
بسم الله الرحمن الرحيم

Network Security

Ali Shakiba
Vali-e-Asr University of Rafsanjan
ali.shakiba@vru.ac.ir
www.1ali.ir

What's ahead?

- The Course's Big Picture
- Introduction to Cryptography and Data Security
  - Overview on the field of cryptology
  - Basics of symmetric cryptography
  - Cryptanalysis
  - Substitution Cipher
  - Modular arithmetic
  - Shift (or Caesar) Cipher and Affine Cipher

Why do we need to study Computer/Networks/Information security?

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—The Art of War, Sun Tzu

Why do we need to study Computer/Networks/Information security?

The art of war teaches
the enemy's not com
receive him; not on th
rather on the fact t
unassailable.

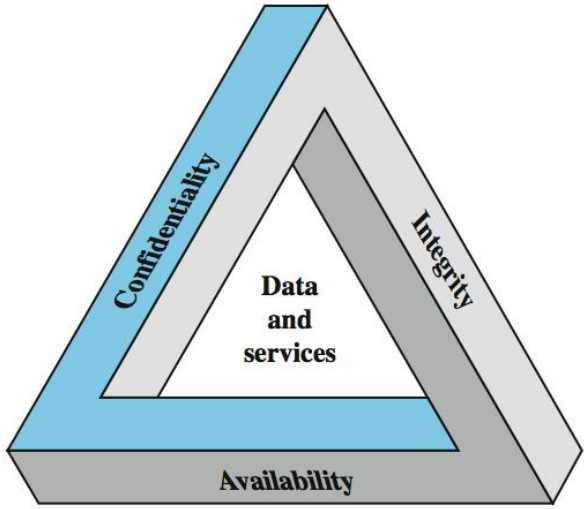
Why these three different terms?

Outline of the Course

- Cryptographic Algorithms
  - Symmetric Ciphers
  - Asymmetric Ciphers
  - Hash Functions
  - Protocols
- Mutual Trust
- Network & Internet Security
- Computer Security

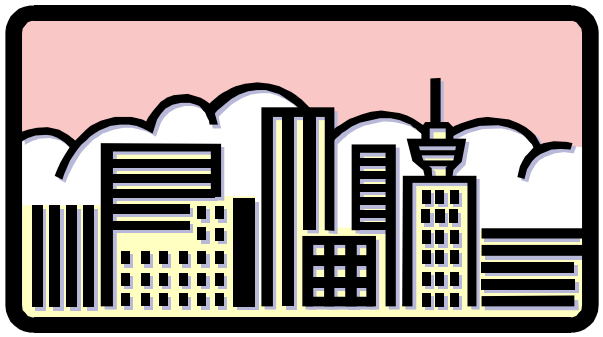
CIA Triad

- Confidentiality
  - Data confidentiality
  - Privacy
- Integrity
  - Data integrity
  - System integrity
- Availability



OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
  - defines a systematic way of defining and providing security requirements
  - for us it provides a useful, if abstract, overview of concepts we will study



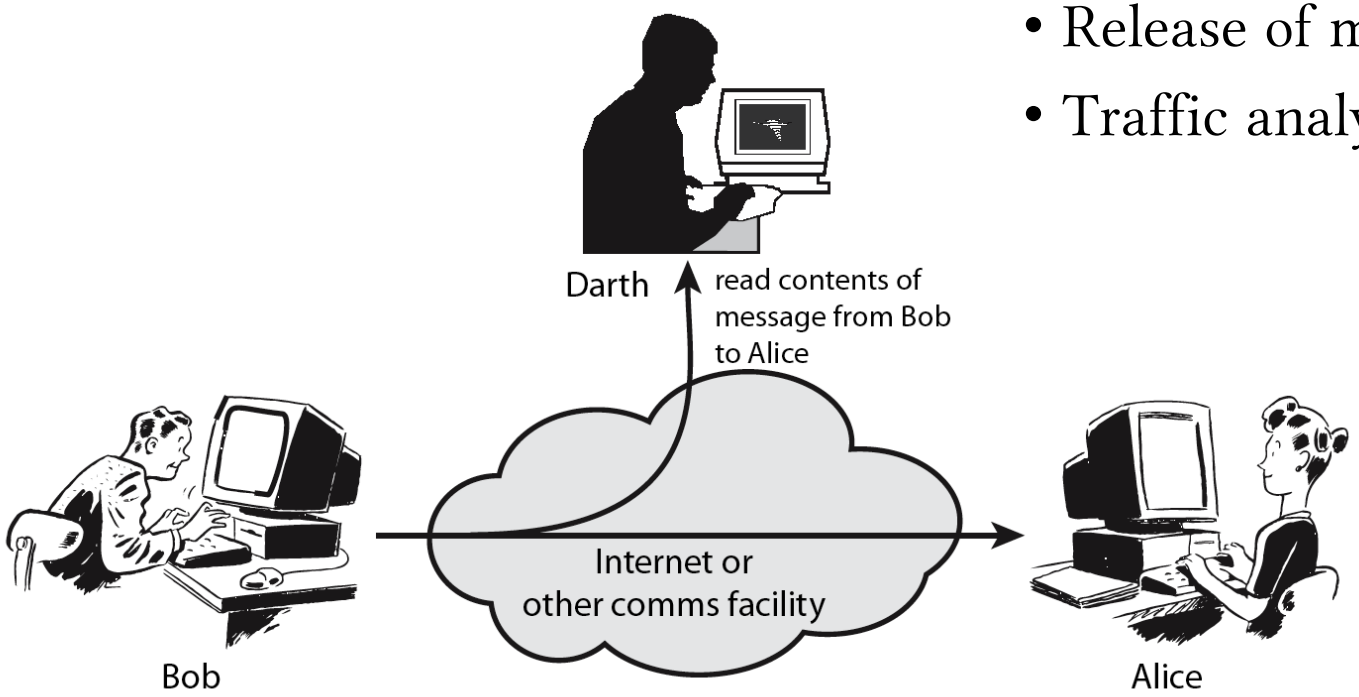
Standards Organizations

- National Institute of Standards & Technology (NIST)
- Internet Society (ISOC)
- International Telecommunication Union Telecommunication Standardization Sector (ITU-T)
- International Organization for Standardization (ISO)

Aspects of Security

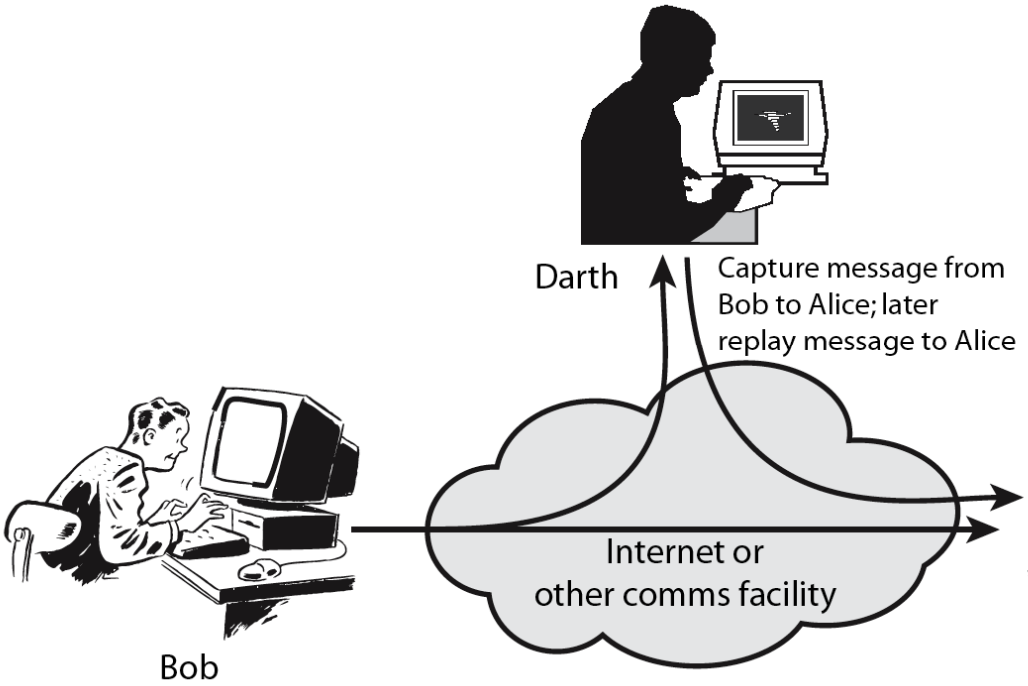
- X.800 considers 3 aspects of information security:
  - security **attack**
  - security **mechanism**
  - security **service**
- note terms (RFC 2828)
  - **threat** – a potential for violation of security
  - **attack** – an assault on system security, a deliberate attempt to evade security services

Passive Attacks



- Release of message content
- Traffic analysis

Active Attacks



- Masquerade
- Replay
- Message modification
- Denial of service

A Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Services

- X.800:

  "a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers"

- RFC 2828:

  "a processing or communication service provided by a system to give a specific kind of protection to system resources"

Security Services (X.800)

1. **Authentication** - assurance that communicating entity is the one claimed
   - have both peer-entity & data origin authentication
2. **Access Control** - prevention of the unauthorized use of a resource
3. **Data Confidentiality** –protection of data from unauthorized disclosure
4. **Data Integrity** - assurance that data received is as sent by an authorized entity
5. **Non-Repudiation** - protection against denial by one of the parties in a communication

Security Mechanism

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**
- hence our focus on this topic

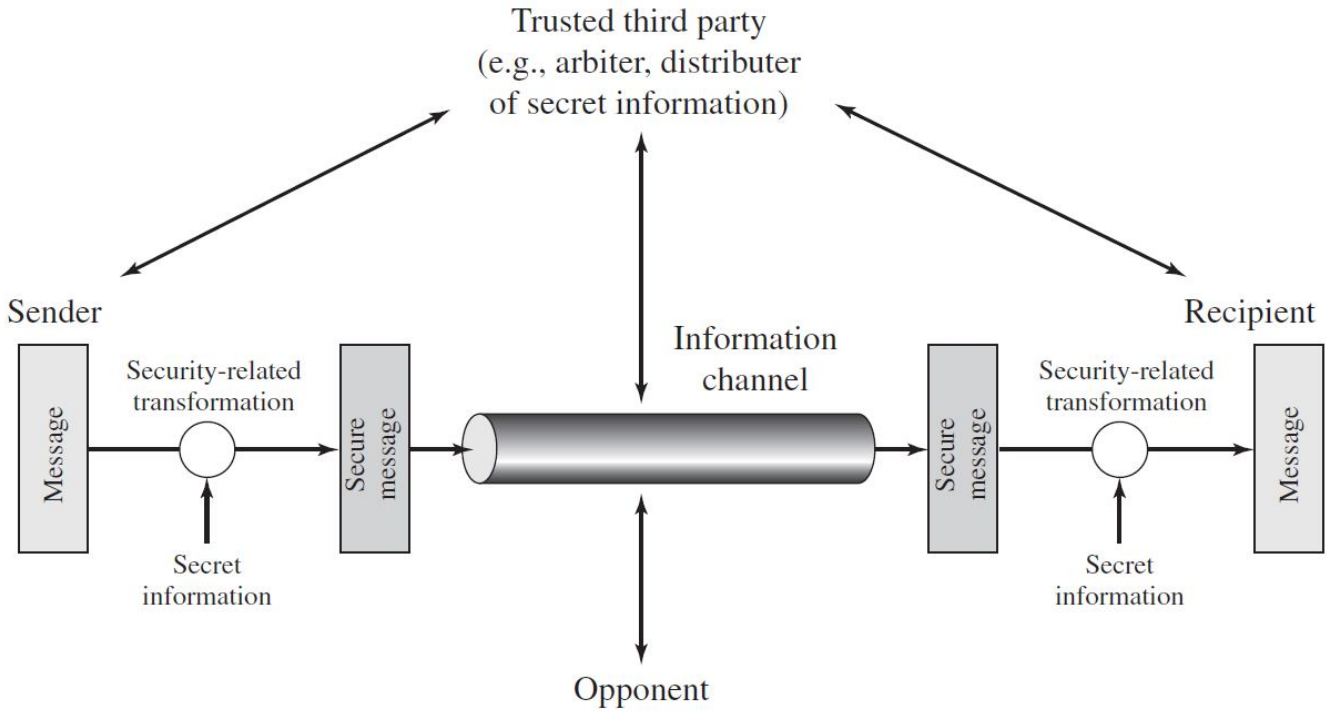
Security Mechanisms (X.800)

- specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery

Security Service vs. Mechanism?

SERVICE \ MECHANISM	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Model for Network Security

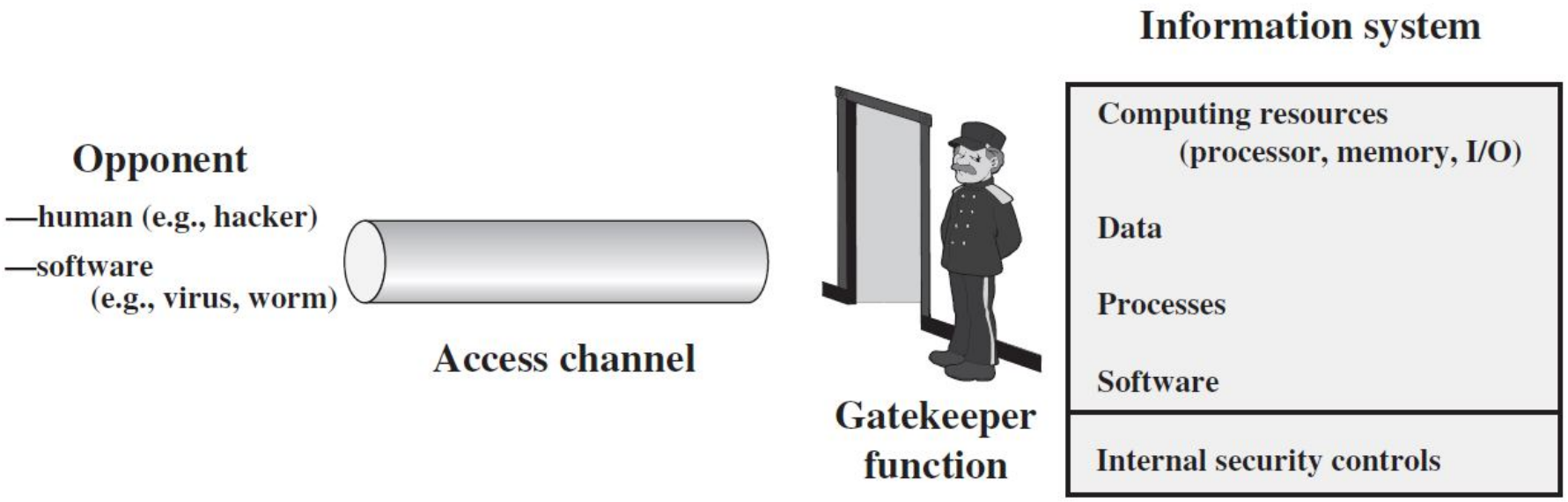


Model for Network Security

using this model requires us to:

1. design a suitable algorithm for the security transformation
2. generate the secret information (keys) used by the algorithm
3. develop methods to distribute and share the secret information
4. specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Model for Network Access Security

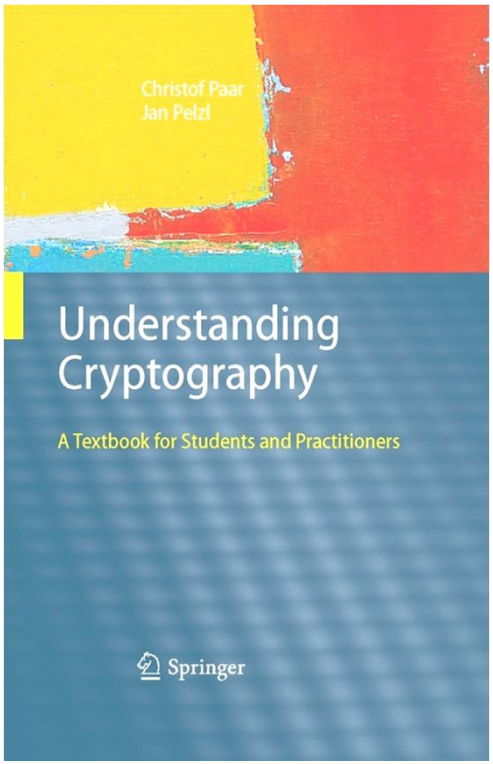
using this model requires us to:

1. select appropriate gatekeeper functions to identify users
2. implement security controls to ensure only authorised users access designated information or resources

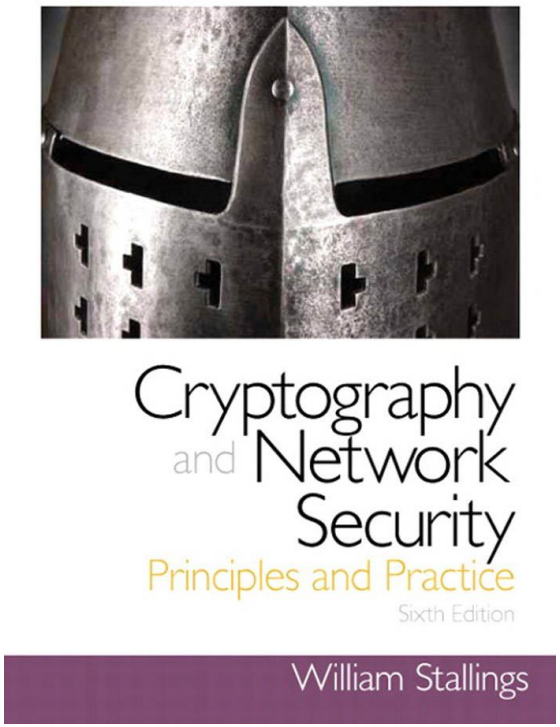
Required References

[PP10] Paar, Christof, and Jan Pelzl. ***Understanding cryptography: a textbook for students and practitioners***. Springer Science & Business Media, 2010.

All Chapters



Required References



[S14] Stallings, William. **Cryptography and Network Security: Principles and Practice**, 6th Edition. Pearson Higher Ed, 2014.

Parts 4 to 6

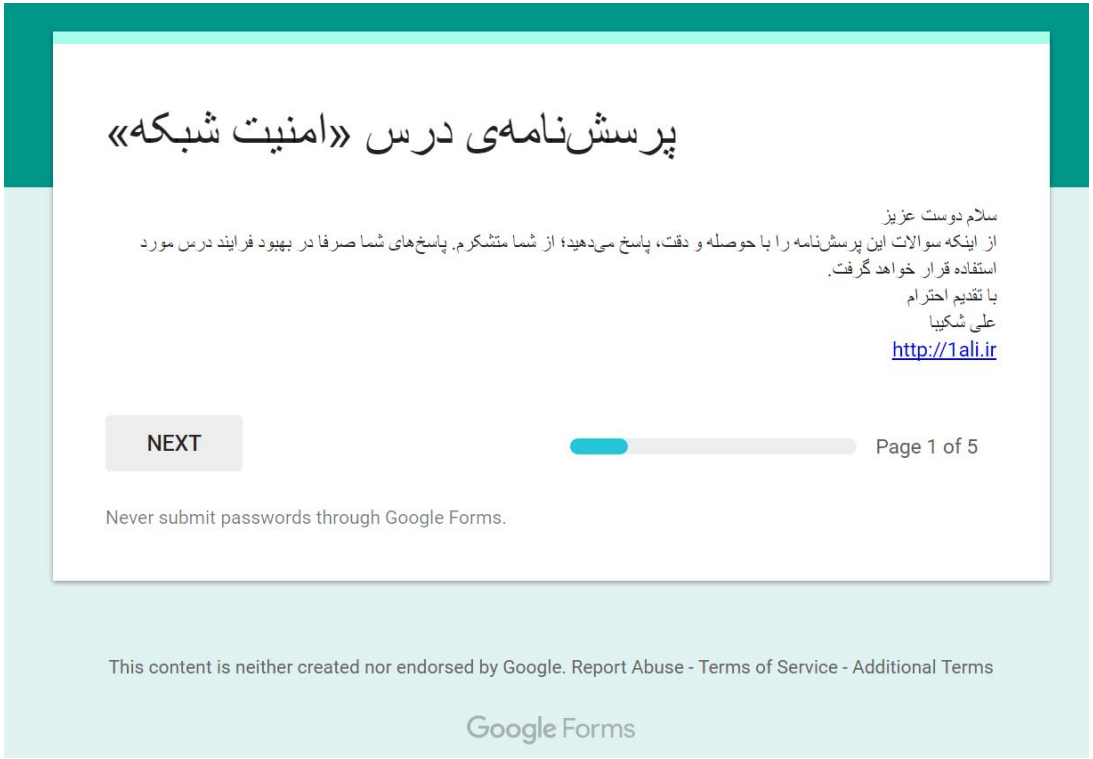
Evaluation

Title		Grade	Description
Exercises		5	At least 10 series, weekly
Project	Written Report	3	
	Presentation	2	
Written Exams	Midterm	4	Thursday, 4th Azar 1395
	Final	6	Consult EDU
Excellence		+2	
Total		**20 + 2**	

Course Page:

http://1ali.ir/network-security-95-1.html

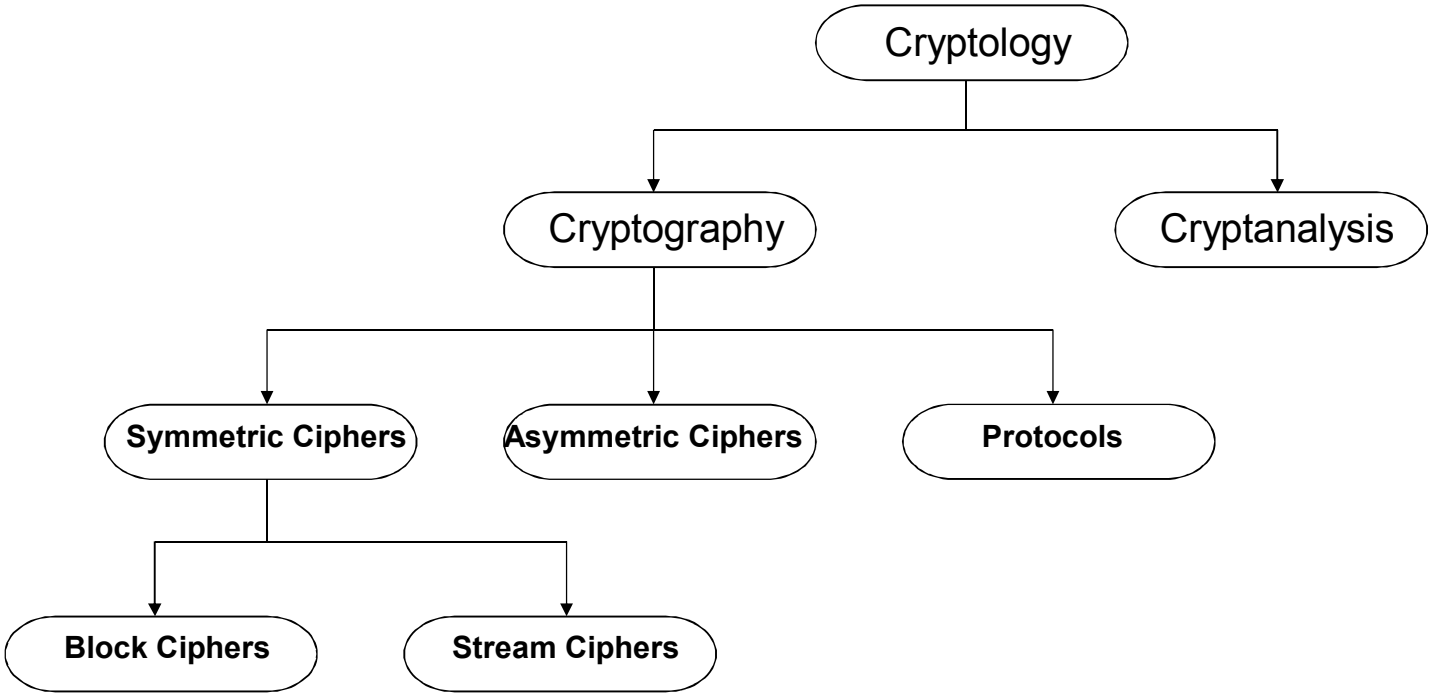
Fill in the SURVEY by the next session, please!



Let's Start Our Journey!

The Empire of Cryptology

Classification of the Field of Cryptology



Some Basic Facts

- **Ancient Crypto:** Early signs of encryption in Eqypt in 2000 B.C.
  Letter-based encryption schemes (e.g., Caesar cipher) popular ever since.

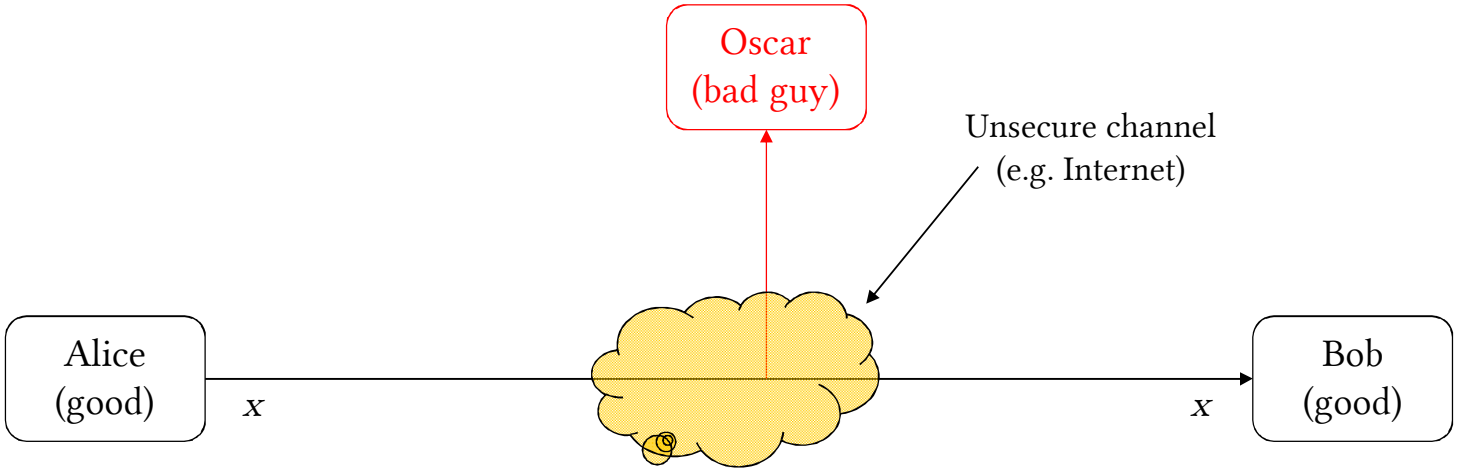
- **Symmetric ciphers:** All encryption schemes from ancient times until 1976 were symmetric ones.

- **Asymmetric ciphers:** In 1976 public-key (or asymmetric) cryptography was openly proposed by Diffie, Hellman and Merkle.

- **Hybrid Schemes:** The majority of today‘s protocols are hybrid schemes, i.e., the use both
  - symmteric ciphers (e.g., for encryption and message authentication) and
  - asymmetric ciphers (e.g., for key exchange and digital signature).

Symmetric Cryptography

- Alternative names: **private-key**, **single-key** or **secret-key** cryptography.



- **Problem Statement:**

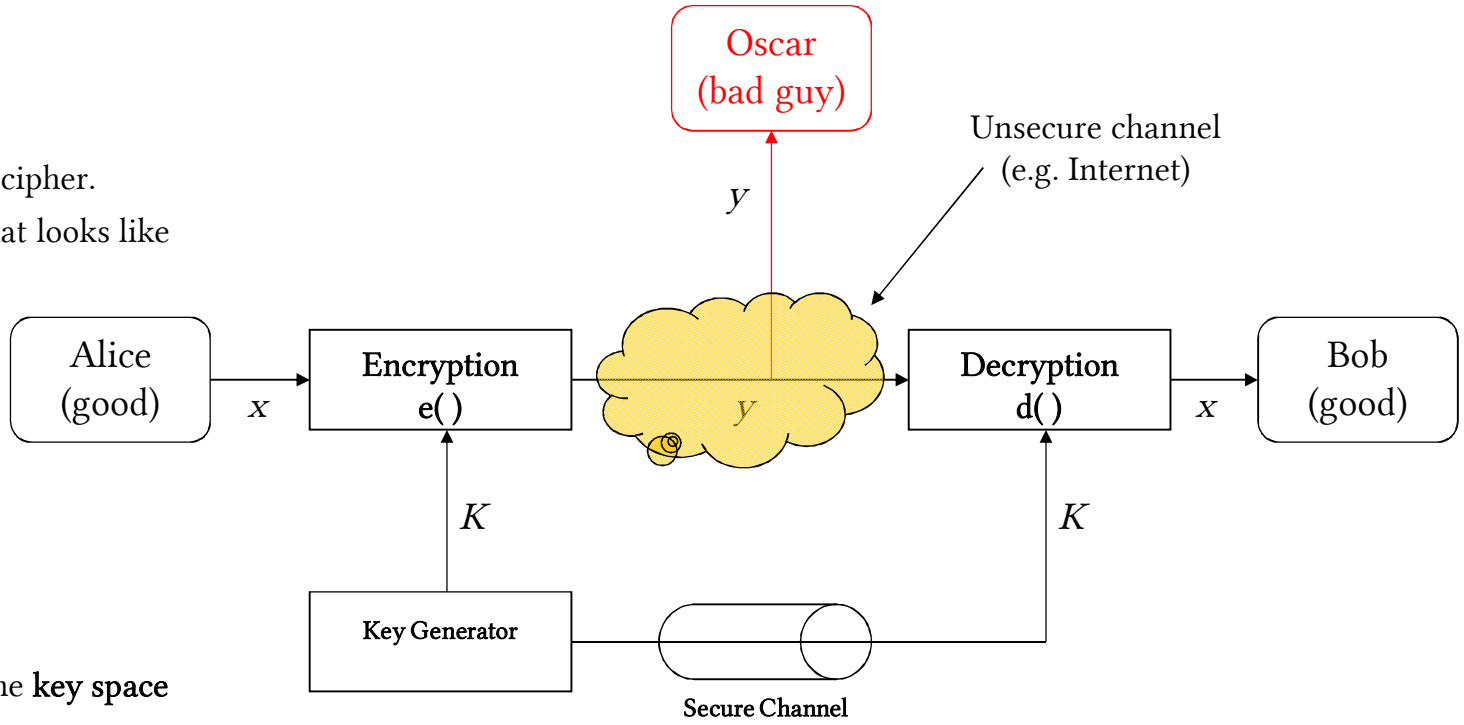
  1) Alice and Bob would like to communicate via an unsecure channel (e.g., WLAN or Internet).

  2) A malicious third party Oscar (the bad guy) has channel access but should not be able to understand the communication.

Symmetric Cryptography

Solution: Encryption with symmetric cipher.

⇒ Oscar obtains only ciphertext y, that looks like random bits



- x is the. **plaintext**
- y is the **ciphertext**
- *K* is the **key**
- Set of all keys {*K*1, *K*2, ...,*Kn*} is the **key space**

Symmetric Cryptography

- Encryption equation $y = e_K(x)$
- Decryption equation $x = d_K(y)$

- Encryption and decryption are inverse operations if the same key K is used on both sides:

$$d_K(y) = d_K(e_K(x)) = x$$

- Important: The key must be transmitted via a **secure channel** between Alice and Bob.
- The secure channel can be realized, e.g., by manually installing the key for the Wi-Fi Protected Access (WPA) protocol or a human courier.
- However, the system is only secure if an attacker does not learn the key K!

⇒ The problem of secure communication is reduced to secure transmission and storage of the key K.