- Public Key Encryption
- Combining Symmetric and Public Key Encryptions
- Key Management: Generation, Transportation, and Distribution
- Public Key Infrastructure
- Hash Function
- Digital Signatures

Symmetric Encryption

- Symmetric encryption (secret key encryption): uses a common key and the same cryptographic algorithm to scramble and unscramble the message.
- Symmetric algorithms are faster than the public key algorithms.





Symmetric Encryption - The key must be shared between the sender and the receiver

Symmetric Encryption Algorithms

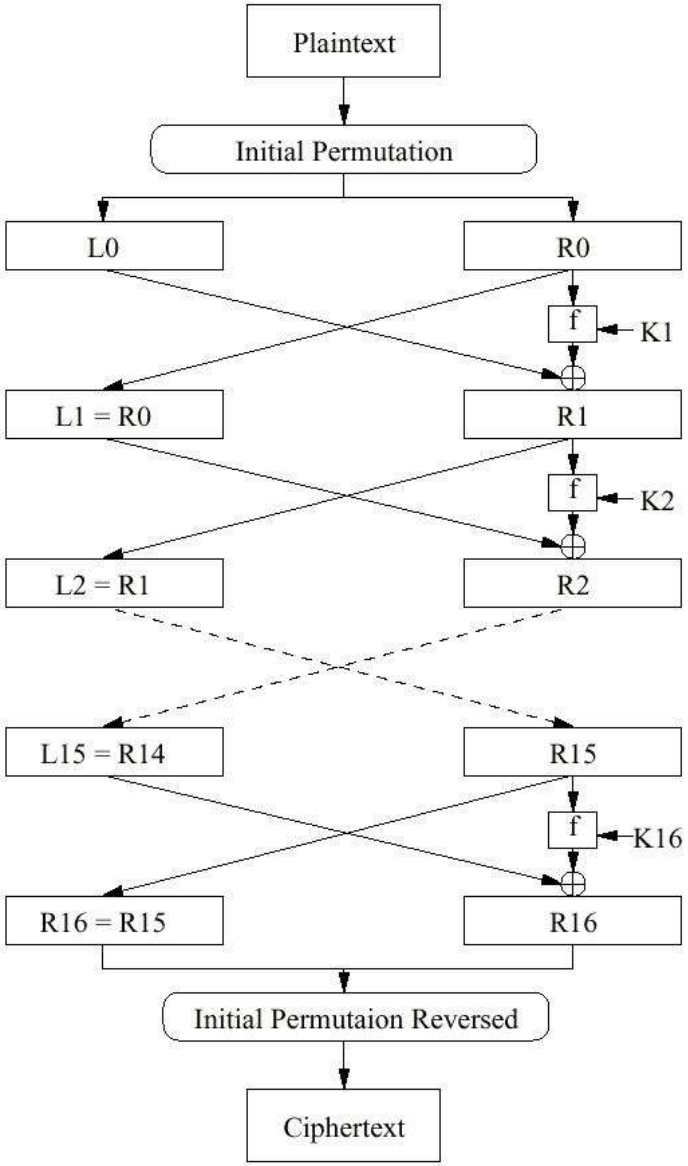
- The most widely used symmetric encryption method in the US is the block ciphers Triple Data Encryption Standard (3DES)
- 3DES uses 64-bit key consisting of 56 effective key bits and 8 parity bits.
- Triple DES encrypts the data in 8-byte chunks, passing it through 16 different iterations consisting of complex shifting, exclusive ORing, substitution, and expansion of the key along with the 64-bit data blocks

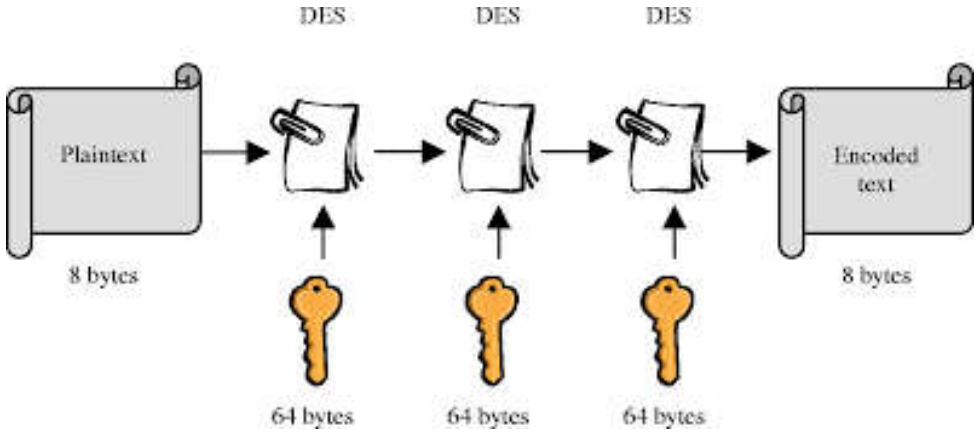
Symmetric Encryption Algorithms

- Weaknesses: key fixed at 56 bits plus 8 bits of parity

=> The National Institute of Standards and Technology (NIST) has presented the **Advanced Encryption Standard (AES) ,** also called Rijndael, which is expected to replace DES.

Symmetric Encryption Algorithms





Symmetric Encryption Algorithms

- Several other symmetric encryption algorithms in use today include International Data Encryption Algorithm (IDEA), Blowfish, Rivest Cipher 4 (RC4), RC5, and CAST-128

Table 11.2 Symmetric key algorithms

Algorithm	Strength	Features (key length)
3DES	Strong	64, 112, 168
AES	Strong	128, 192, 256
IDEA	Strong	64, 128
Blowfish	Weak	32–448
RC4	Weak	
RC5	Strong	32, 64, 128
BEST	Strong	
CAST-128	Strong	32, 128

Problem with Symmetric Encryption

- The Key Exchange Problem
- The Trust Problem
  - The integrity of data can be compromised because the receiver cannot verify that the message has not been altered before receipt.
  - It is possible for the sender to repudiate the message because there are no mechanisms for the receiver to make sure that the message has been sent by the claimed sender.
  - The secret key may not be changed frequently enough to ensure confidentiality

Content

- Intro
- Block Cipher
- Symmetric Encryption
- Public Key Encryption
- Combining Symmetric and Public Key Encryptions
- Key Management: Generation, Transportation, and Distribution
- Public Key Infrastructure
- Hash Function
- Digital Signatures

Public Key Encryption

- Public key encryption,commonly known asymmetric encryption, uses two different keys, a public key known to all and a private key known only to the sender and the receiver.
- To encrypt a message from sender A to receiver B, both A and B must create their own pairs of keys. Then A and B publicize their public keys – anybody can acquire them.

Public Key Encryption

- When A has to send a message M to B
  - A uses B's public key to encrypt M
  - On receipt of M, B then uses his or her private key to decrypt the message M
- Data confidentiality and integrity in public key encryption is also guaranteed

Public Key Encryption

- Data confidentiality and integrity in public key encryption is also guaranteed

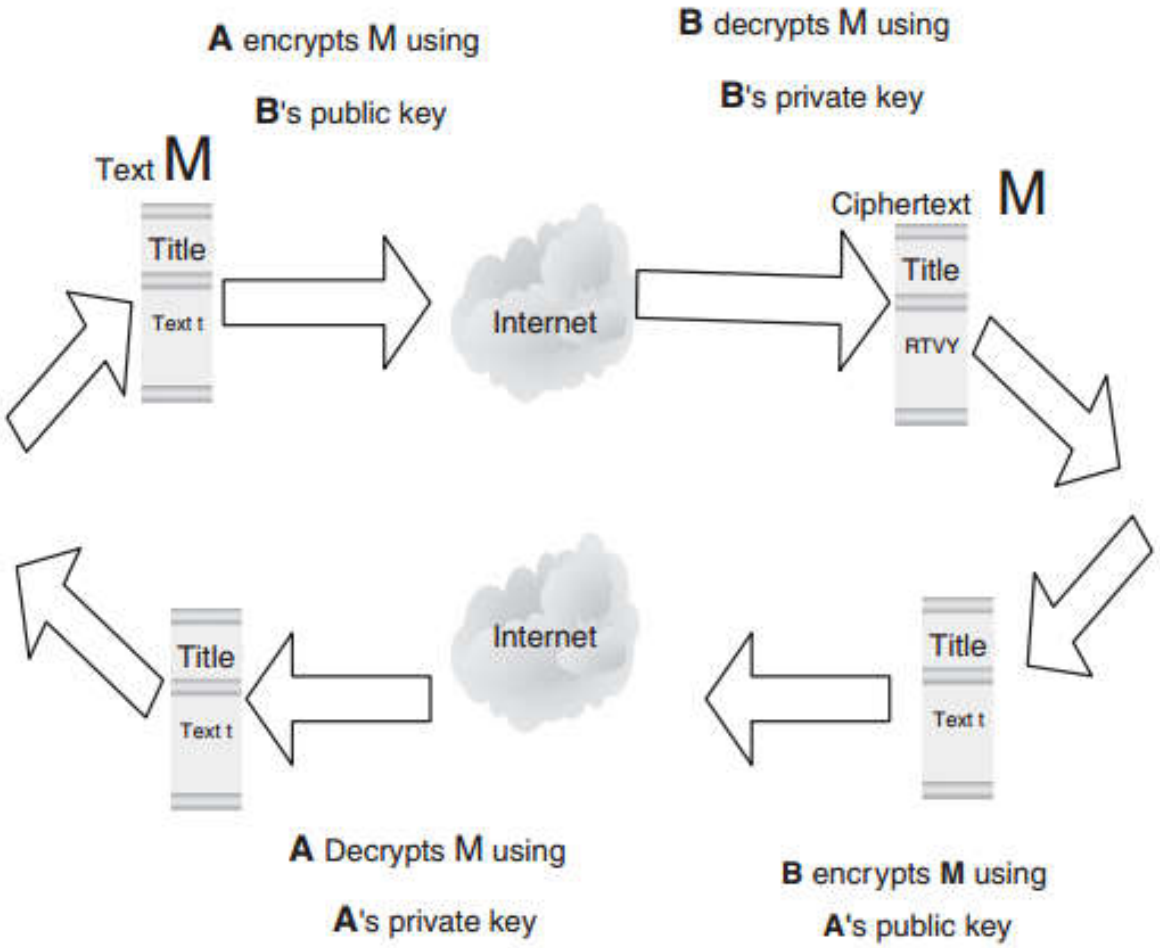


Fig. 11.4 Public Key Encryption with Data Integrity and Confidentiality

Public Key Encryption

- Guaranteeing of sender nonrepudiation and user authentication:
  - After both A and B have created their own pairs of keys and exchanged the public key pair.
  - A, the sender, then encrypts the message to be sent to B, the recipient, using the sender's private key.
  - Upon receipt of the encrypted message, B, the recipient, then uses A's, the sender's public key to decrypt the message.
  - The return route is also similar

Public Key Encryption

- Guaranteeing of sender nonrepudiation and user authentication:

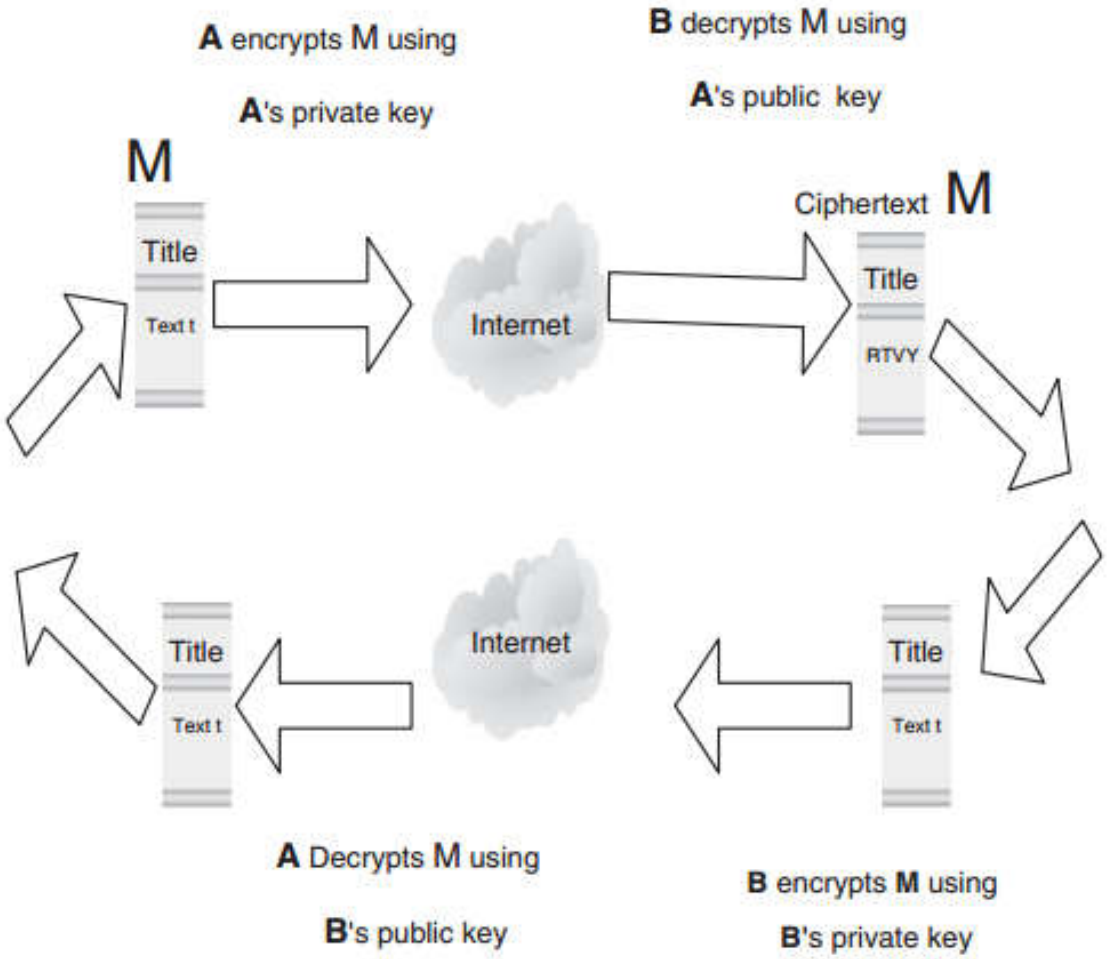
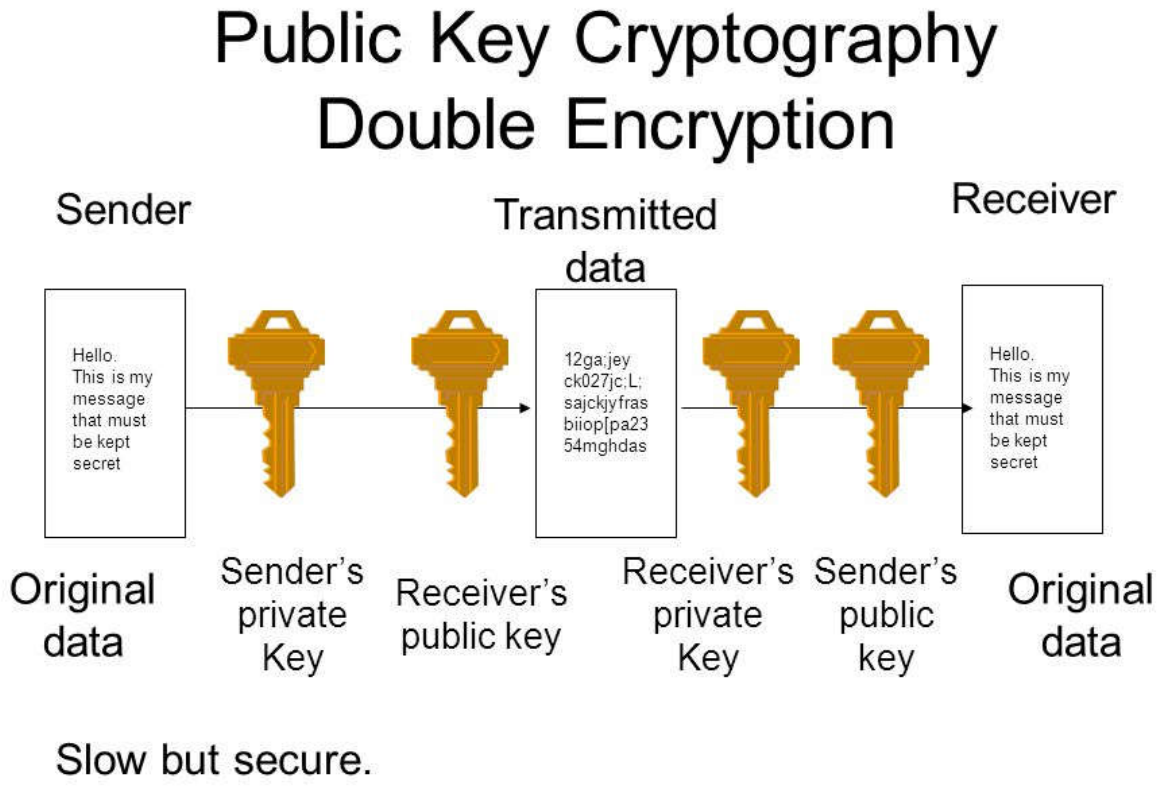


Fig. 11.5 Authentication and Non-repudiation

Public Key Encryption

- To ensure all four aspects of security: data confidentiality and integrity and authentication and nonrepudiation of users, a double encryption is required as illustrated:



Public Key Encryption

- The core of public key encryption is that no secret key is passed between two communicating parties
- Public key encryption can support all communication topologies including one-to-one, one-to-many, many-to-many, and many-to-one, and along with it, several to thousands of people can communicate with one party without exchange of keys

=> suitable for Internet communication and electronic commerce applications

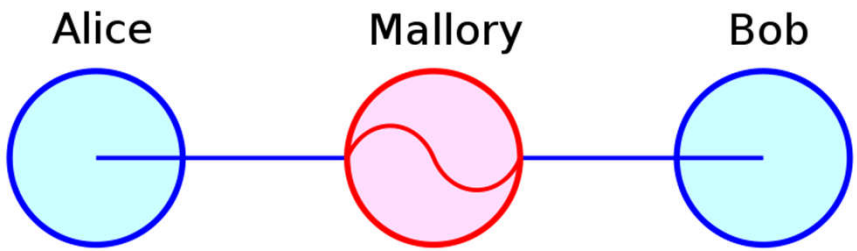
Public Key Encryption Algorithms

Table 11.3 Public key algorithms

Algorithm	Strength	Features (key length)
RSA	Strong	768, 1024
ElGamal	Strong	768, 1024
DSA	Strong	512 to 1024
Diffie-Halmann	Strong	768, 1024

Problem with Public Key Encryption

- The biggest problem for public key cryptographic scheme is speed. Public key algorithms are extremely slow compared to symmetric algorithms (public key calculations take longer than symmetric key calculations)
- man-in-the-middle attack



Public Key Encryption Services

- Secrecy which makes it extremely difficult for an intruder who is able to intercept the ciphertext to be able to determine its corresponding plaintext.
- Authenticity which makes it possible for the recipient to validate the source of a message.
- Integrity which makes it possible to ensure that the message sent cannot be modified in any way during transmission.
- Nonrepudiation which makes it possible to ensure that the sender of the message cannot later turn around and disown the transmitted message.

Content

- Intro
- Block Cipher
- Symmetric Encryption
- Public Key Encryption
- Combining Symmetric and Public Key Encryptions
- Key Management: Generation, Transportation, and Distribution
- Public Key Infrastructure
- Hash Function
- Digital Signatures

Enhancing Security: Combining Symmetric and Public Key Encryptions

- Weaknesses of Symmetric & Public key encryption.

⇒ A hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem.

- A hybrid cryptosystem can be constructed using any two separate cryptosystems:
  - a **key encapsulation** scheme, which is a public-key cryptosystem
  - a **data encapsulation** scheme, which is a symmetric-key cryptosystem.

Enhancing Security: Combining Symmetric and Public Key Encryptions

- To encrypt a message addressed to Alice in a hybrid cryptosystem, Bob does the following:
  - Obtains Alice's public key.
  - Generates a fresh symmetric key for the data encapsulation scheme.
  - Encrypts the message under the data encapsulation scheme, using the symmetric key just generated.
  - Encrypt the symmetric key under the key encapsulation scheme, using Alice's public key.
  - Send both of these encryptions to Alice.
- To decrypt this hybrid ciphertext, Alice does the following:
  - uses her private key to decrypt the symmetric key contained in the key encapsulation segment.
  - uses this symmetric key to decrypt the message contained in the data encapsulation segment.

Content

- Intro
- Block Cipher
- Symmetric Encryption
- Public Key Encryption
- Combining Symmetric and Public Key Encryptions
- Key Management: Generation, Transportation, and Distribution
- Public Key Infrastructure
- Hash Function
- Digital Signatures

Key Management: Generation, Transportation, and Distribution

- The key exchange problem.
- The strength of an encryption algorithm lies in its key distribution techniques.
- Symmetric & public key encryption problems can be solved using a trusted third party or an intermediary:
  - For symmetric key cryptography, the trusted intermediary is called a Key Distribution Center(KDC)
  - For public key cryptography, the trusted and scalable intermediary is called a Certificate Authority (CA)

Key Distribution Center(KDC)

- First both the message sender A and the message receiver B each must have a secret key they each share with the KDC.

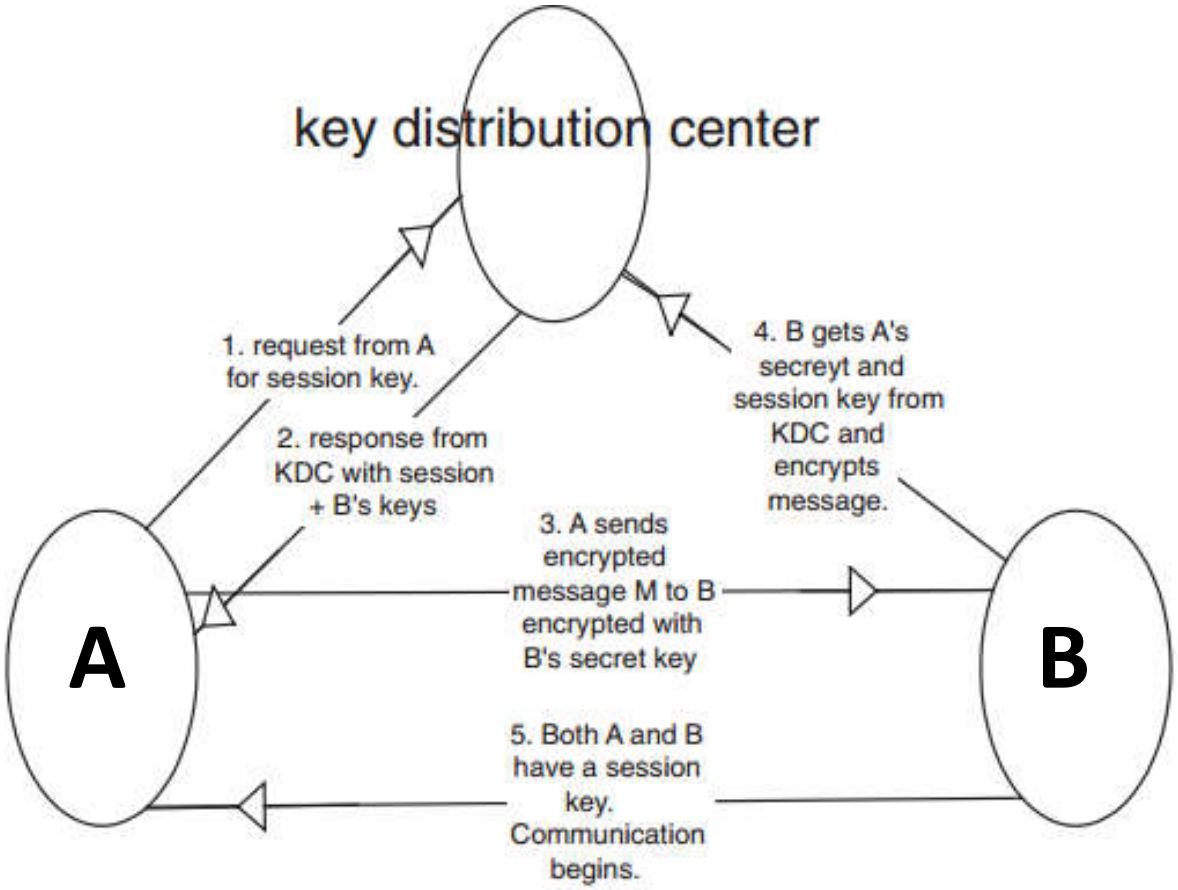


Fig. 11.7 The Working of a KDC

Key Distribution Center(KDC)

- A initiates the communication process by sending a request to the KDC for a session key and B's secret key

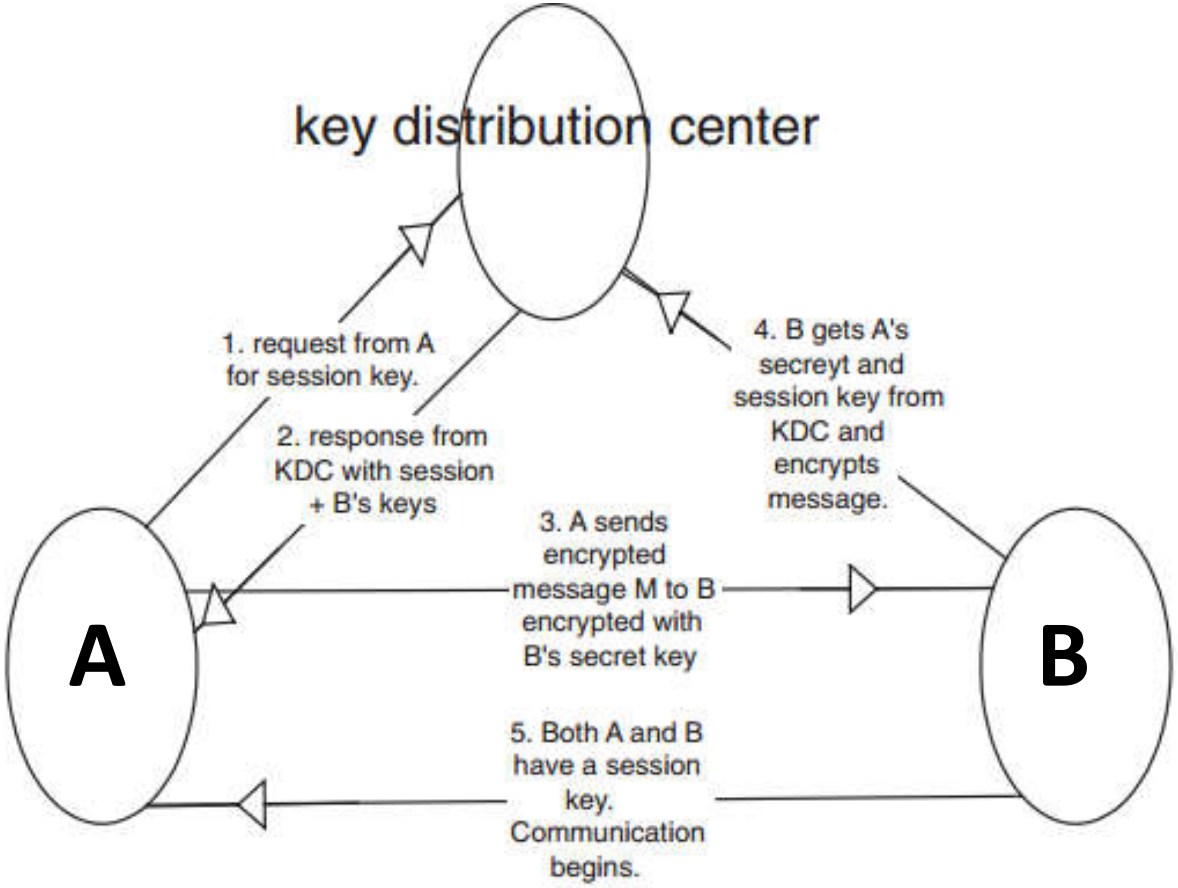


Fig. 11.7 The Working of a KDC

Key Distribution Center(KDC)

- The KDC responds to this request by sending a two-part packet to A.
  - The first part to be sent to A: B's secret key, and a session key
  - The second part, to be sent to B, consists of A's identity and a copy of the session key given to A
- The packet is encrypted by the secret key the KDC shares with A.
- When A receives the packet, A then gets out B's secret key and encrypts the message together with B's part of the packet with B's secret key and sends it to B

Key Distribution Center(KDC)

- On receipt, B uses the secret key B shares with the KDC to decrypt the package from A to recover the session key. Now the session key has been distributed to both A and B

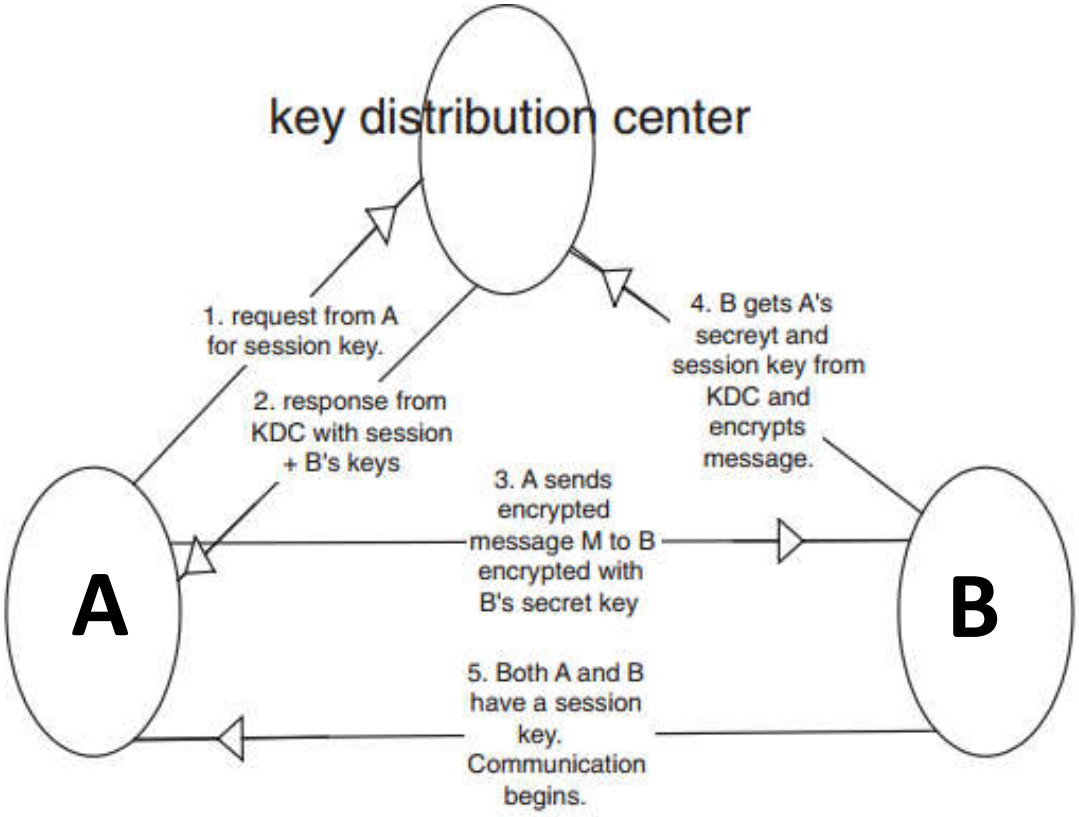


Fig. 11.7 The Working of a KDC

Key Distribution Center(KDC)

- The KDC has several disadvantages including the following:
  - The two network communicating elements must belong to the same KDC
  - Security becomes a problem because a central authority having access to keys
  - In large networks, the KDC then becomes a bottleneck since each pair of users needing a key must access a central node at least once. Also the failure of the central authority could disrupt the key distribution system

=> Solution: Public Key Infrastructure (PKI)

Public Key Management

- Solutions for distribution of public keys:
  - Public announcements where any user can broadcast their public keys or send them to selected individuals
  - Public directory which is maintained by a trusted authority. The directory is usually dynamic to accommodate additions and deletions
  - Certificate Authority (CA) to distribute certificates to each communicating element. Each communicating element in a network or system communicates securely with the CA to register its public key with the CA.

Public Key Management – Certificate Authority

- The CA then certifies that a public key belongs to a particular entity (person or a server in a network).
- In the Internet, CAs are equivalent to the digital world's passport offices because they issue digital certificates and validate the holder's identity and authority.
- Once the CA verifies the identity of the entity, the CA creates a *digital certificate* that binds the public key of the element to the identity.
- The certificate contains the public key and other identifying information about the owner of the public key (for example, a human name or an IP address). *The certificate is digitally signed by the CA*.

Public Key Management – Digital Certificates

- A digital certificate is a digitally signed message used to attest to the validity of the public key of a communicating element.
- Digital certificates must adhere to a format

Table 11.4 The ITU-T X.509 digital certificate format [6]

Field	Purpose
Version number	Most certificates use X.509 version 3.
Serial number	Unique number set by a CA
Issuer	Name of the CA
Subject issued certificate	Name of a receiver of the certificate
Validity period	Period in which certificate will valid
Public-key algorithm information of the subject of the certificate	Algorithm used to sign the certificate with digital signature
Digital signature of the issuing authority	Digital signature of the certificate signed by CA
Public key	Public key of the subject

Public Key Management – Digital Certificates

- The server sends the public key in a certificate signed by a *certificate authority*. The client checks that digital signature. If the signature is valid, the client knows that the CA has certified that this is the server's authentic certificate, not a certificate forged by a man-in the-middle.
- Several companies now offer digital certificates – that means they are functioning as CAs: VeriSign, American Express, Netscape, US Postal Service, and Cybertrust.

Key Escrow

- Key escrow (also known as a “fair” cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys.
- These third parties may include businesses, who may want access to employees' private communications, or governments, who may wish to be able to view the contents of encrypted communications.

Content

- Intro
- Block Cipher
- Symmetric Encryption
- Public Key Encryption
- Combining Symmetric and Public Key Encryptions
- Key Management: Generation, Transportation, and Distribution
- Public Key Infrastructure
- Hash Function
- Digital Signatures

Public Key Infrastructure (PKI)

- Public key infrastructure (PKI) as the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke certificates based on public key cryptography - **Merike Kaeo**
- PKI creates and distributes digital certificates widely to many users in a trusted manner.
- PKI is made up of four major pieces:
  - The certificates that represent the authentication token.
  - The CA that holds the ultimate decision on subject authentication
  - The registration authority (RA) that accepts and processes certificate signing requests on behalf of end users
  - The Lightweight Directory Access Protocol (LDAP) directories that hold publicly available certificate information [8].

Public Key Infrastructure (PKI)

- CA (Certificate Authority):
  - CAs are vital in PKI technology to authoritatively associate a public key signature with an alleged identity by signing certificates that support the PKI
- Registration Authority (RA):
  - An authority in a network that verifies user requests for a digital certificate and tells the Certificate Authority (CA) to issue it.
- Lightweight Directory Access Protocols (LDAP)
  - These are repositories that store and make available certificates

Public Key Infrastructure (PKI)

- Certificates:
  - Public keys are distributed through digital certificates
  - The validation of the identity of the public key on the certificate is made by the CA that signs the certificate before it is issued to the user
  - Certificate has nine fields. The first seven make up the body of the certificate. Any change in these fields may cause the certificate to become invalid. If a certificate becomes invalid, the CA must revoke it

Content

- Intro
- Block Cipher
- Symmetric Encryption
- Public Key Encryption
- Combining Symmetric and Public Key Encryptions
- Key Management: Generation, Transportation, and Distribution
- Public Key Infrastructure
- Hash Function
- Digital Signatures

Hash Function

- Another way to provide data integrity and authenticity is to use hash functions
- A hash function is a mathematical function that takes an input message M of a given length and creates a unique fixed length output code (usually a 128-bit or 160-bit stream, called a hash or a message digest).
- The same hash function on the same message always results in the same message digest.

Hash Function

- In ensuring data integrity and authenticity, both the sender and the recipient perform the same hash computation using the same hash function on the message before the message is sent and after it has been received. If the two computations of the same hash function on the same message produce the same value, then the message has not been tampered with during transmission.

Results	
Original text	Hello world!
Original bytes	48:65:6c:6c:6f:20:77:6f:72:6c:64:21 (length=12)
CRC32	1b851995
MD5	86fb269d190d2c85f6e0468ceca42a20
SHA-1	d3486ae9136e7856bc42212385ea797094475802
SHA-256	c0535e4be2b79ffd93291305436bf889314e4a3faec05ecffcbb7df31ad9e51a

Hash Function

- There are various standard hash functions of message digest length including the 160-bit (SHA-1 and MD5) and 128-bit streams (RSA, MD2, and MD4).
- The most popular of these hash algorithms are SHA and MD5

Table 11.5 Standard hash algorithms

Algorithm	Digest length (bits)	Features (key length)
SHA-1	160	512
MD5	160	512
HMAC-MD5	Version of MD5	512 (key version of MD5)
HMAC-SHA-1	Version of SHA-1	512 (key version of SHA-1)
PIPEND	160	128

Content

- Intro
- Block Cipher
- Symmetric Encryption
- Public Key Encryption
- Combining Symmetric and Public Key Encryptions
- Key Management: Generation, Transportation, and Distribution
- Public Key Infrastructure
- Hash Function
- Digital Signatures

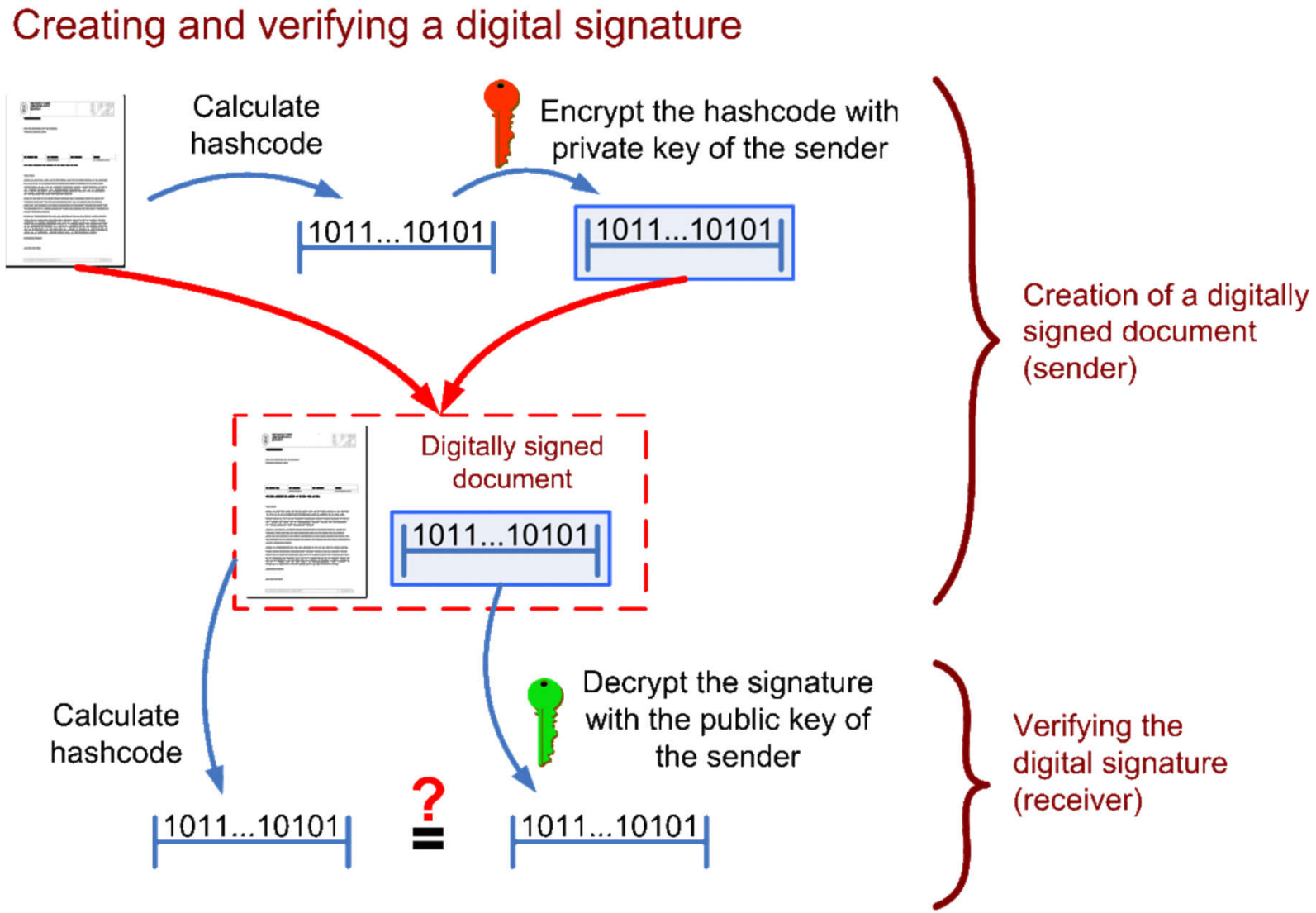
Digital Signature

- Hash functions: ensure the integrity and authenticity of the message. About the nonrepudiation of the users?
- A digital signature is defined as an encrypted message digest, by the private key of the sender, appended to a document to analogously authenticate it.
- A digital signature is used to confirm the identity of the sender and the integrity of the document. It establishes the nonrepudiation of the sender.

Digital Signature

- Digital signatures are formed using a combination of public key encryption and one-way secure hash function according to the following steps:
  - The sender of the message uses the message digest function to produce a message authentication code (MAC).
  - This MAC is then encrypted using the private key and the public key encryption algorithm. This encrypted MAC is attached to the message as the digital signature.
  - The recipient separates the received message into two: the original document and the digital signature.
  - Using the sender's public key, the recipient then decrypts the digital signature which results in the original MAC.
  - The recipient then uses the original document and inputs it to the hash function to produce a new MAC.
  - The new MAC is compared with the MAC from the sender for a match.

Digital Signature



Readmore

- http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
- http://en.wikipedia.org/wiki/Public_key_infrastructure
- http://en.wikipedia.org/wiki/Cryptography
- Guide to Computer Network Security (Chapter 11, pg227-pg246)