CY 261 CRYPTOGRAPHY

Dr. Qasem Abu Al-Haija
Department Of Cybersecurity

10/10/2023

Chapter 1: Introduction to Cryptography

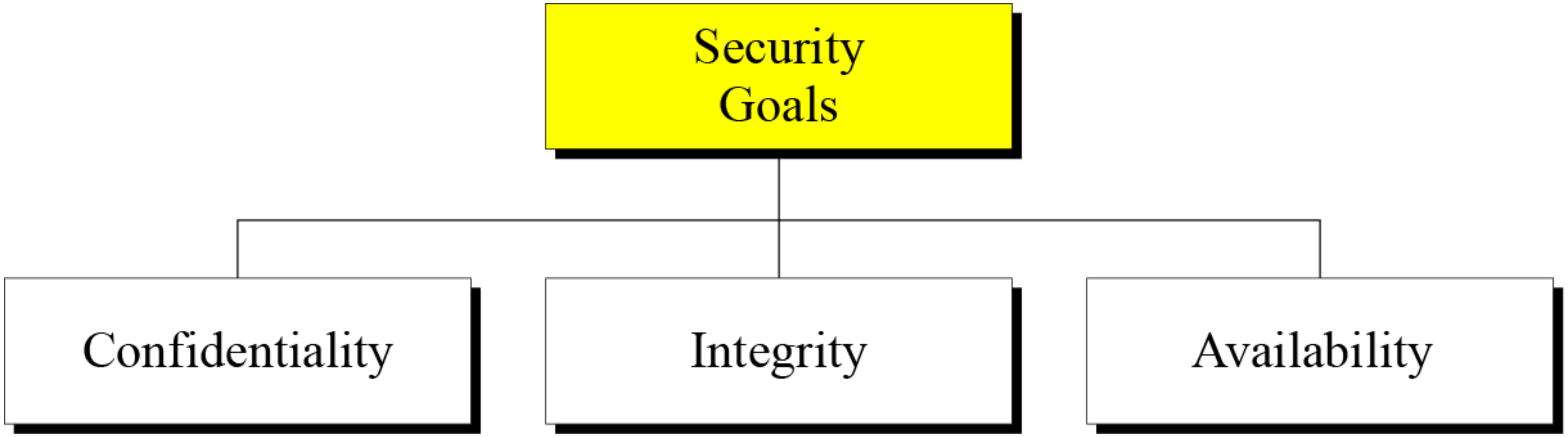
Objectives

- To define three security goals
- To define security attacks that threaten security goals
- To define security services and how they are related to the three security goals
- To define security mechanisms to provide security services
- To introduce two techniques, cryptography and steganography, to implement security mechanisms.

Outline

- What is cryptography and cryptology?
- The main components of a crypto system.
- Problems solved by cryptography.
- Basic concepts: symmetric cryptography, asymmetric cryptography, digital signatures.
- Types of algorithms and related concepts.

Topic 1: Security Goals



- Figure 1 Taxonomy of security goals

Topic 1: Security Goals

- Figure 1 Taxonomy of security goals

1.1 Confidentiality

- Confidentiality is probably the most common aspect of information security.

- We need to protect our confidential information.

- An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

1.2: Integrity

- Information needs to be changed constantly.

- Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

1.3: Availability

- The information created and stored by an organization needs to be available to authorized entities.

Topic 2: ATTACKS

- The three goals of security—confidentiality, integrity, and availability—can be threatened by security attacks.
- Topics discussed in this section:

2.1 Attacks Threatening Confidentiality

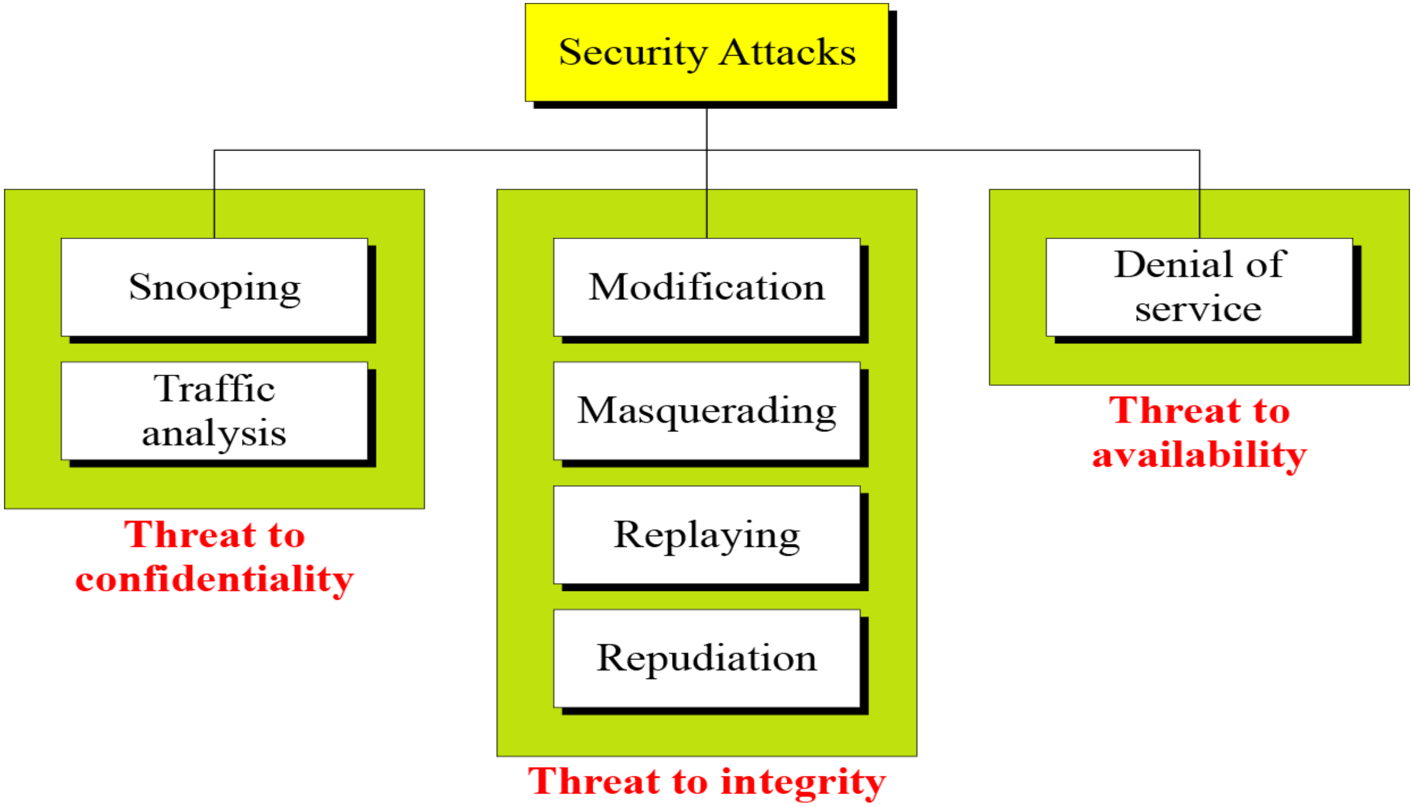
2.2 Attacks Threatening Integrity

2.3 Attacks Threatening Availability

2.4 Passive versus Active Attacks

Topic 2: ATTACKS

- Figure 1.2 Taxonomy of attacks with relation to security goals



2.1: Attacks Threatening Confidentiality

- **Snooping** refers to unauthorized access to or interception of data.

- **Traffic analysis** refers to obtaining other information by monitoring online traffic.

2.2: Attacks Threatening Integrity

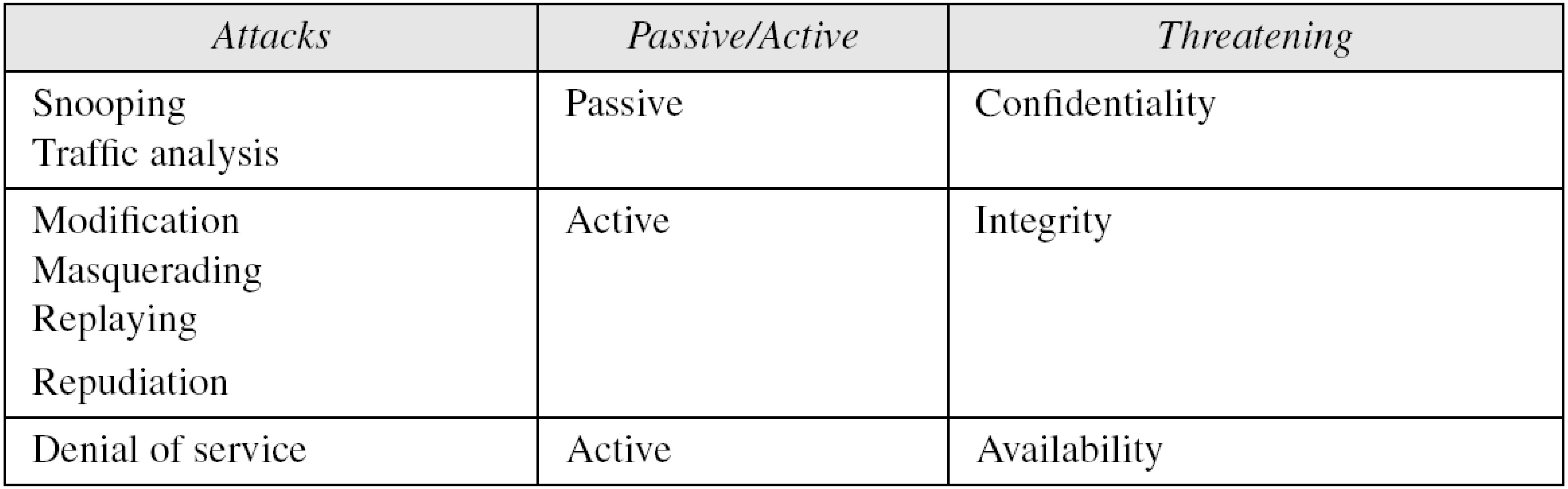
- **Modification** means that the attacker intercepts the message and changes it.
- **Masquerading** or **spoofing** happens when the attacker impersonates somebody else.
- **Replaying** means the attacker obtains a copy of a message sent by a user and later tries to replay it.
- **Repudiation** means that sender of the message might later deny that he/she has sent the message; the receiver of the message might later deny that he/she has received the message.

2.3: Attacks Threatening Availability

- **Denial of service** (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

2.3: Passive Versus Active Attacks

Table 2.1 Categorization of passive and active attacks



Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

Topic 3: SERVICES AND MECHANISMS

- ITU-T provides some security services and some mechanisms to implement those services.
- Security services and mechanisms are closely related because a mechanism or combination of mechanisms is used to provide a service.
- Topics discussed in this section:

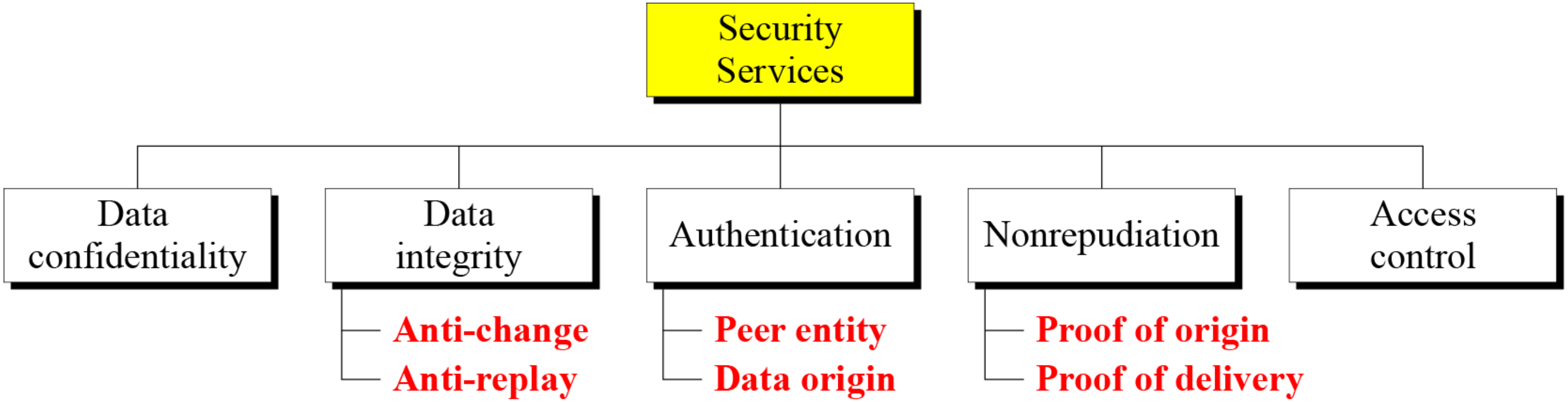
  3.1 Security Services

  3.2 Security Mechanism

  3.3 Relation between Services and Mechanisms

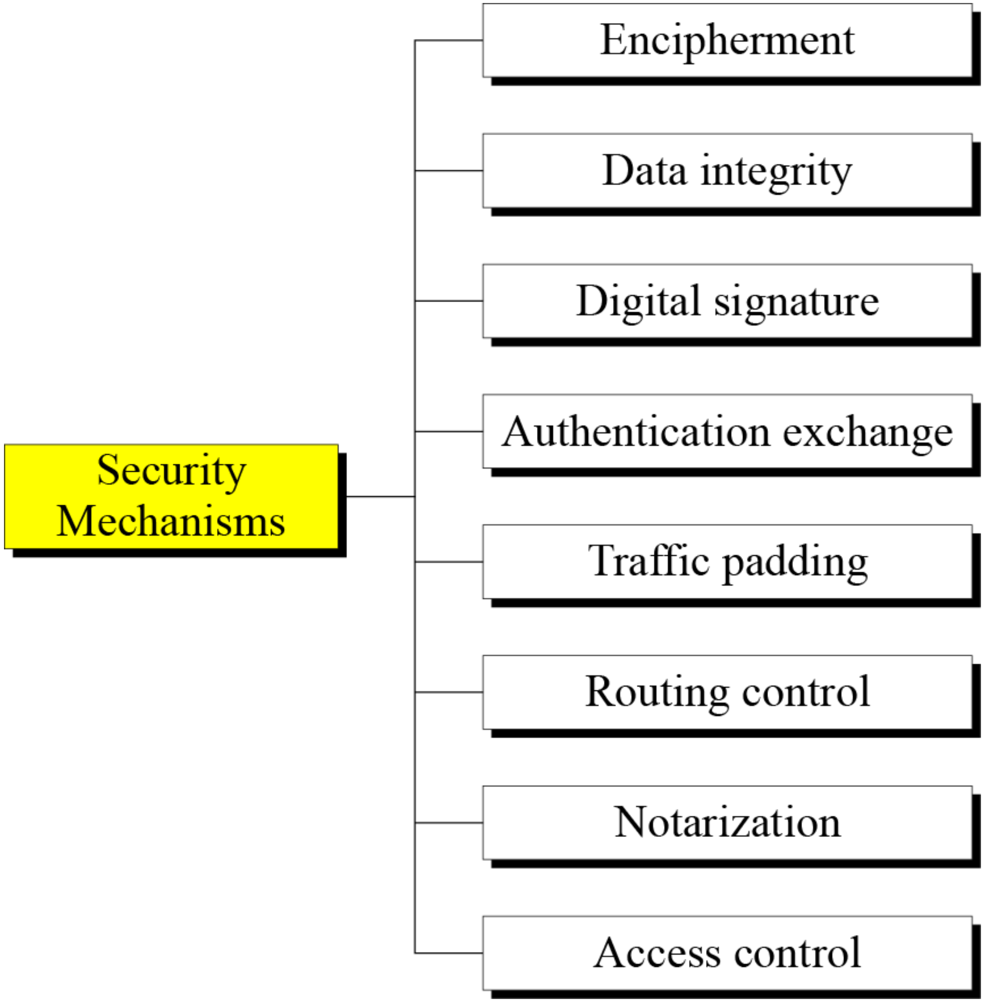
3.1 Security Services

- Figure 3.1 Security services



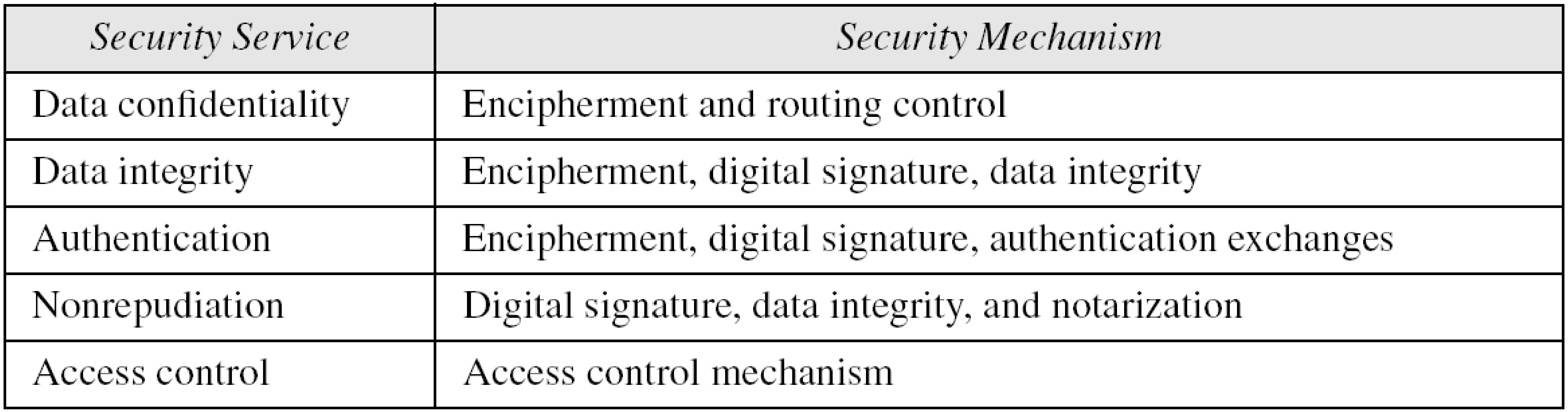
3.2: Security Mechanism

Figure 3.2 Security mechanisms



3.3: Relation between Services and Mechanisms

Table 1.1 Relation between security services and mechanisms



Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

Topic 4: TECHNIQUES

- Mechanisms discussed in the previous sections are only theoretical recipes to implement security.
- The actual implementation of security goals needs some techniques. Two techniques are prevalent today: cryptography and steganography.
- Topics discussed in this section

  4.1 Cryptography

  4.2 Steganography

Sub-Topic 4.1: Cryptography

- Cryptography, a word with Greek origins, means “secret writing.” However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.

Sub-Topic 4.2: Steganography

- The word steganography, with origin in Greek, means “covered writing,” in contrast with cryptography, which means “secret writing.”

Cryptography and Cryptology

- □ **Encryption:** transformation of intelligible, understandable information into unintelligible form to disguise its meaning and intent from intruders.

- □ **Decryption:** The inverse transformation of encrypted information into intelligible form.
- □ Both encryption and decryption are based on keys. It should be difficult or impossible to decrypt a message without knowing the key.

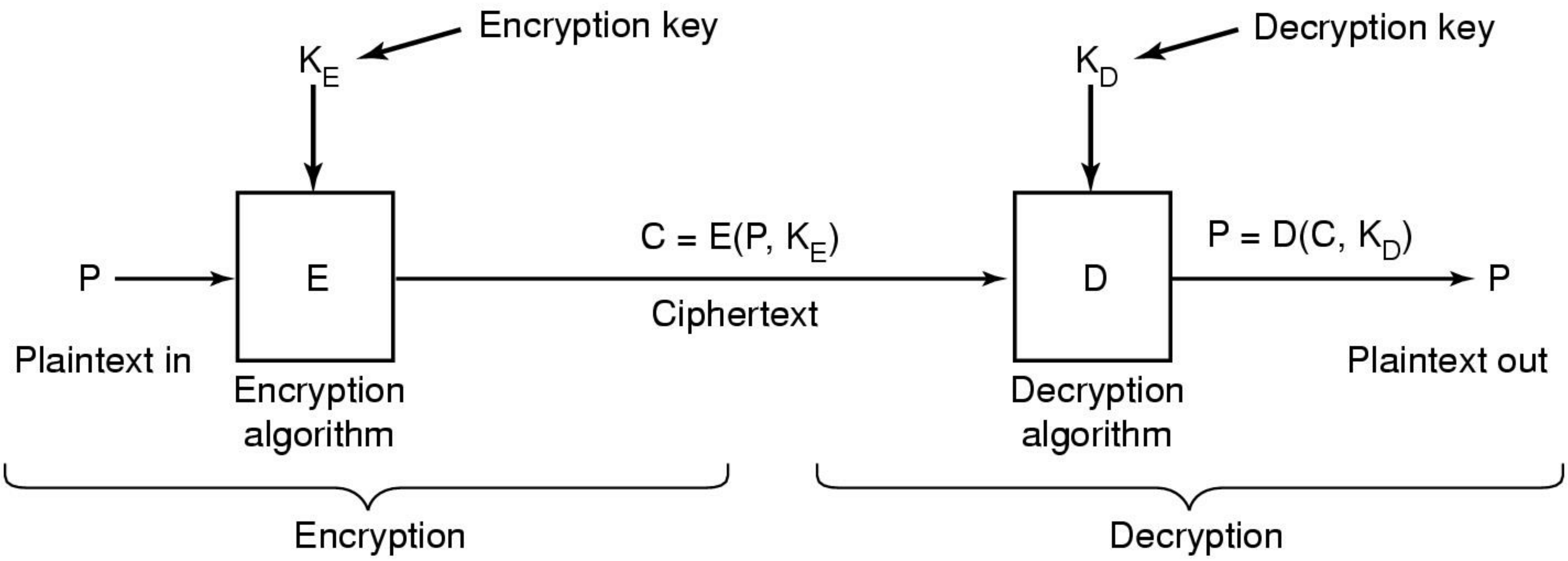
- □ **Cryptography**: A Greek word that means **"secret writing."** However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. (Study of encryption principles/methods (encryption + decryption))

- □ **Cryptanalysis (codebreaking) :** analyzing encrypted information with the intent of recovering the original plain information without knowing the key. (study of principles/ methods of deciphering ciphertext *without* knowing the key).

- □ **Cryptology:** Field of both cryptography and cryptanalysis.

The Encryption and Decryption Process

- The encryption model



The major components of a cryptosystem

- **Plain text:** the original message before encryption.
- **Encryption Algorithm:** the algorithm used to transform the plaintext into unintelligible form (the cipher text).
- **The cipher text:** the encrypted text.
- **Encryption key:** the encryption process is always based on a key.
- **Decryption Algorithm:** used to transforms cipher text back to plaintext.
- **The Decryption key:** the key used in the decryption process.

All algorithms must be public; only the keys are secret.

Intruders and Cryptanalysis

- It is assumed that there is an intruder who listens to all communications, and he may copy or delete any message
  - An active intruder modifies some messages and re-inserts them
  - A passive intruder just listens
- To decrypt a message without having a key, an intruder practices the art of cryptanalysis

What Does Cryptography Solve?

- **Confidentiality**
  - Ensure that nobody can get knowledge of what you transfer even if listening to the whole conversation
- **Integrity**
  - Ensure that the message has not been modified during the transmission
- **Authenticity**
  - You can verify that you are talking to the entity you think you are talking to
- **Identity**
  - You can verify who is the specific individual behind that entity
- **Non-repudiation**
  - The individual behind that asset cannot deny being associated with it

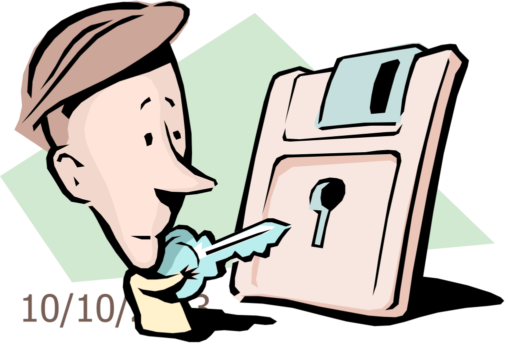
Classical Encryption Techniques

Cryptography is classified according to the number of keys used:

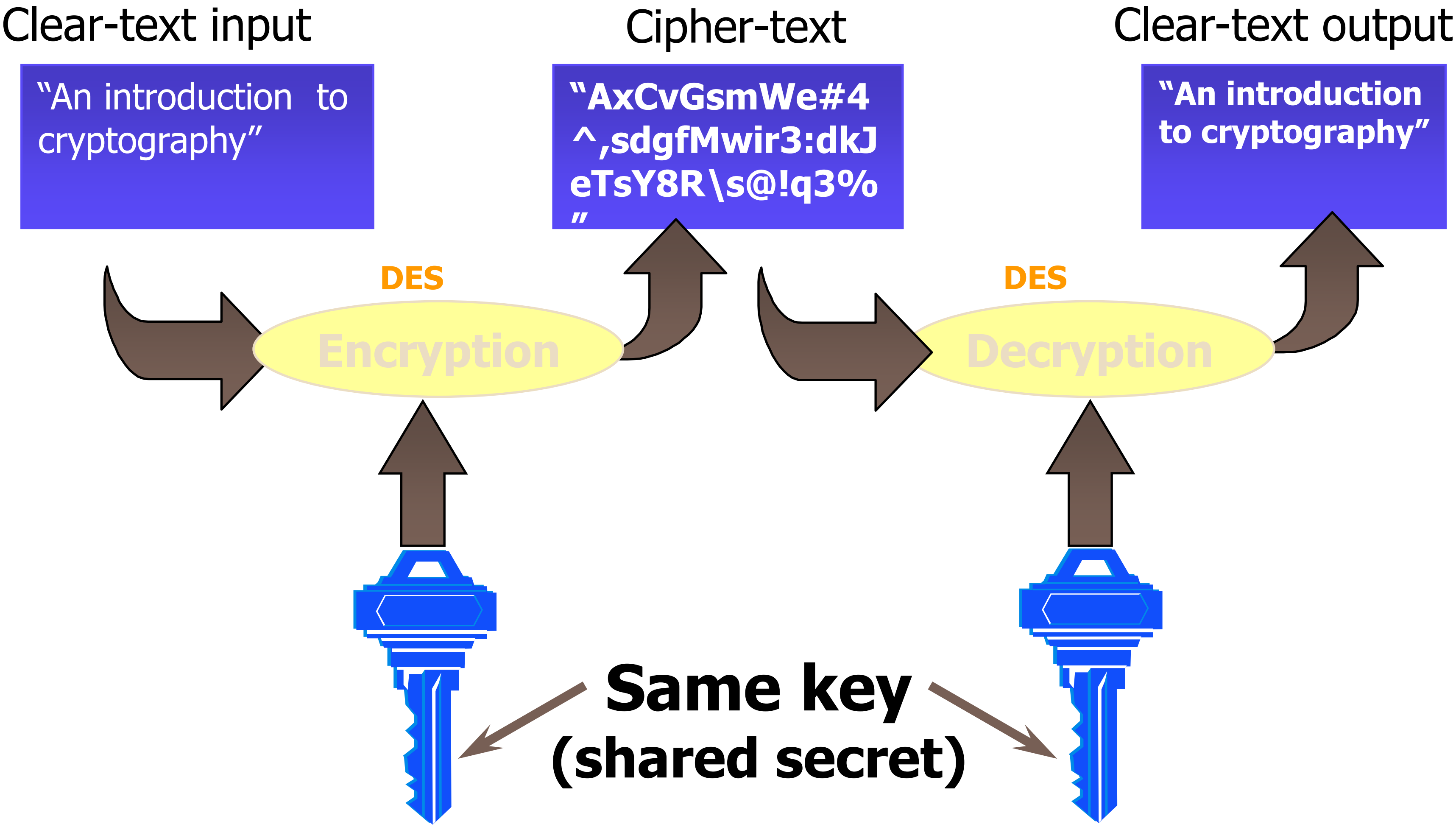
- **Symmetric key cryptography (Private-Key cryptography)**
  - The same key to encrypt and decrypt. Like DES Data Encryption Standard.
- **Asymmetric key cryptography (Public-Key Cryptography)**
  - Two mathematically related keys are used; one is the public key to encrypt, and the other is the private key to decrypt. Like RSA or Al Gamal, DSA.

Symmetric Encryption

- Also referred to as conventional encryption or single-key encryption
- Was the only type of encryption in use prior to the development of public-key encryption in the 1970s
- Remains by far the most widely used of the two types of encryption
- sender and recipient share a common key



Symmetric Encryption



Clear-text input

"An introduction to cryptography"

Cipher-text

"AxCvGsmWe#4
^,sdgfMwir3:dkJ
eTsY8R\s@!q3%
"

Clear-text output

"An introduction to cryptography"

DES

Encryption

DES

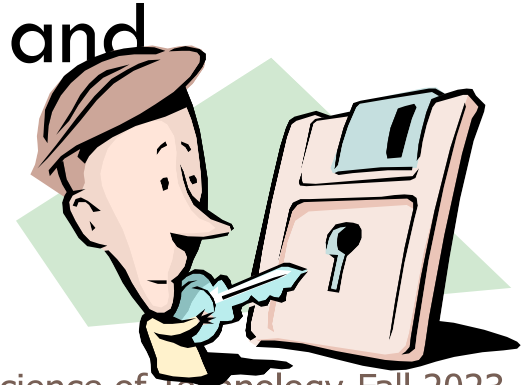
Decryption

Same key

(shared secret)

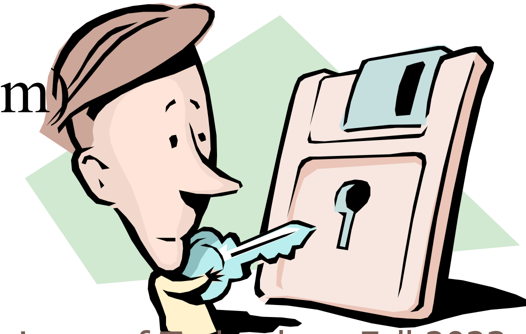
Symmetric Encryption

- In a symmetric encryption system, both the sender and receiver must possess the same key.
- The sender encrypts the message using the key and the receiver decrypts the cipher-text message using the same secret key.
- The word "symmetric" here means that the same key is used for encryption and decryption.



Examples of Symmetric Cipher

- □ DES (Data Encryption Standard)
- □ AES (Advanced Encryption Standard)
- □ Twofish
- □ Serpent
- □ Blowfish
- □ CAST5
- □ RC4
- □ Triple DES
- □ IDEA (International Data Encryption Algorithm)

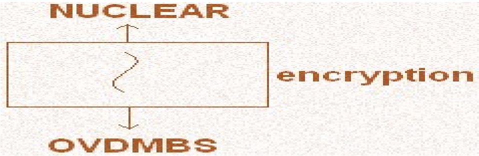


Requirements

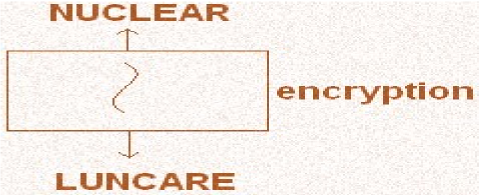
- Two requirements for secure use of symmetric encryption:
  - A strong encryption algorithm
  - A secret key known only to sender / receiver
- Mathematically have:
  - $C = \mathrm{E}_K(M)$
  - $M = \mathrm{D}_K(C)$
- Assume encryption algorithm is known
- Implies a secure channel to distribute key

Types of encryption operations used

- Substitution Cipher
  - Replace the actual bits character or block of characters with substitutes.



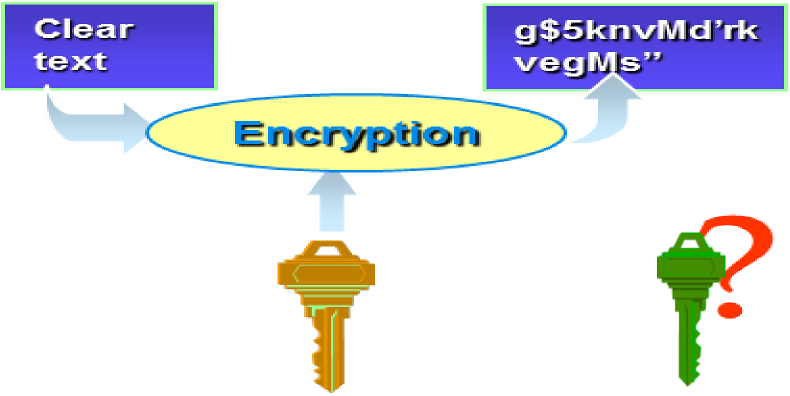
- Transposition Cipher
  - Rearrange the order of the bits characters or block of characters that are being encrypted or decrypted.



- Product Cipher
  - Combination between transposition cipher and substitution cipher.

Asymmetric Encryption

- Things to remember about asymmetric keys:
  - The relation between the two keys is unknown and from one key you cannot gain knowledge of the other, even if you have access to clear-text and cipher-text
  - The two keys are interchangeable. All algorithms make no difference between public and private key. When a key pair is generated, any of the two can be public or private



Asymmetric key cryptography characteristics

- Something encrypted with the public key can only be decrypted with the private key. (Asymmetric Encryption)
- Something encrypted with the private key can only be decrypted with the public key. (Asymmetric Digital Signature)

Asymmetric Encryption Model

- The essential steps are as follows
  - Each entity in a network generates a pair of keys (a public and a private key) to be used for encryption and decryption of messages respectively.
  - Each entity publishes its encryption key by placing it in a public domain or file. This is the public key. The private key is kept private by the owner.
  - If user A wishes to send a message to user B, then A encrypts the message by using B's public key.
  - When user B receives the encrypted message, then B decrypts it by using B's private key. No other recipient can decrypt the message because only B knows B's private key.Something encrypted with the public key can only be decrypted with the private key.

Requirements

- Encryption and decryption with the public-key cryptosystem are denoted by:

$$E_{K_{UB}}(M) = C$$

$$D_{K_{PB}}(C) = M$$

- There is some source A for a message, which generates a message in plaintext M . Along with the message M, the encryption public key for the user destination B, these will be as input parameters to perform the encryption algorithm. A produces the cipher text C. The intended receiver B, in possession of the corresponding private key K_{PB}, is able to recover the original message M by using the decryption algorithm.

Examples of Asymmetric Cipher

- There are many asymmetric cryptosystems, such as
  - RSA
  - Rabin
  - ElGamal
  - Elliptic curve cryptography

Asymmetric Digital Signature

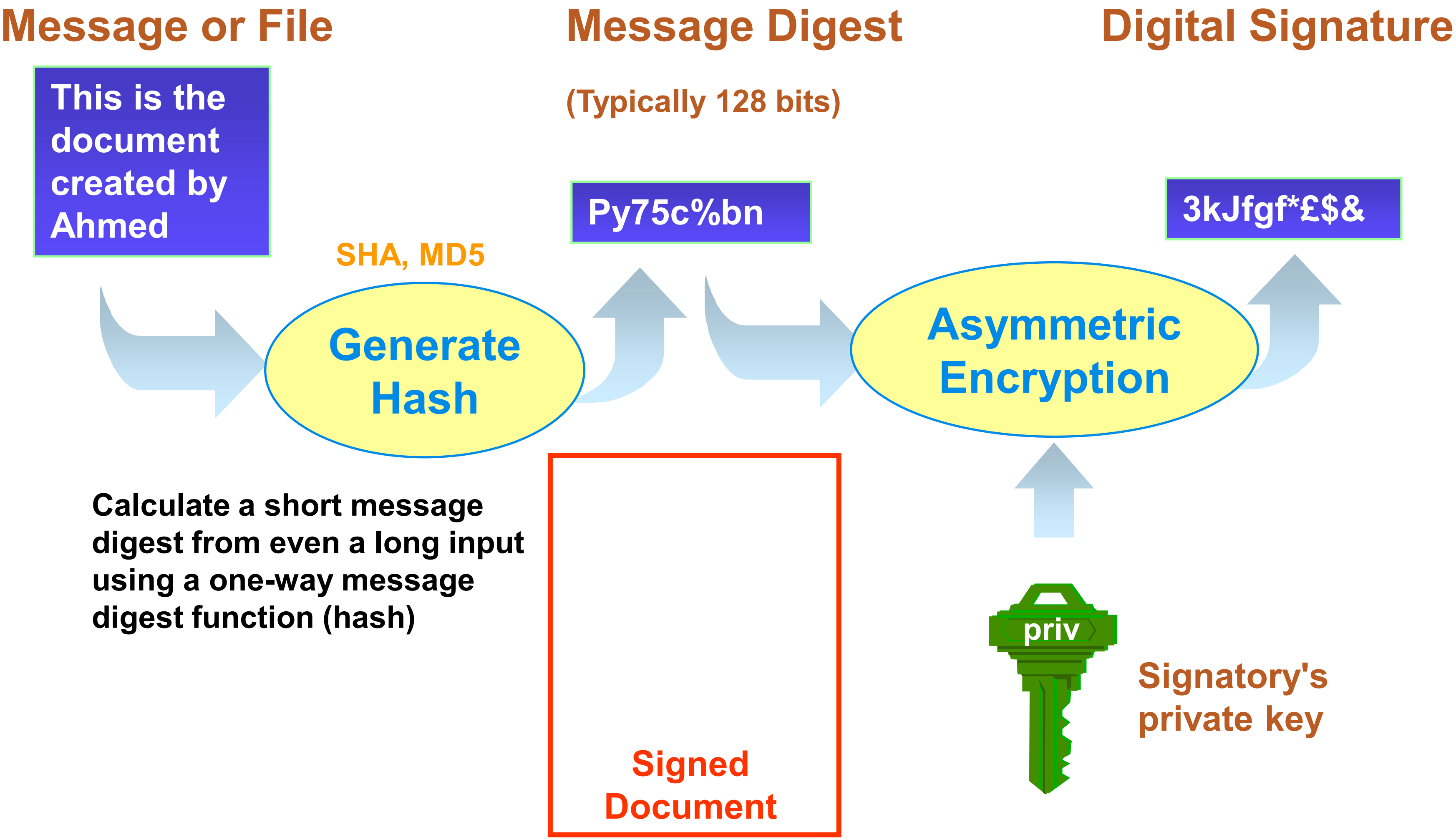
- A digital signature is “data appended to, or a cryptographic transformation of, a data unit, that allows a recipient of the data unit to prove the source, and integrity of the data unit and protect against forgery”
- Digital signatures make public key cryptography a most practical tool in real-life applications, being the most reliable method for authentication, data integrity and non-repudiation.

Asymmetric Digital Signature Model

- A digital signature depends on two fundamental assumptions:
  - first, the private key is secure and only the owner of the key has access to it,
  - and second, the only way to produce a digital signature is to use the private key.
- The first assumption has no technical answer except that keys must be protected. But the second assumption can be examined from a mathematical point of view.

K_{PB}

Creating a Digital Signature



Message or File

This is the document created by Ahmed

SHA, MD5

Generate Hash

Message Digest

(Typically 128 bits)

Py75c%bn

Asymmetric Encryption

Digital Signature

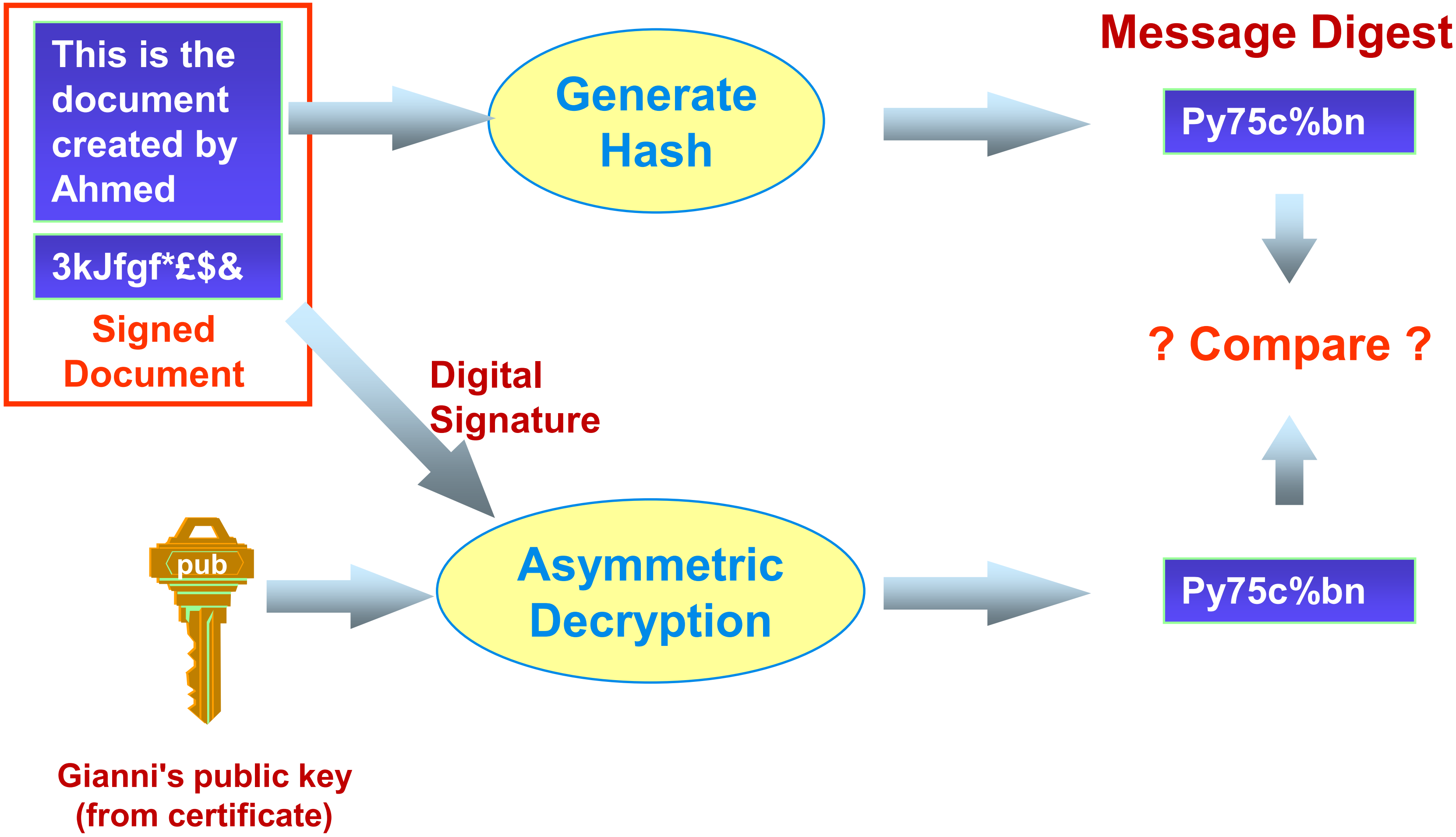
3kJfgf*£$&

Calculate a short message digest from even a long input using a one-way message digest function (hash)

Signed Document

Signatory's private key

Verifying a Digital Signature



This is the document created by Ahmed

3kJfgf*£$&

Signed Document

Generate Hash

Message Digest

Py75c%bn

? Compare ?

Digital Signature

Asymmetric Decryption

Py75c%bn

Gianni's public key (from certificate)

Properties of Digital Signature

- It must have the following properties.
  - The signature must be verifiable by third parties, to resolve disputes.
  - It must be possible to verify the author, the date and time of the signature.
  - It must be possible to authenticate the contents at the time of the signature.

Examples of Digital Signature

- Many digital signature schemes have been proposed such as
  - DSS (Digital Signature Standard)
  - ElGamal
  - RSA (Rivest-Shamir Adleman)
  - Rabin and Knapsack

Symmetric-key
vs.
Asymmetric-key cryptography

Advantages of symmetric-key

- Have high rates of data throughput .
- Keys for symmetric-key ciphers are relatively short.

Disadvantages of symmetric-key

- In a two-party communication, the key must remain secret at both ends. In order to use a secure channel, it requires prior communication of the key between sender and receiver before any ciphertext is transmitted. In practice, this may be very difficult to achieve, because there is no security channel in wireless communication systems.
- In a large network, there are many key pairs to be managed. It requires a large amount of keys. For a cryptosystem with n users, since each user has to possess n-1 keys, the required total number of keys are n(n-1)/2. Thus, when the number of users increases, the risk of revealing the secret information was drastically increased.

Advantages of Asymmetric-key

- The concept of asymmetric-key cryptography evolved from an attempt to solve two of the most difficult problems associated with conventional encryption.
  - Key distribution.
  - Many public-key schemes yield relatively efficient digital signature mechanisms
- Only the private key must be kept secret.
- Depending on the mode of usage, a private key/public key pair may remain unchanged for considerable periods of time.

Disadvantages of Asymmetric-key

- Slower than the best known symmetric-key schemes.
- Key sizes are typically much larger.