İTÜ
Computer Security

Basic Cryptography

Dr. Şerif Bahtiyar
bahtiyars@itu.edu.tr

1

Before Starting

Russian man charged over 'massive' US hack attacks

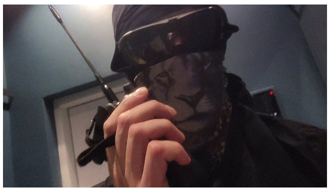
A Russian man extradited to the US has been charged with hacking into US banks, brokers and financial news firms.

https://www.bbc.com/news/technology-45472766

2

Before Starting

Rules of engagement issued to hacktivists after chaos



The International Committee of the Red Cross (ICRC) has, for the first time, published rules of engagement for civilian hackers involved in conflicts.

https://www.bbc.com/news/technology-66998064

3

Outline

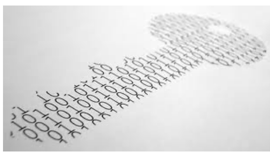
- Basic concepts
- Classification of cryptographic systems
- Computationally secure
- Unconditionally secure algorithm
- Symmetric-key cryptography
- Message authentication and hash
- Public-key cryptography
- Key management
- Random numbers

4

Basic Concepts

Cryptography

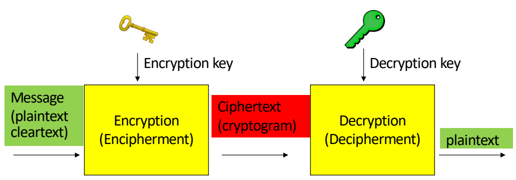
- Crypto: secret, hidden
- Graph: writing or study
- Cryptography is a study of secret writing to ensure secure systems in the presence of adversaries.



5

Basic Concepts

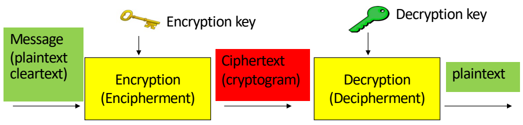
Basic scenario



6

Basic Concepts

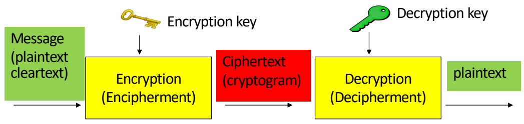
- Plaintext: the original message
- Ciphertext: the scrambled message
- Encrypt: converting plaintext to ciphertext
- Cipher: algorithm for transforming plaintext to ciphertex



7

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



8

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 -> 459 (İ->4, T->5, Ü->9)
- Transpositions (T)

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

  STSST
- Requirement: no information be lost!

9

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)

10

Classification of Cryptographic Systems

The way in which the plaintext is processed.

- Block cipher

  Istanbul -> qwertyuo
- Stream cipher

  Istanbul -> qstanbul

  Istanbul -> qwanbul

  .

  .

  Istanbul -> qwertyuo

11

Computationally Secure

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	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

12

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

https://www.youtube.com/watch?v=2imi8NEpF2Q

13

Unconditionally Secure Algorithm

Problems of OTP in practice

- large amount of random number generation
- protection and safe distribution of those keys

- How Hackers get OTP!

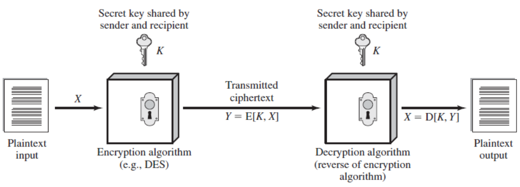
https://www.youtube.com/watch?v=ake-oTgoxfE

14

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.

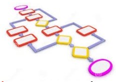


15

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

16

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 = $E_K(X)$ or E(K, X)

X = $D_K(Y)$ or D(K, Y)

17

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

18

Symmetric-key Cryptography

Approaches to attacking symmetric encryption scheme:

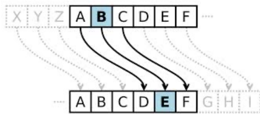
Brute-force attack: try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

19

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

20

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

21

Symmetric-key Cryptography

Rotor machines

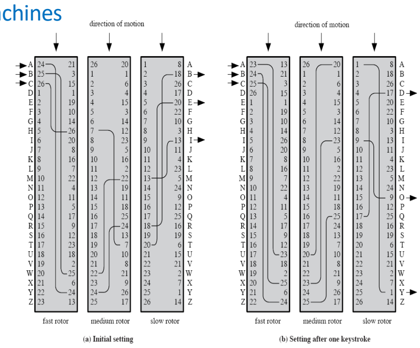


Figure 2.7 Three-Rotor Machine With Wiring Represented by Numbered Contacts

22

Symmetric-key Cryptography

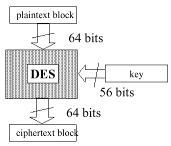
- Modern symmetric encryption systems use block or stream ciphers.
- Block ciphers operate on a block of data (file transfer, e-mail, database,…)
  - Limitation: Entire block must be available before processing
  - Advantage: Reuse of keys
  - DES, 3DES, AES
- Stream ciphers process messages one bit 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

23

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



24

Symmetric-key Cryptography

Table 2.1 **Comparison of Three Popular Symmetric Encryption Algorithms**

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

25

Symmetric-key Cryptography

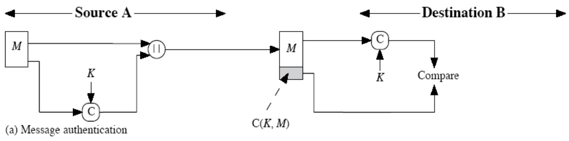
Table 2.2 **Average Time Required for Exhaustive Key Search**

Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/μs	Time Required at 10^{13} decryptions/μs
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1.125$ years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.3 \times 10^{21}$ years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.8 \times 10^{33}$ years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	$2^{191}\ \mu s = 9.8 \times 10^{40}$ years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	$2^{255}\ \mu s = 1.8 \times 10^{60}$ years	1.8×10^{56} years

26

Message Authentication and Hash

- 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

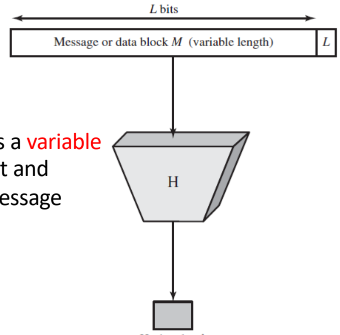


(a) Message authentication

27

Message Authentication and Hash

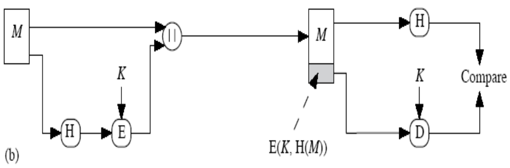
A hash function accepts a variable size message M as input and produces a fixed size message digest as output H(M).



28

Message Authentication and Hash

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



(b)

Hash without confidentiality

29

Message Authentication and Hash

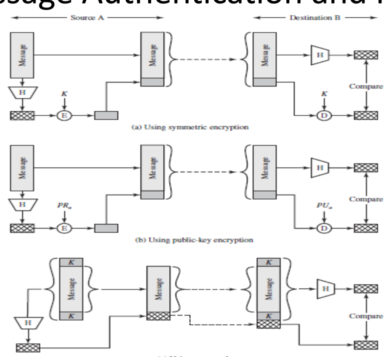
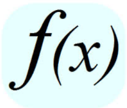


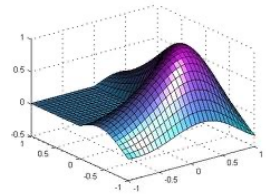
Figure 2.5 Message Authentication Using a One-Way Hash Function

30

Public-key Cryptography

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





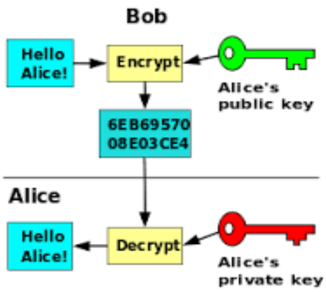
31

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*.

32

Public-key Cryptography

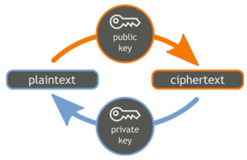


33

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



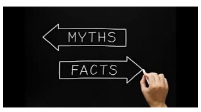
- Keys are related to each other but it is not feasible to find out private key from the public one

34

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)

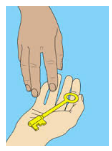


35

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



36

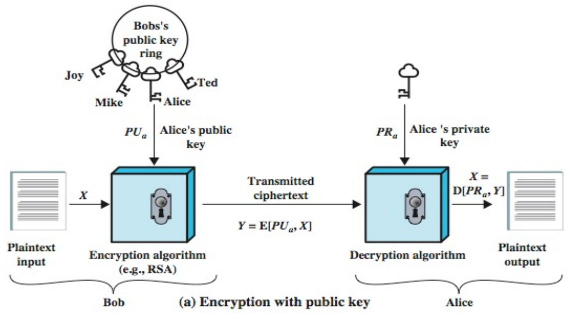
Public-key Cryptography

Application categories

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

37

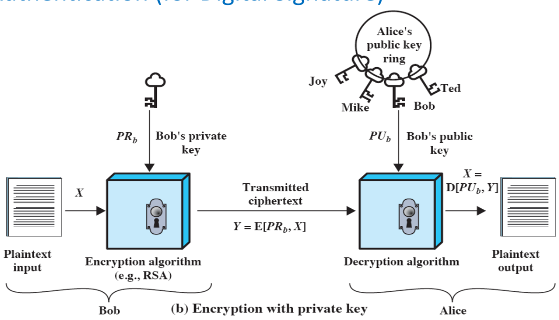
Public-key Cryptography



38

Public-key Cryptography

Authentication (for Digital Signature)



39

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

40

Key Management

Digital signature

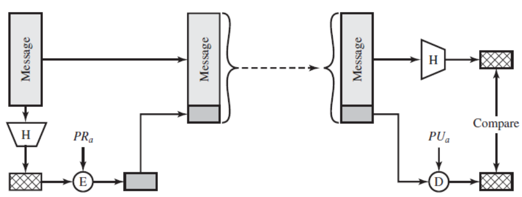
- Mechanism for non-repudiation
- Provide the ability to:
  - verify author, date and time of signature
  - authenticate message contents
  - be verified by third parties to resolve disputes

41

Key Management

Digital signature

Digital signature does not provide confidentiality

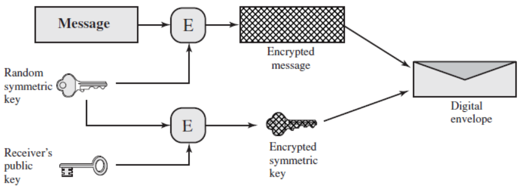


42

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

43

Random Numbers

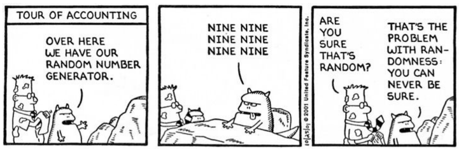
Random numbers in cryptography are used for

- 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)

44

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

45

Random Numbers

Pseudorandom Number Generators

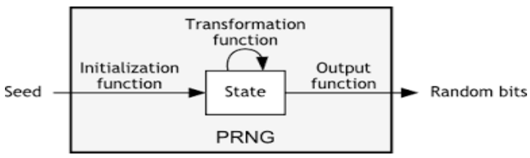
- Often use deterministic algorithmic techniques to create random numbers
  - Although are not truly random
  - Can pass many tests of randomness
  - But are not statistically random
- Known as pseudorandom numbers

46

Random Numbers

Pseudorandom Number Generators

Created by Pseudorandom Number Generators



47

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

48