Cryptography

ACHRAF FAYAD

ECE

2018/2019

Need for Security

- **In the past, computer networks were used in universities and companies**
- **Nowadays, millions of users (ordinary) use networks for banking, shopping, paying taxes.**
- **Network security is crucial and critical**

- **Most security issues are caused by malicious people trying to:**
  - Gain some benefit
  - Get attention
  - Harm someone

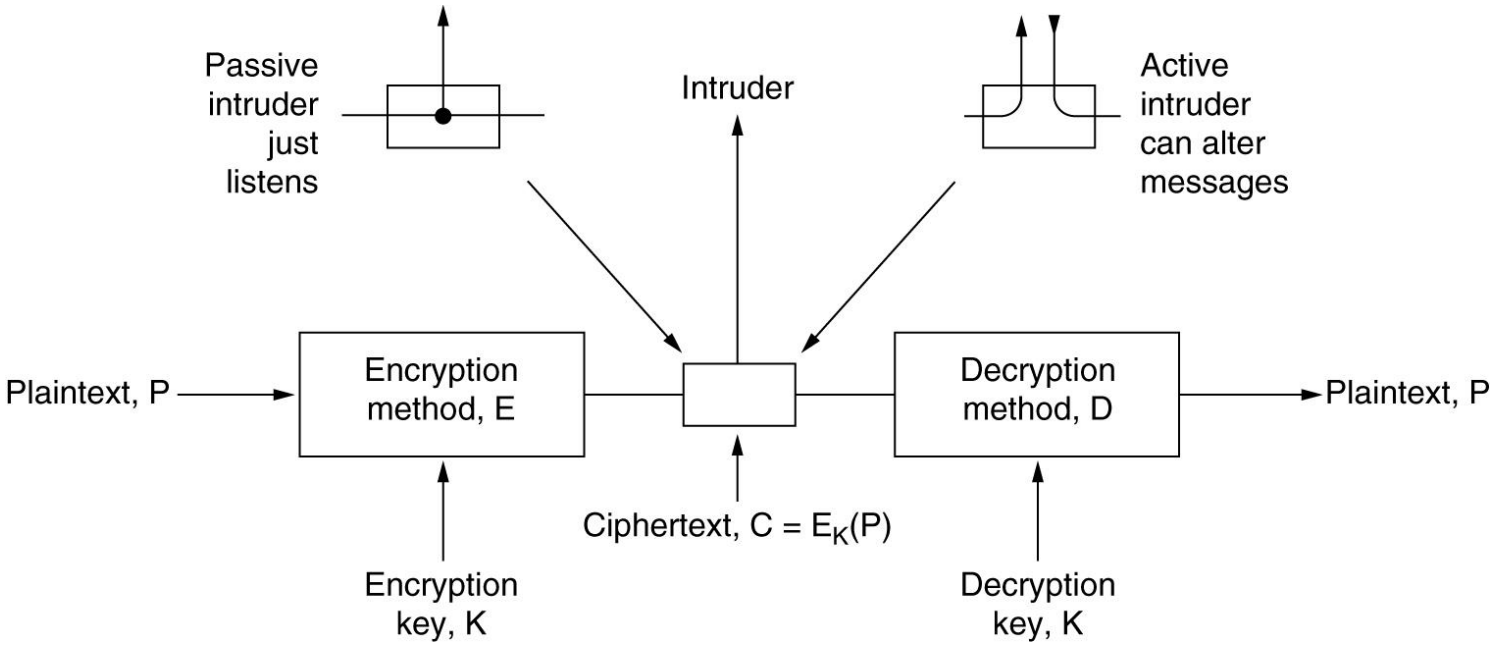
The main goals of Cryptography

- **Privacy or confidentiality**
  - It is the service used to keep the content of information secret from all but those authorized one to have it. There are number of approaches to providing confidentiality, cryptography deals with protection through mathematical algorithms which render data unintelligible.
- **Data Integrity**
  - It refers to the unauthorized manipulation of data.
- **Authentication**
  - It is a service related to identification. This function applies to both entity authentication and data origin authentication.
- **Non-repudiation:**
  - It is a service which prevents an entity from denying previous commitments or action.

Introduction to Cryptography

- **Cryptography** *comes from Greek <KRYPTOS> secret writing*
- **Cipher** *is a character for character or bit for bit transformation without regard to the linguistic structure of the message*
- **Code** *replaces one word by another word*
- **Codes are not used any more**
- **Code Example:**
  - USA army kept Navajo Indians speaking to each other using Navajo words in World War II.
  - Japanese could never break the code during 3 years of war in the pacific ocean. The language is highly tonal and not written.

Introduction to Cryptography



Introduction to Cryptography

- **The length of the key is a major design issue.**
- **A key length of 2 digits means that there are 100 possibilities, 6 digits however means million possibilities and so on.**
- **The work factor for breaking a the system by exhaustive search of the key space is exponential with respect to key length.**
- **Finally, the key length is also dependent of the application.**
- **If a 128 bit key is sufficient for a routine commercial use, more than 256 bit keys are needed to protect governmental information across networks.**

Substitution Ciphers

- **Each letter or group of letters is replaced by another letter or group of letters:**

Caesar cipher

- **It is the oldest known cipher (attributed to Julius Caesar).**
- **a becomes D, b becomes E.**
- **Example: attack → DWWDFN**

- **Caesar cipher generalization**
  - **Each alphabet letter is shifted by k (the key)**

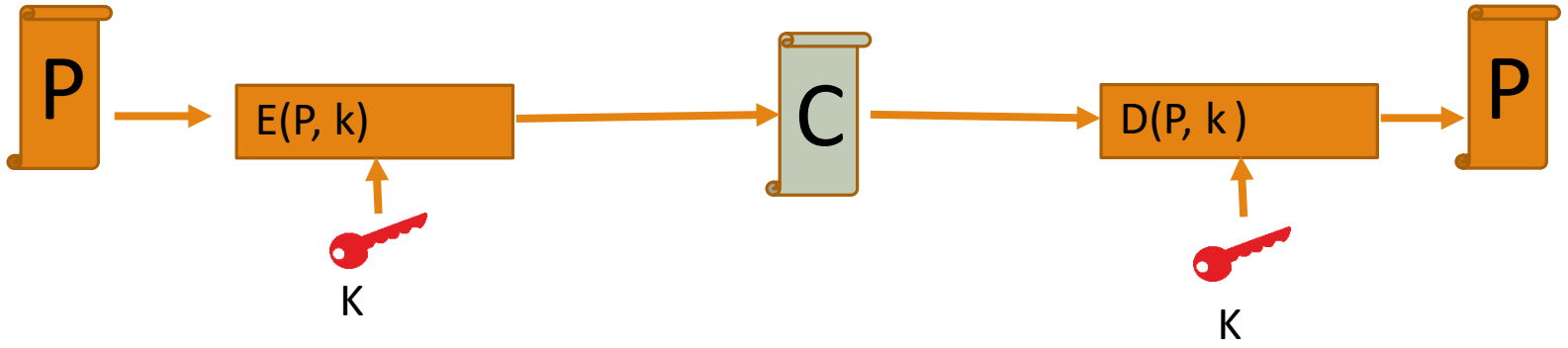
Symmetric Key Algorithms

- **Modern cryptography uses same basic ideas as traditional cryptography (transposition and substitution).**
- **The emphasis, however, is different.**
- **The basic objective is to render the public encrypting algorithm as complex as possible.**
- **In this case, even with a big amount of enciphered text, it shall not be possible for the cryptanalyst to break the text without knowing the key.**

- **Cryptographic algorithms can be implemented in hardware (for speed) or software (for flexibility)**

Symmetric Key Algorithms

- **The use the same key for encryption and decryption.**
- **Block ciphers are mainly used. They take n-bit blocks of plain text and transform them into n-bit blocks of ciphertext.**



Symmetric Key Algorithms

- **DES (Data Encryption Standard)**
  - **Initially IBM planned to use 128 bits. It was reduced to 56 bits and the DES design was kept secret.**
  - **It was widely used.**
  - **Nowadays it is not considered secure anymore.**
  - **The plaintext is encrypted as blocks of 64 bits. Each block outputs a 64 bit cipher.**
  - **Length key 56 bits.**
- **Triple DES (3DES)**
  - **The solution proposed by IBM**
  - **Length key 112 bit key**
- **AES stands 'The Advanced Encryption Standard'**
  - **Fully public design**
  - **Key lengths: 128, 192, 256**
  - **It shall be public or licensed on non-discriminatory terms.**

.

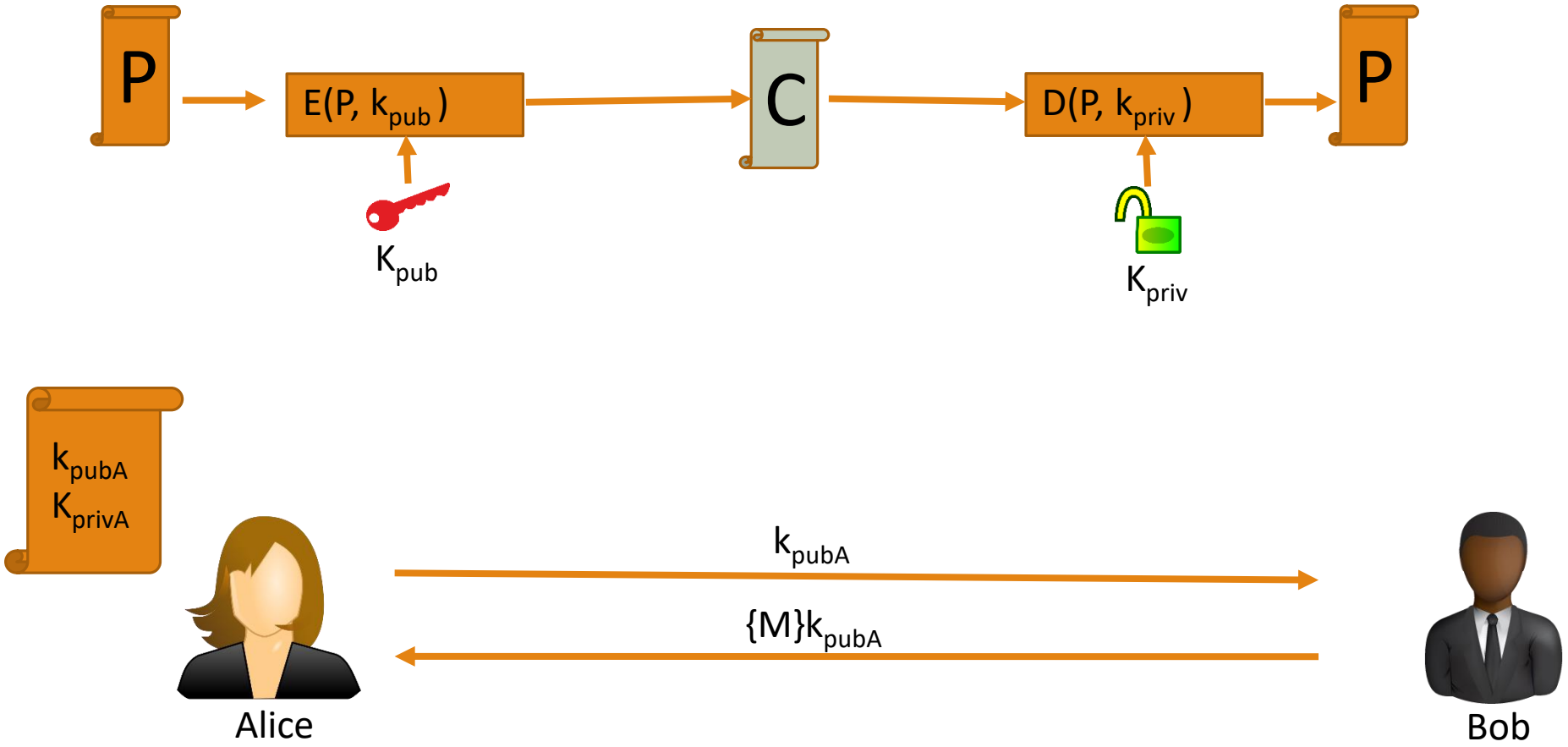
.

.

Public Key Algorithms
Asymmetric Key Algorithms

- **There are several shortcomings associated with symmetric-key schemes**
  - **Distributing the key was historically the weakest part in most cryptosystems (mainly in symmetric key algorithms) .**
    - **The key must be established using a secure channel.**
  - **If the key was stolen, every thing goes down.**
  - **Keys have to be protected from thieves but shall be also distributed.**
- **In public key algorithms, the encryption method and key are published (on a webpage for instance). The decryption key is kept secret.**
- **Main Security Mechanisms of Public-Key Algorithms:**
  - **Key Establishment**
  - **Nonrepudiation**
  - **Identification**
  - **Encryption**

Public Key Algorithms



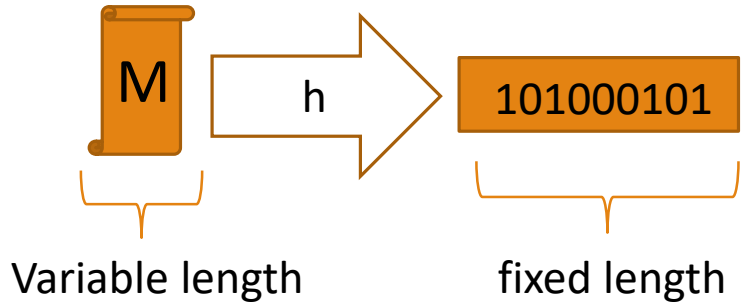
Public Key Algorithms

- **RSA: Rivest, Shamir, Adleman**
  - **This makes it slow with respect to 128 bit symmetric key algorithms.**
  - **Disadvantage: needs a 1024 bit for good security.**
  - **Used for digital signature.**
  - **Used for symmetric key exchange,**
- **DH (Diffie-Hellman)**
  - **Used for symmetric key exchange**
- **Elliptic Curve**
  - **Shorter keys are as strong as long key for RSA**
  - **Low on CPU consumption.**
  - **Low on memory usage.**

……

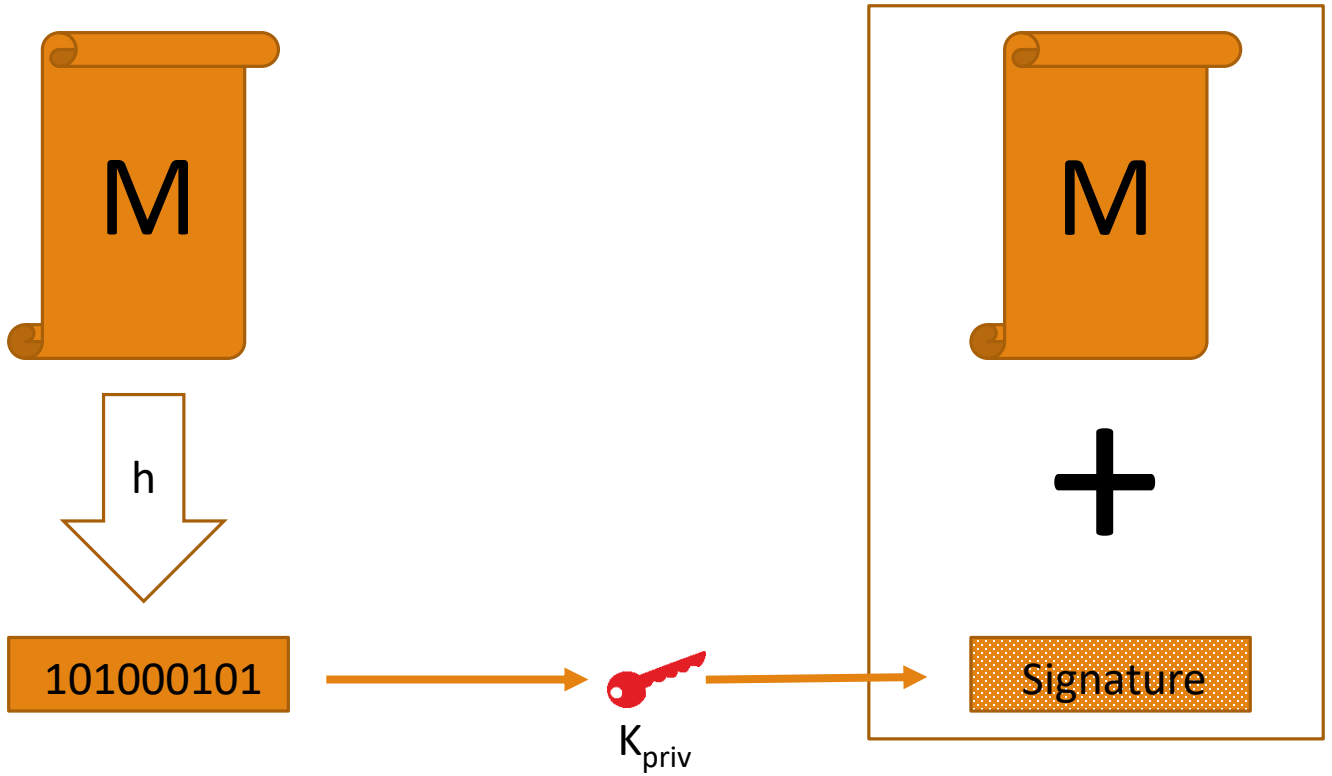
Hash function

- **A cryptographic hash function, is a function which takes arbitrary length bit strings as input and produces a fixed length bit string as output, the output is often called a hashcode or hash value.**
- **A hash function which has the one-way property is that it is preimage resistant.**
- **hash function needs to satisfy the following three properties**
  - Given M, it is easy to compute h(M).
  - Given h(M), it is impossible to find M
  - Given M, it is not possible to find M' such that h(P)=h(P')
  - Changing one bit in the input produces a very different output.d
  - **Message Digest :**
    - **MD4 et MD5 (output bitlength of 128 bits).**
  - **Secure Hash Algorithm (SHA)**
    - **SHA-1: (output bitlength of 160 bits)**
    - **SHA-256 : (output bitlength of 256 bits)**
    - **SHA-512: (output bitlength of 512 bits)**

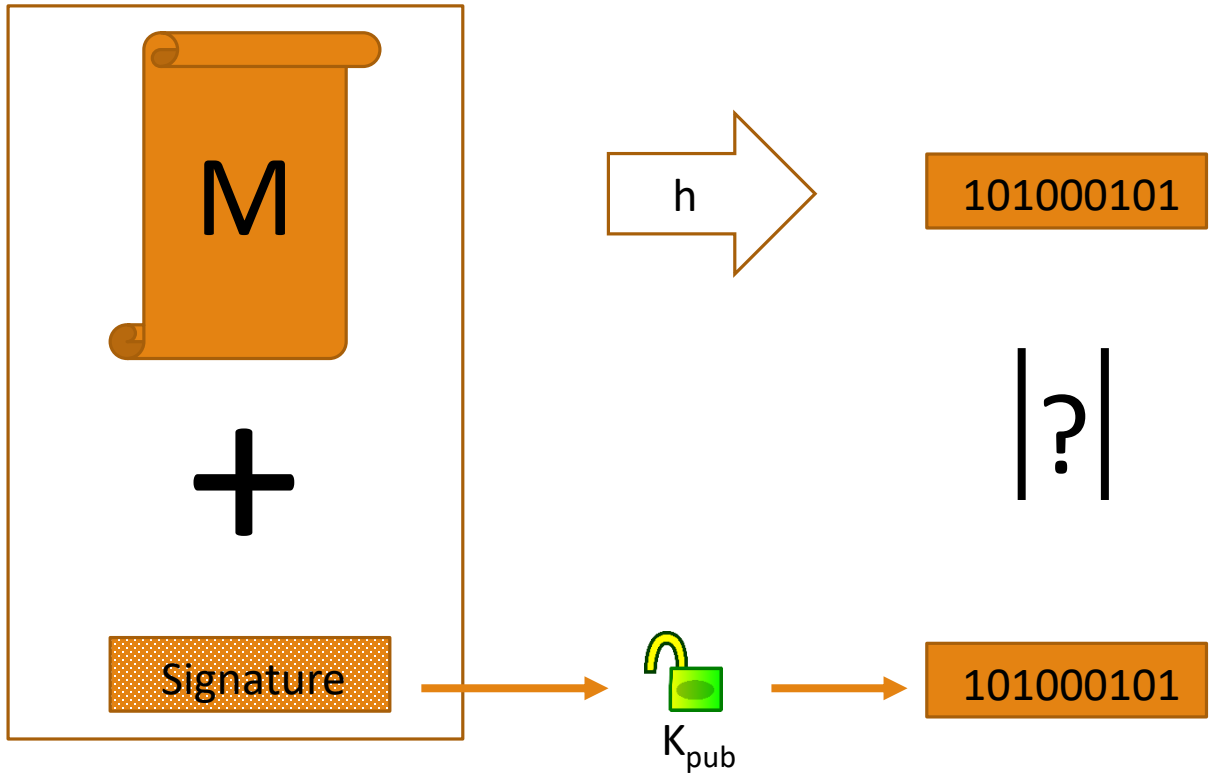


Digital Signatures / signing

- We can use digital signatures to:
  - Control access to data
  - Allow users to authenticate themselves to a system,
  - Allow users to authenticate data,
  - Sign ‘real’ documents.



Digital Signatures / Verification



References

[1] Cryptography: An Introduction (3rd Edition) : Nigel Smart

[2] Understanding Cryptography : Christof Paar · Jan Pelzl