İTÜ
Computer Security

Basic Cryptography

Dr. Şerif Bahtiyar

bahtiyars@itu.edu.tr

Fall 2015

Before Starting

Apple's App Store infected with XcodeGhost malware in China

http://www.bbc.com/news/technology-34311203

Outline

- Basic concepts
- Symmetric-key cryptography
- Public-key cryptography
- Key management
- Random numbers

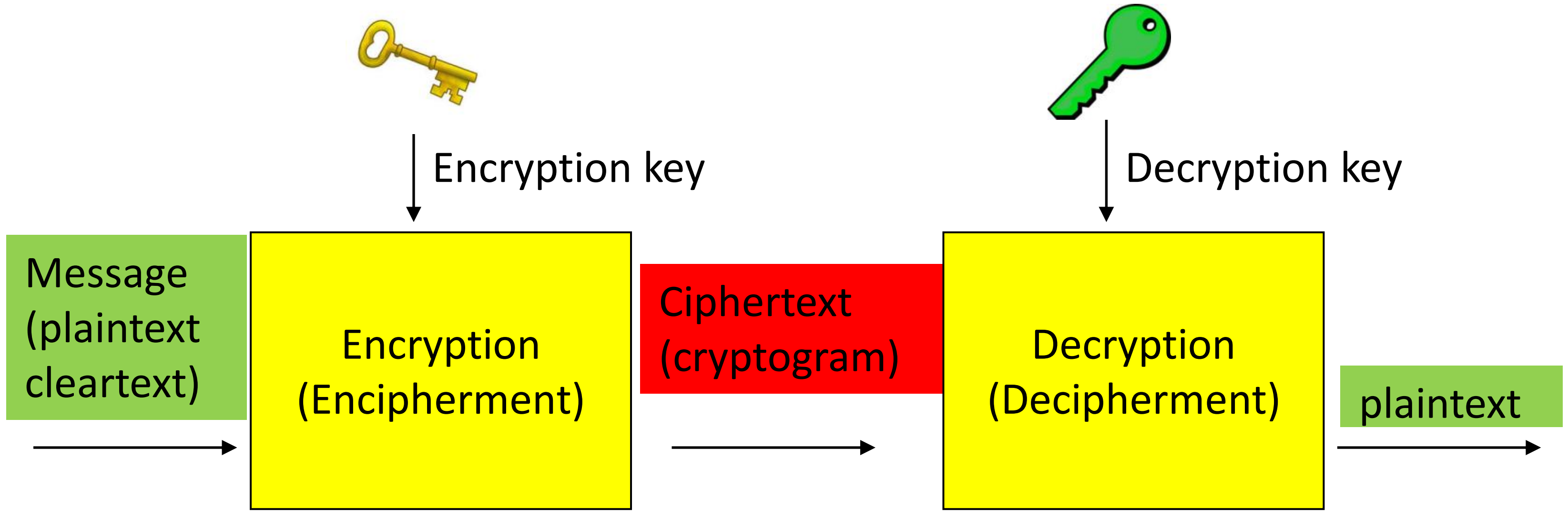
Basic concepts

Cryptography

- Crypto: secret, hidden
- Graph: writing or study
- Cryptography is a study of secret writing to ensure secure systems in the presence of adversaries.

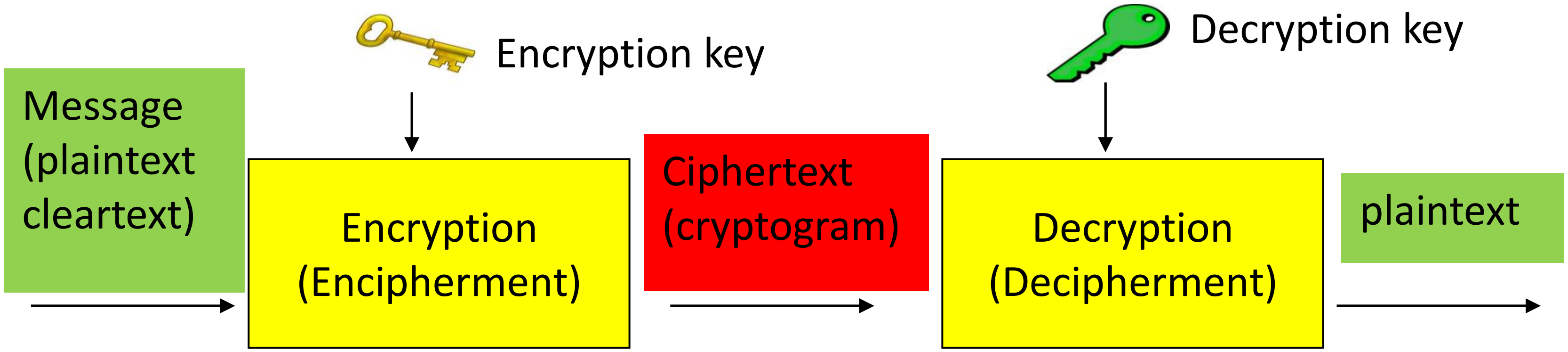
Basic concepts

Basic scenario



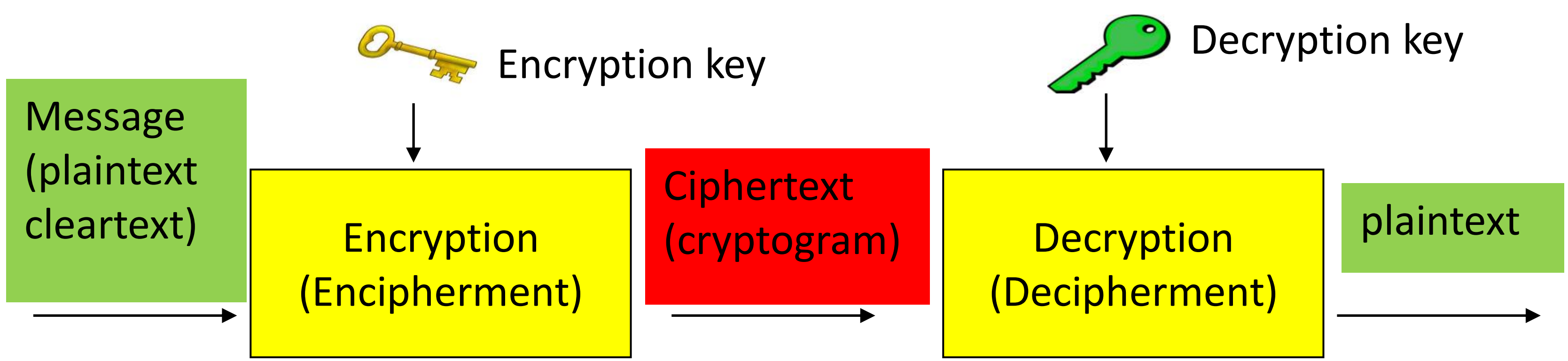
Basic concepts

- Plaintext: the original message
- Ciphertext: the scrambled message
- Encrypt: converting plaintext to ciphertext
- Cipher: algorithm for transforming plaintext to ciphertex



Basic concepts

- Decrypt: recovering plaintext from ciphertext
- Key: information used in cipher known only to sender/receiver
- Cryptanalysis: The process of attempting to discover the plaintext or key
- Cryptology: The areas of cryptography + cryptanalysis



Basic concepts

Classification of Cryptographic Systems

Type of Operations (Symmetric-key cryptography)

- It is used for transforming plaintext to ciphertext.
- Substitution (S) (bit, letter, or group of bits or letters)

  İTÜ -> 439 (İ->4, T->3, Ü->9)
- Transpositions (T)

  İTÜ->TÜİ (123 -> 231)
- Product: multiple stages of substitutions and transpositions

  STSST
- Requirement: no information be lost!

Basic concepts

Classification of Cryptographic Systems

The Number of Keys Used

- Sender and receiver use the same key (symmetric, single-key, conventional encryption)


- Sender and receiver use different keys (asymmetric, two-key, public-key encryption)


Basic concepts

Classification of Cryptographic Systems

The way in which the plaintext is processed.

- Block cipher

Istanbul -> qwertyuo

- Stream cipher

Istanbul -> qstanbul

Istanbul -> qwanbul

.

.

Istanbul -> qwertyuo

Basic concepts

An encryption scheme is computationally secure if :

- The cost of breaking the cipher exceeds the value of the encrypted information.
- The time required to break the cipher exceeds the useful lifetime of the information.

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

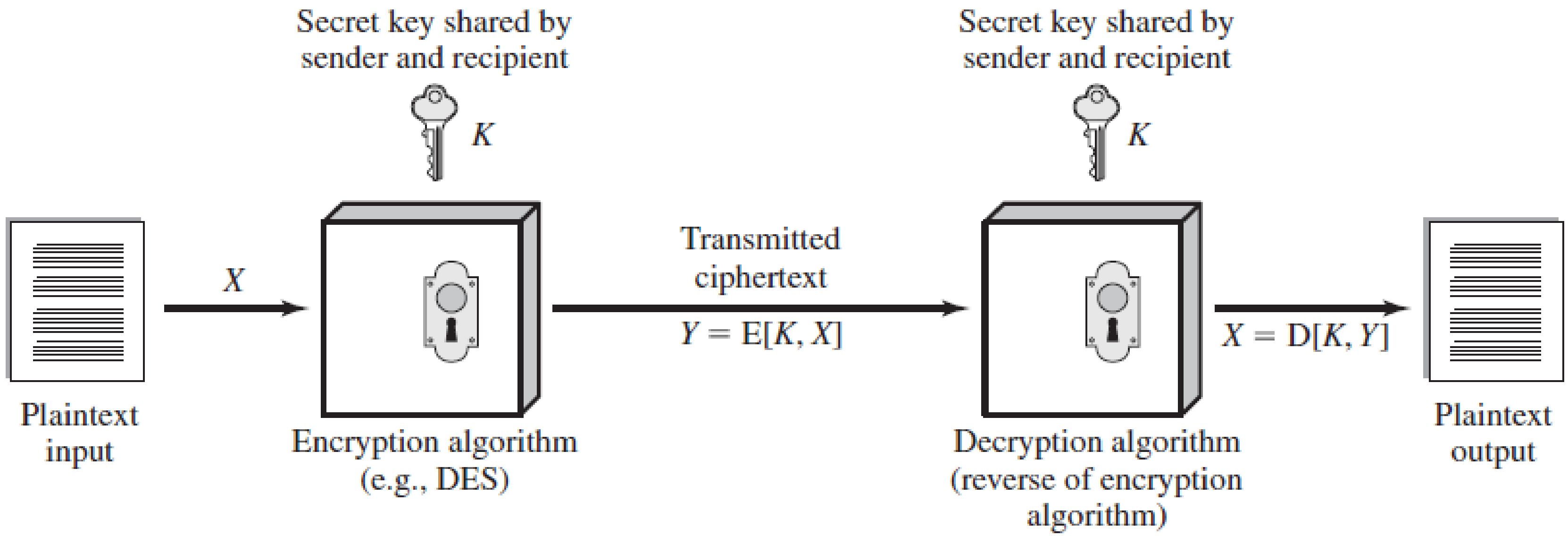
Basic concepts

Unconditionally Secure Algorithm

- Only One-Time Pad (OTP) algorithm is unconditionally secure
  - key is random and as long as the plaintext
  - key is not re-used
- Problems of OTP in practice
  - large amount of random number generation
  - protection and safe distribution of those keys

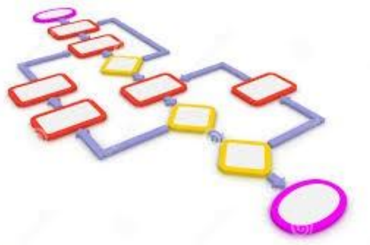
Symmetric-key cryptography

- Sender and receiver share the same key (secret key)
- Known as Conventional or Single-key or Classical
- It was only type prior to invention of public-key cryptography.



Symmetric-key cryptography

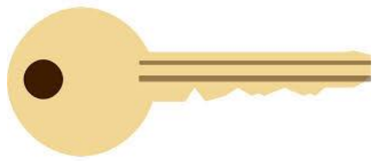
There are two requirements for secure use of symmetric encryption:



- Strong encryption algorithm

  The opponent should be unable to decrypt ciphertext or discover the key even with ciphertexts together with the plaintext.

- Secure Key Distribution: Sender and receiver must have obtained copies of secret key in a secure fashion and must keep the key secure



Symmetric-key cryptography

- Generally, it is assumed that opponent
  - Knows encryption algorithm
  - Does not know keys

- This implies that a secure channel to distribute keys is needed.
- Notation

$$Y = \mathrm{E}_K(X) \text{ or } \mathrm{E}(K, X)$$

$$X = \mathrm{D}_K(Y) \text{ or } \mathrm{D}(K, Y)$$

Symmetric-key cryptography

Approaches to attacking symmetric encryption scheme:

- Cryptanalysis relay on
  - the nature of the algorithm
  - some knowledge of the general characteristics of the plaintext or plaintext-ciphertext pairs

Symmetric-key cryptography

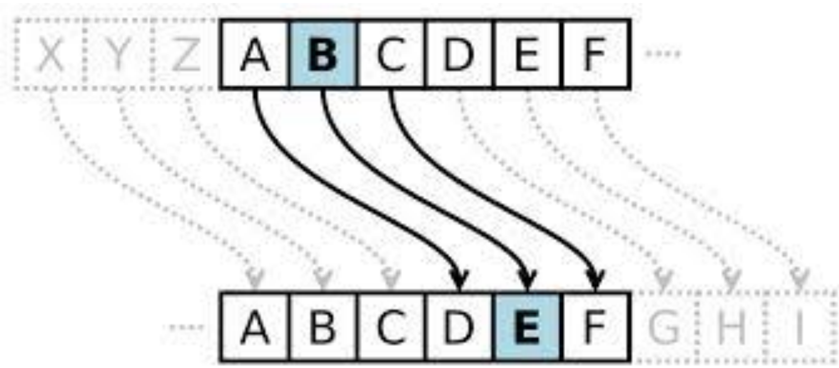
Approaches to attacking symmetric encryption scheme:

- Brute-force attack: try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

Symmetric-key cryptography

Earliest known is Caesar's cipher

- Replace each letter by the one with 3 letters down in the alphabet
- a becomes d, b becomes e, …, y becomes b, z becomes c



- no key
- Uses substitution

Symmetric-key cryptography

Rotor machines

- Basic idea: multiple stages of substitutions
- Widely used in WW2
  - German (Enigma), Japan (Purple)
- Implemented as a series of cylinders that move after each letter is encrypted
  - each cylinder represents a substitution alphabet
- 3 cylinders = 26*26*26 = 17576 different substitution alphabets
  - This number is even bigger for 4 and 5 cylinders

Symmetric-key cryptography

Rotor machines

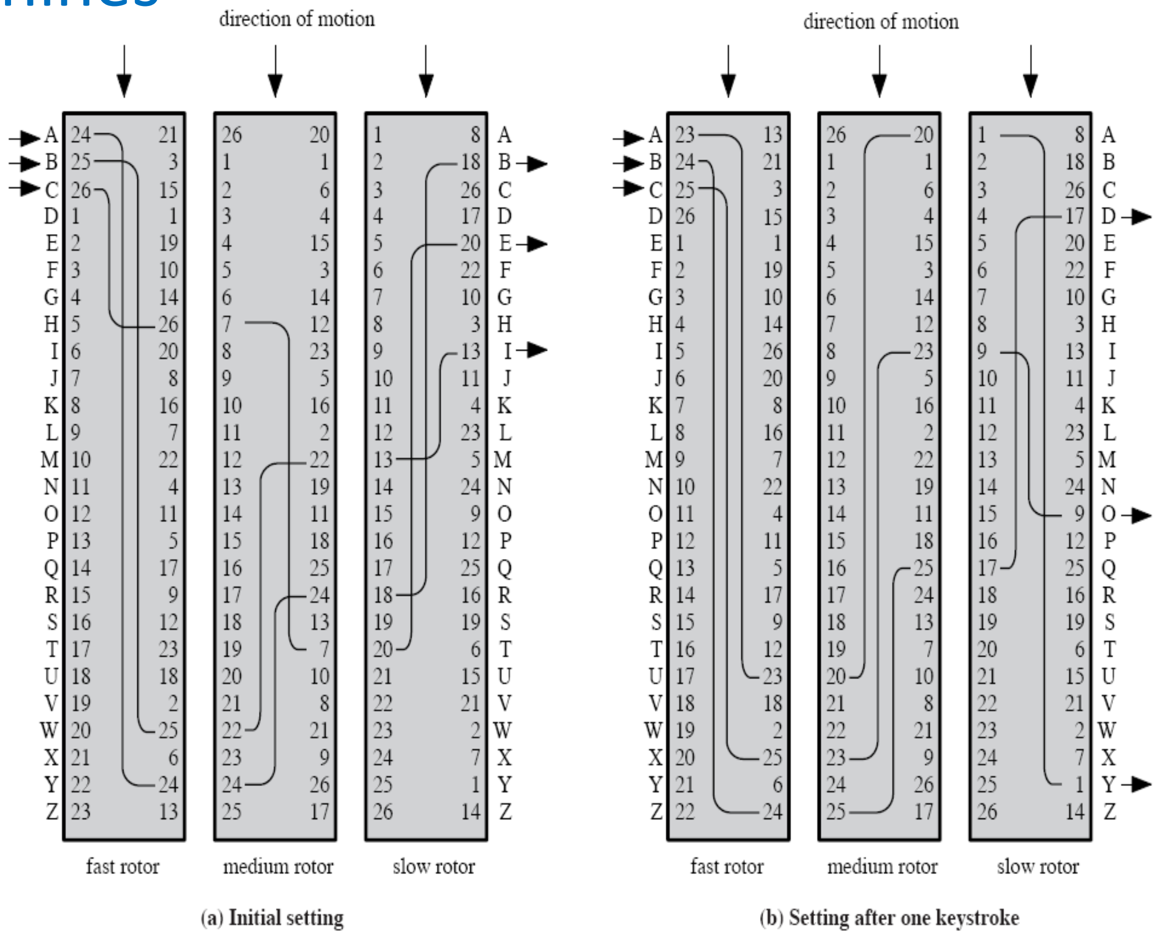


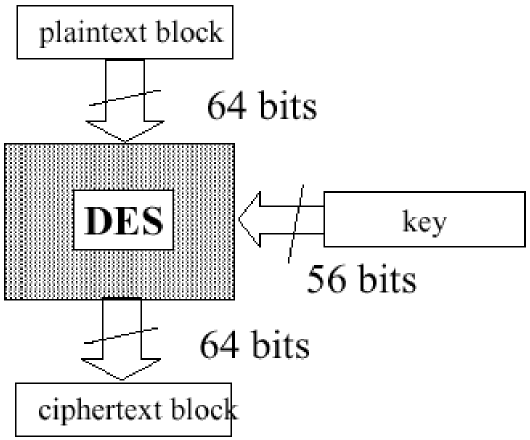
Figure 2.7 Three-Rotor Machine With Wiring Represented by Numbered Contacts

Symmetric-key cryptography

- Modern symmetric encryption systems use block or stream ciphers.
- Block ciphers operate on a block of data (file transfer, e-mail, database,…)
  - Limitation: Entire block must be available before processing
  - Advantage: Reuse of keys
  - DES, 3DES, AES
- Stream ciphers process messages one bit or byte at a time (browser,…)
  - Limitation: Pseudorandom stream generator
  - Advantage: Almost always faster and use far less code than do block ciphers. Need not wait the entire block.
  - RC4

Symmetric-key cryptography

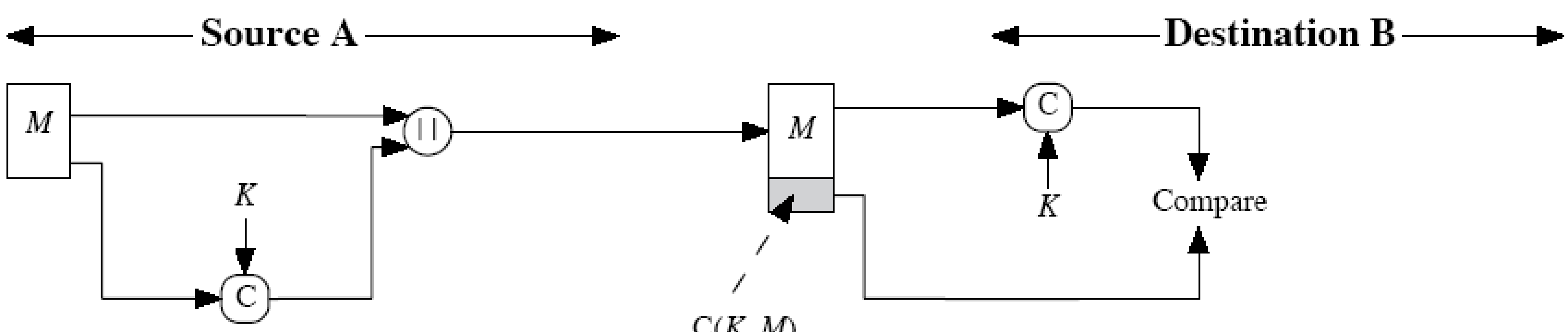
DES (Data Encryption Standard)



- Most widely used block cipher in world
- Adopted in 1977 by NIST
- Encrypts 64-bit data using 56-bit key
- Has widespread use
- Considerable controversy over its security
- DES is basically a product cipher
  - several rounds of substitutions and permutations
  - actually not that simple
- Originally designed for hardware implementation
  - software implementations validated in 1993
  - but software DES is slow

Symmetric-key cryptography

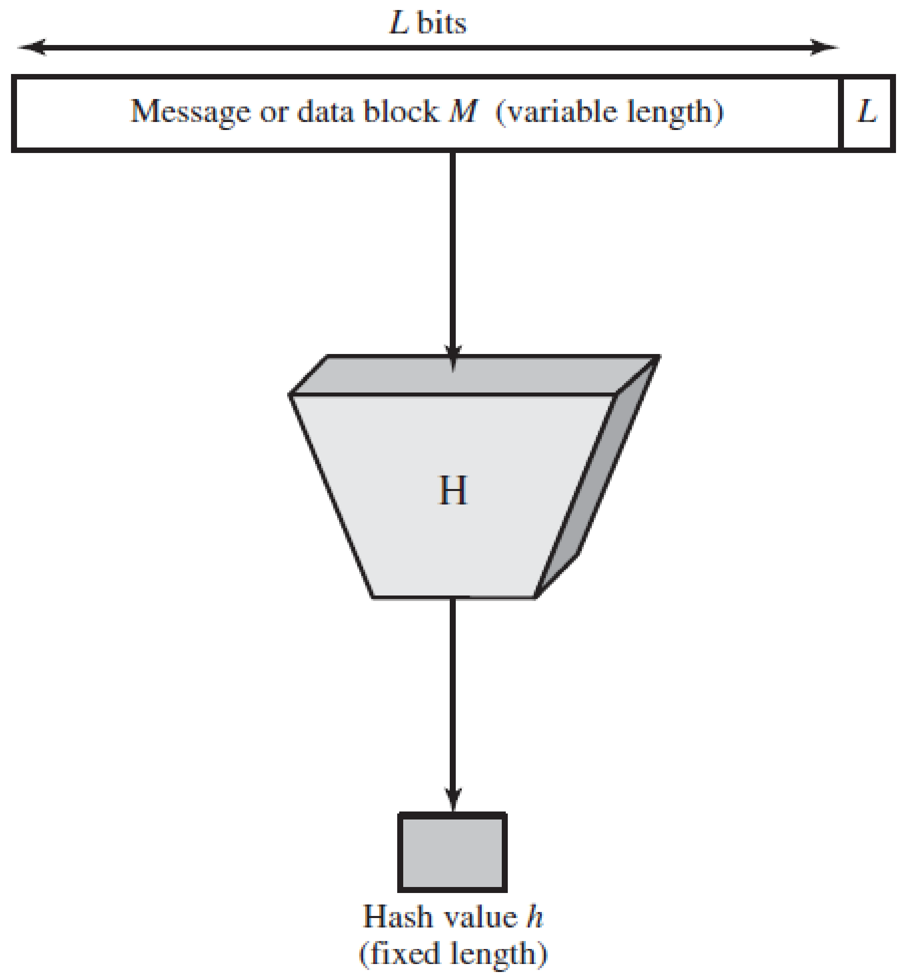
- Message authentication: It is the procedure that allows parties to verify that received or stored messages are authentic.
- The authentication algorithm need not be reversible.
- Message authentication code (MAC) uses a secret key to generate a small fixed-size block of data.
- Is MAC a signature?
  – No, because the receiver can also generate it



(a) Message authentication

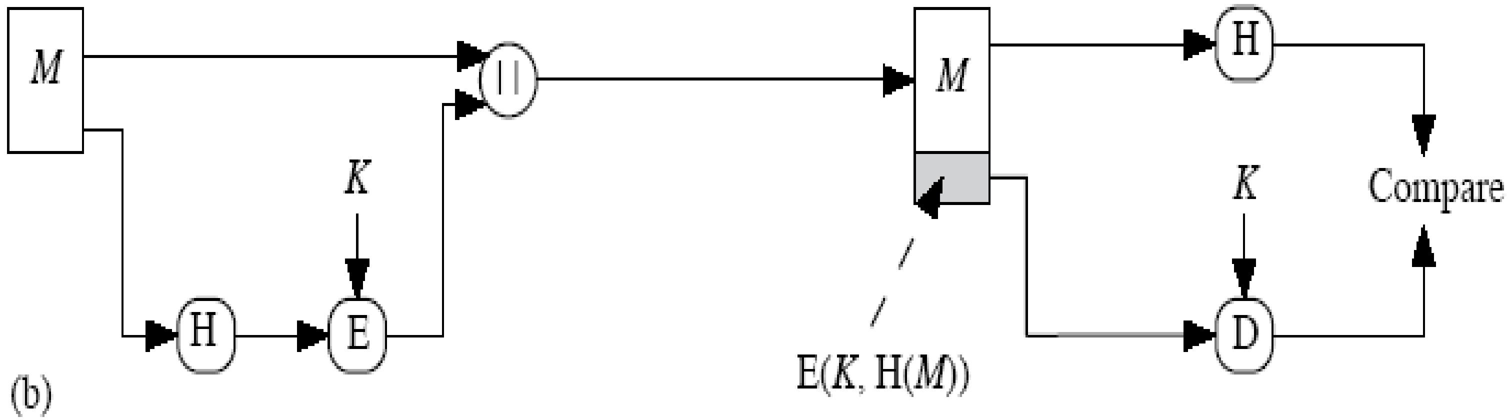
Symmetric-key cryptography

A hash function accepts a variable size message M as input and produces a fixed size message digest as output H(M).



Symmetric-key cryptography

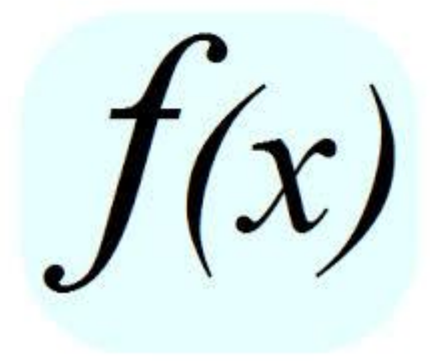
- Unlike MAC, a hush function does not take a secret key as input.
- We can use hash functions within authentication and digital signatures
  - with or without confidentiality

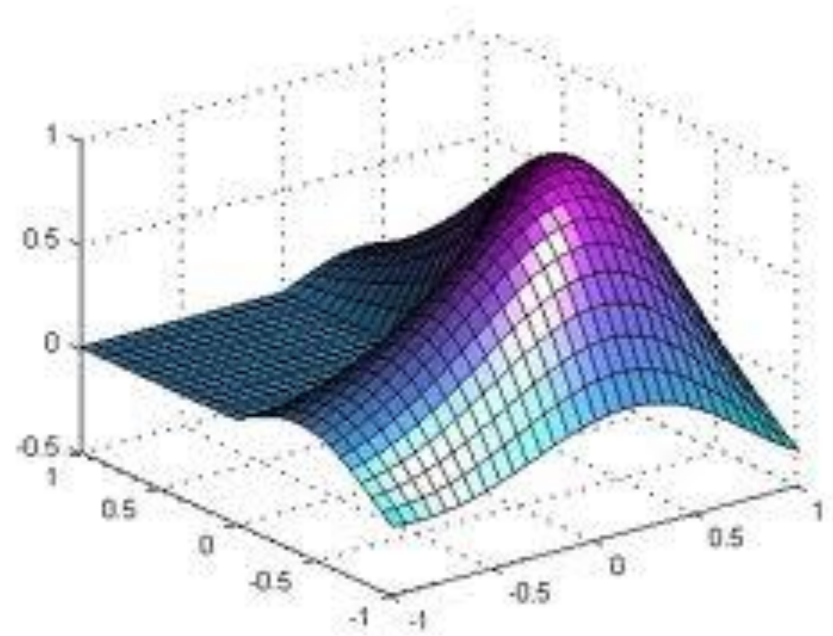


Hash without confidentiality

Public-key cryptography

Public-key algorithms are based on mathematical functions rather than on simple operations on bit patterns.





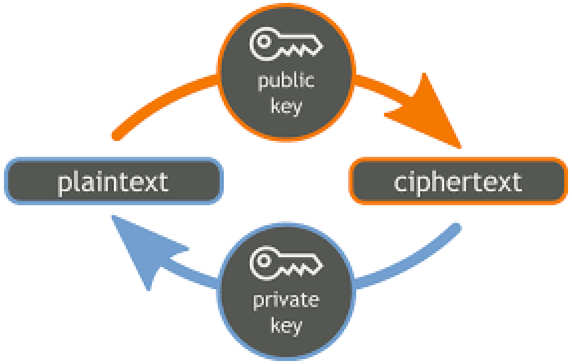
Public-key cryptography

- Public-key cryptography is invented by Whitfield Diffie and Martin Hellman in 1976
- NSA says that they knew public-key cryptography back in 60's
- First documented introduction of public-key cryptography is by James Ellis of UK's Communications-Electronics Security Group in 1970
- RSA: Block cipher in which the plaintext are integers beetween *0* and *n-1* for some *n*.

Public-key cryptography

There are 2 keys in public-key cryptography

- Public-key: may be known by anybody, and can be used to encrypt messages, and verify signatures
- Private-key: known only to the owner, used to decrypt messages, and sign (create) signatures

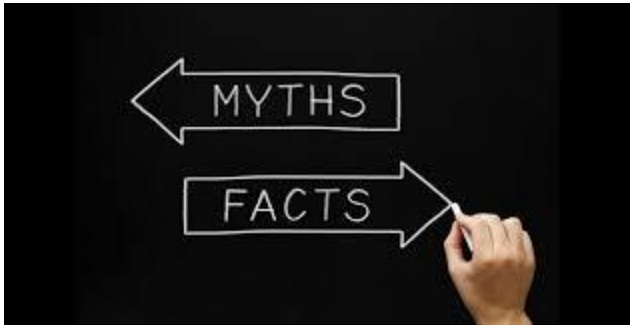


- Keys are related to each other but it is not feasible to find out private key from the public one

Public-key cryptography

Some misconceptions

- Public-key cryptography replaces symmetric cryptography
- Public-key cryptography is more secure (no evidence for that, security mostly depends on the key size in both schemes)
- Key distribution is trivial in public-key cryptography since public keys are public (key distribution is easier, but not trivial)



Public-key cryptography

Public-key cryptography initially developed to address two key issues:

- Key distribution
  - Symmetric crypto requires a trusted Key Distribution Center (KDC)
  - In PKC you do not need a KDC to distribute secret keys, but you still need trusted third parties

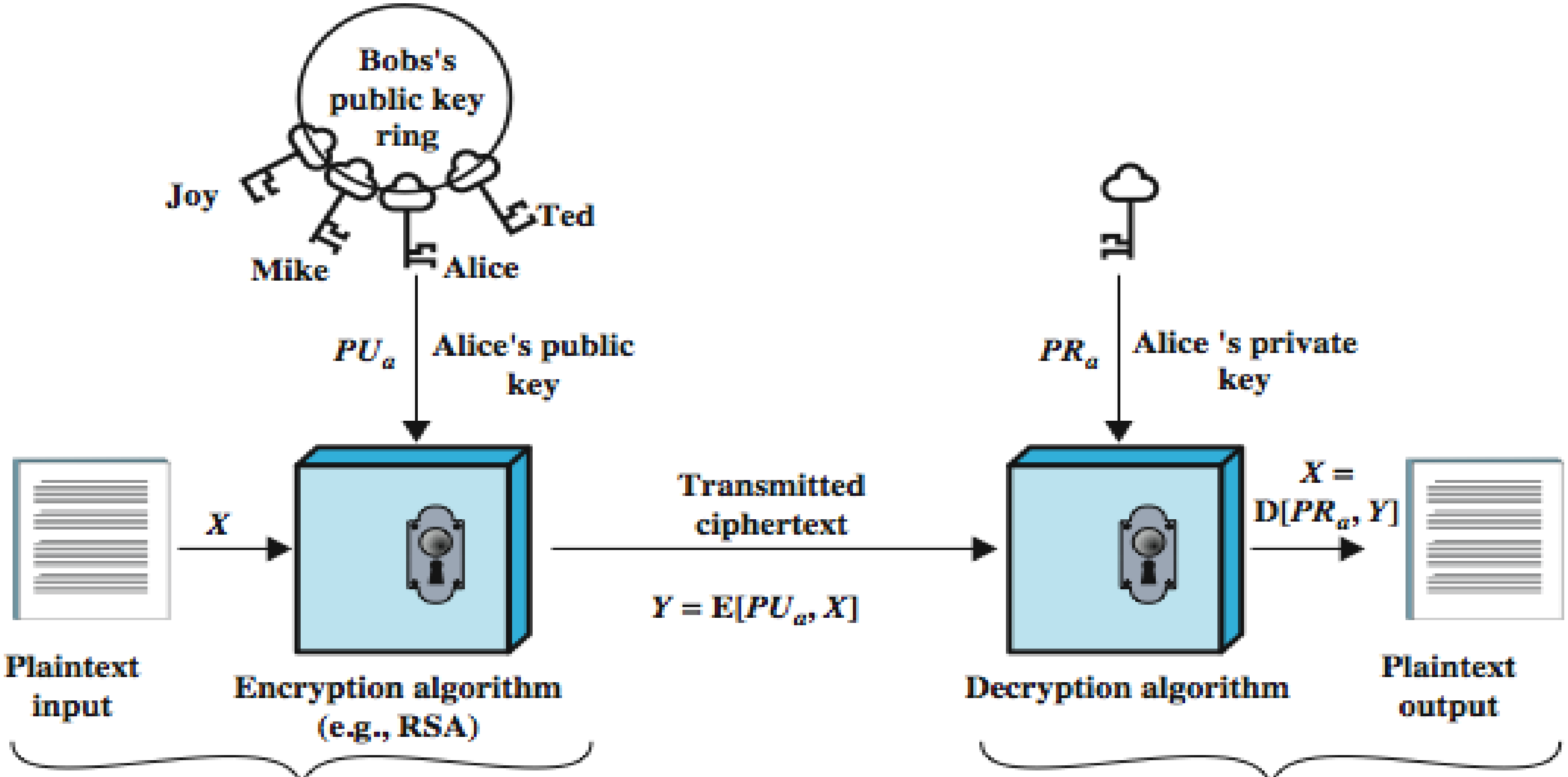
- Digital signatures (non-repudiation)
  - Not possible with symmetric crypto

Public-key cryptography

Application categories

- Encryption/decryption : to provide secrecy
- Digital signatures : to provide authentication and non-repudiation
- Key exchange: to agree on a session key

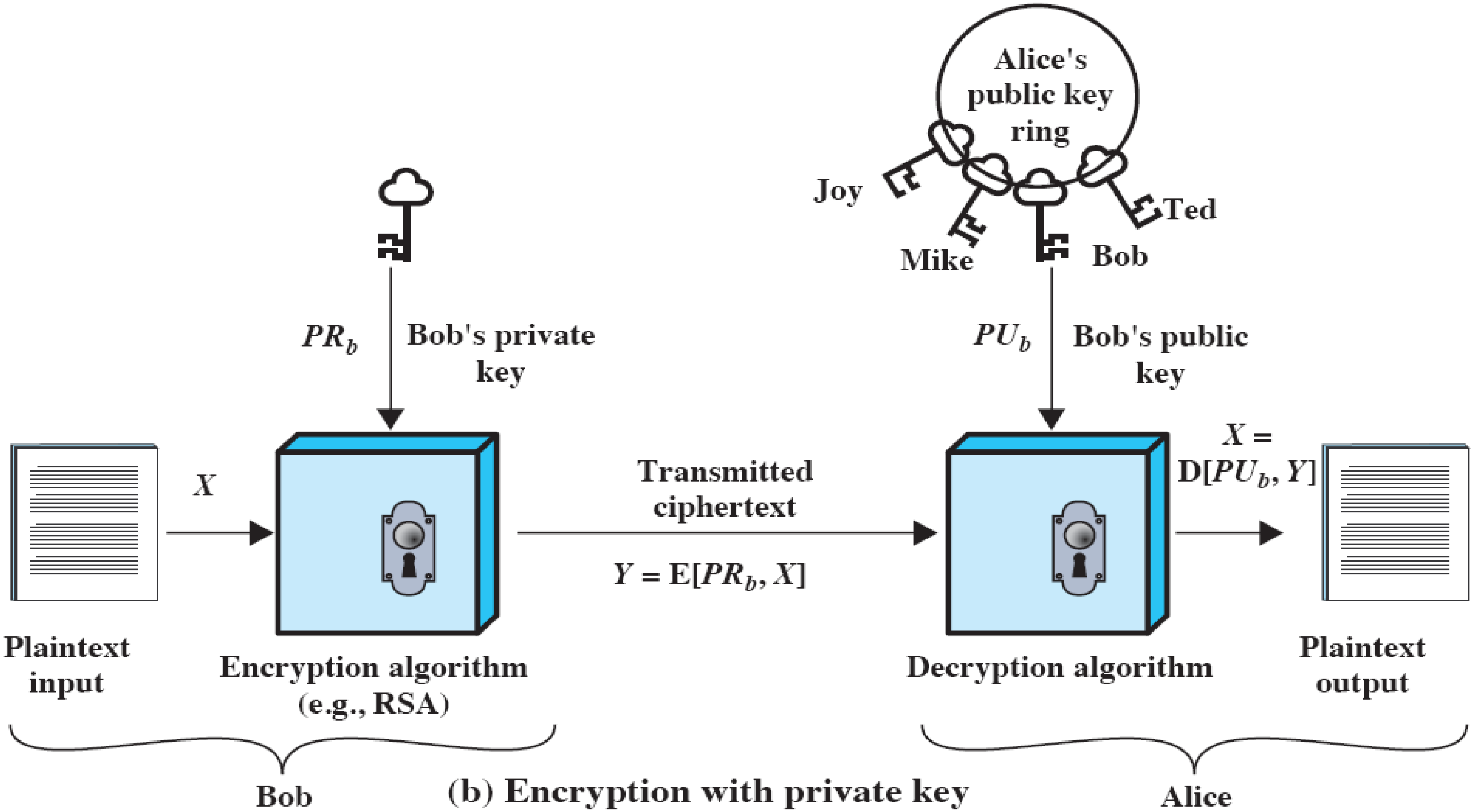
Public-key cryptography



(a) Encryption with public key

Public-key cryptography

Authentication (for Digital Signature)



(b) Encryption with private key

Key management

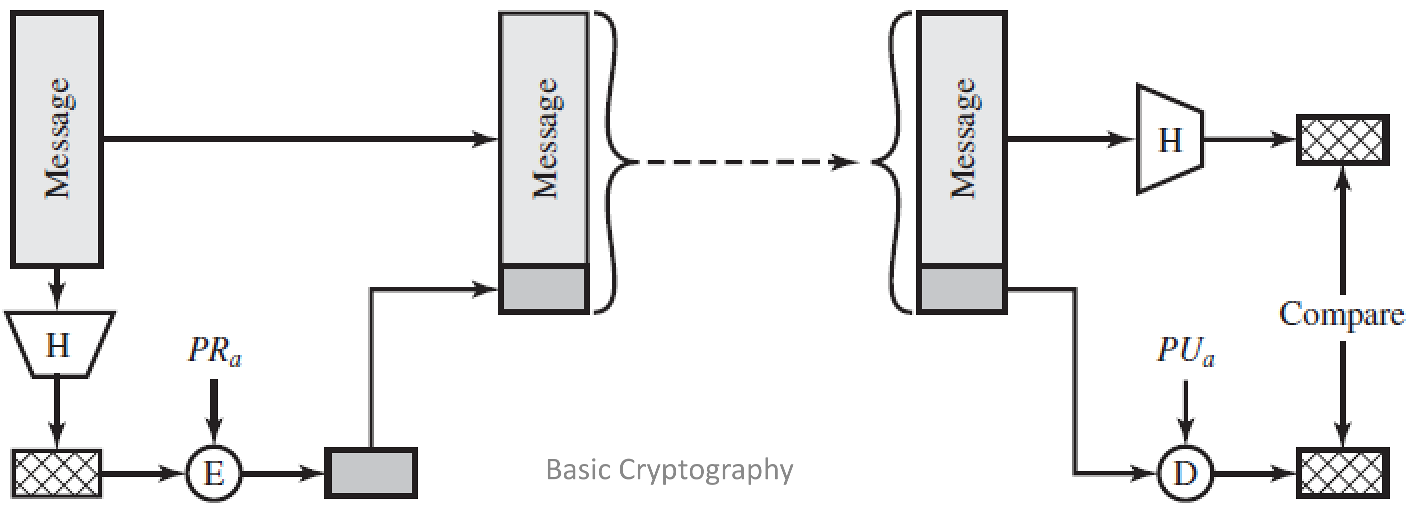
Key management and distribution with the use of public-key encryption:

- The secure distribution of public key
- The use of public-key encryption to distribute secret keys
- The use of public-key encryption to create temporary keys for message encryption

Key management

Digital signature

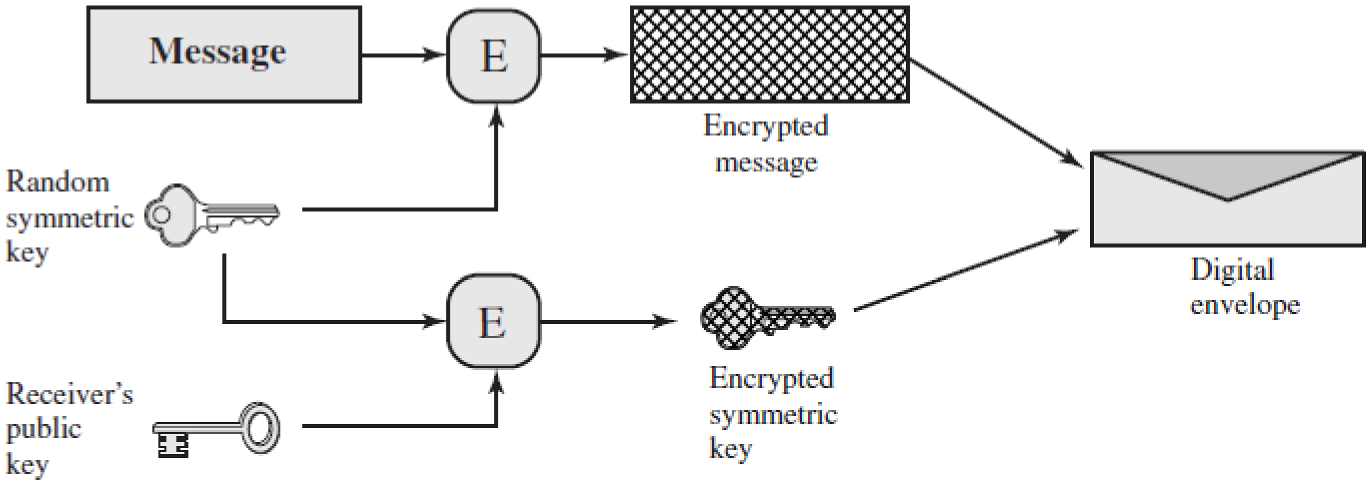
- Mechanism for non-repudiation
- Provide the ability to:
  - verify author, date and time of signature
  - authenticate message contents
  - be verified by third parties to resolve disputes
- Digital signature does not provide confidentiality



Key management

Digital envelopes

- It uses public key encryption to protect a symmetric key
- In the envelope, the message is protected without needing to first arrange for sender and receiver to have the same secret key.



(a) Creation of a digital envelope

Random Numbers

Random numbers in cryptography are used for

- Nonces in authentication protocols to prevent replay attacks
- Session keys, symmetric keys
- Public key generation
- Keystream for stream ciphers
- Key distribution scenarios, such as Kerberos (prevents replay attacks)

Random Numbers

- Characteristics of random numbers
  - Statistical randomness criteria
    - Uniform distribution of zeros and ones
    - Independence of the bits in the sequence
  - Unpredictability of future values from previous values
- True random numbers provide these but very hard to obtain and use in practice

Random Numbers

Pseudorandom Number Generators

- Often use deterministic algorithmic techniques to create random numbers
  - Although are not truly random
  - Can pass many tests of randomness
  - But are not statistically random
- Known as pseudorandom numbers
- Created by Pseudorandom Number Generators

Summary

- Introduces basic concepts of cryptography
- Operations of symmetric and asymmetric encryptions
- MAC and Hash functions
- Key distribution, digital signature, digital envelope,
- Random numbers and Pseudorandom