# Introduction to Cryptography
# Lecture 1

Monika K. Polak

January 20, 2021

# Course Description

- This course provides an introduction to cryptography, its **mathematical** foundations, and its relation to security.
- It covers classical cryptosystems, private-key cryptosystems (including DES and AES), hash functions and public-key cryptosystems (including RSA).
- The course also provides an introduction to data integrity and authentication.

- Instructor: Monika Polak
- **Required Materials**
  Christof Paar and Jan Pelzl, Understanding Cryptography, SpringerLink, 2010
- Slides from the book (link)
  Remark: **Slides for the course may be different and will be posted on myCourses**
- Syllabus and Schedule (link)
- Grading components

| Component | Weight |
|---|---|
| Homeworks | 50% |
| Activity | 10% |
| Midterm exam | 20% |
| Final Exam | 20% |

# Activity task 1 (1% of the final grade)

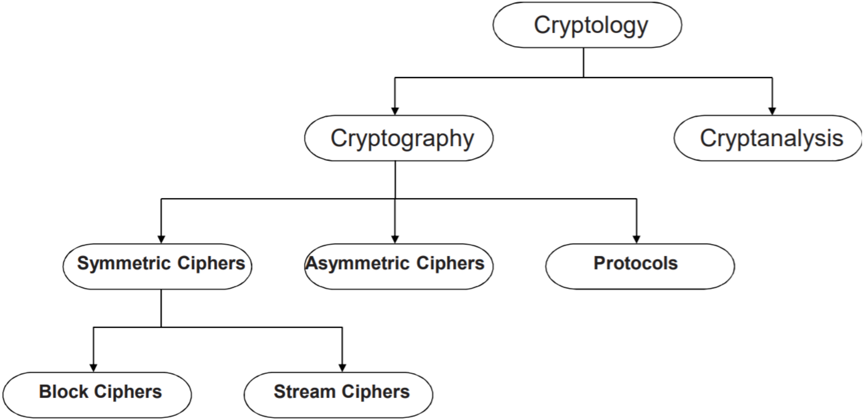
- Answer the question:

  **What is your expectation for this course?**

- and submit it to the proper dropbox on myCourses
- due Sunday, January 31, 11:59PM

# Content of this lecture

- Overview on the field of cryptology
- Basics of symmetric cryptography
- Shift (or Caesar) Cipher


Cryptology
Cryptography
Cryptanalysis
Symmetric Ciphers
Asymmetric Ciphers
Protocols
Block Ciphers
Stream Ciphers

# The Goals of Practical Cryptography

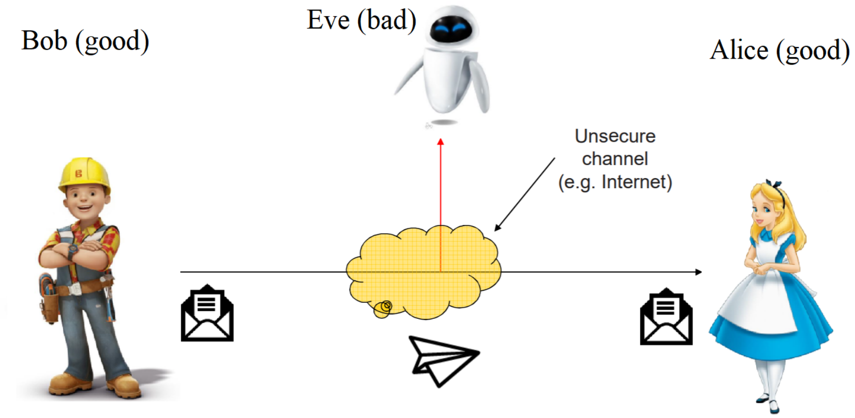
- **Confidentiality**
  - **Data confidentiality**
    Assures that private or confidential information is not made available or disclosed to unauthorized individuals
  - **Privacy**
    Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed
- **Authentication**
  We can establish the identity of a remote user (or system).
- **Integrity**
  We can provide a means to ensure data is not viewed or altered during storage or transmission.
- **Non-Repudiation**
  It must not be possible for the user to refute his or her actions.

# Some Basic Facts

- **Ancient Crypto**: Early signs of encryption in Eqypt in ca. 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

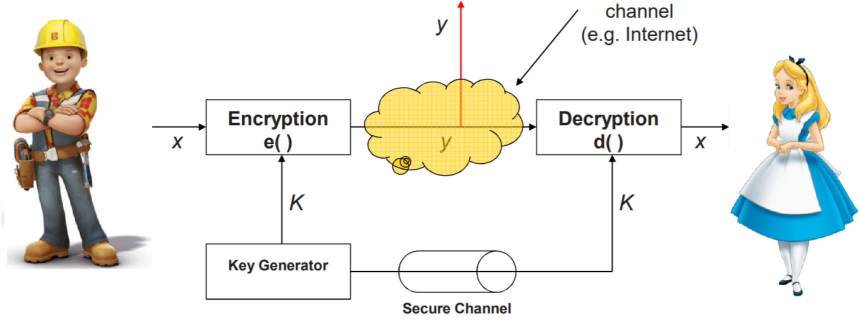
Alternative names: private-key, single-key or secret-key cryptography.




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

# Symmetric Cryptography

**Solution:** Encryption with symmetric cipher.
⇒ Eve obtains only ciphertext y, that
looks like random bits




x is the plaintext, y is the ciphertext, K is the key
Set of all possible keys 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:

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

# Symmetric Cryptography

- 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.

# Shift (or Caesar) Cipher

- Ancient cipher, allegedly used by Julius Caesar
- Replaces each plaintext letter by another one.
- Replacement rule is very simple: Take letter that follows after $K$ positions in the alphabet
  Needs mapping from letters $\rightarrow$ numbers:

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

# Shift (or Caesar) Cipher

- Replacement rule is very simple: Take letter that follows after $K$ positions in the alphabet

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

- Example for $K = 7$
  **Plaintext** = ATTACK = 0, 19, 19, 0, 2, 10
  **Ciphertext** = haahr = 7, 0, 0, 7, 17
  Note that the letters "wrap around" at the end of the alphabet, which can be mathematically be expressed as reduction modulo 26, e.g., $19 + 7 = 26 \equiv 0 \mod 26$

# Shift (or Caesar) Cipher

- Elegant mathematical description of the cipher. Let $K, x, y \in \{0, 1, \ldots, 25\}$

  **Encryption:**

  $$y = e_K(x) \equiv (x + K) \mod 26$$

  **Decryption:**

  $$x = d_K(x) \equiv (y - K) \mod 26$$

- Is the shift cipher secure?
  **No!** several attacks are possible, including:
  - Exhaustive key search (key space is only 26)
  - Letter frequency analysis (Lecture 2)

Thanks for Your attention.