Cryptocomplexity I

Kryptokomplexität I

Wintersemester 2023/2024

Chapter 1: Tasks and Aims of Cryptology

Dozent: Prof. Dr. J. Rothe

Websites

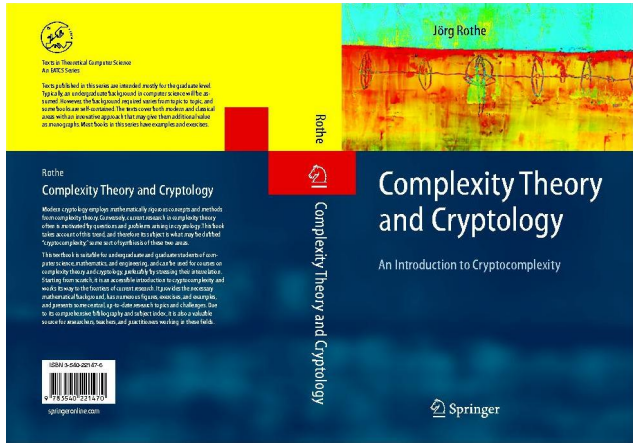
- All information and all material (slides, literature, exercises, ...) for this module can be found in **ILIAS**.
- In addition, slides, exercises, and other material can also be downloaded from:

  `https://ccc.cs.uni-duesseldorf.de/~rothe/cryptocomp1`

Literature

Jörg Rothe: "Komplexitätstheorie und Kryptologie. Eine Einführung in Kryptokomplexität", eXamen.Press, Springer-Verlag, 2008

Jörg Rothe: "Complexity Theory and Cryptology. An Introduction to Cryptocomplexity", EATCS Texts in Theoretical Computer Science, Springer-Verlag, 2005



Literature

- **Douglas R. Stinson: "Cryptography: Theory and Practice"**, Chapman & Hall/CRC, 2. Auflage, 2002
- **Johannes Buchmann: "Einführung in die Kryptographie"**, Springer-Verlag, 2. Auflage, 2001
- **Arto Salomaa: "Public-Key Cryptography"**, Springer-Verlag, 1990
- **Oded Goldreich: "Foundations of Cryptography"**, Cambridge University Press, 2001
- **Bruce Schneier: "Applied Cryptography"**, John Wiley & Sons, 1996

What is Cryptology?

Cryptology

is the art &

science of

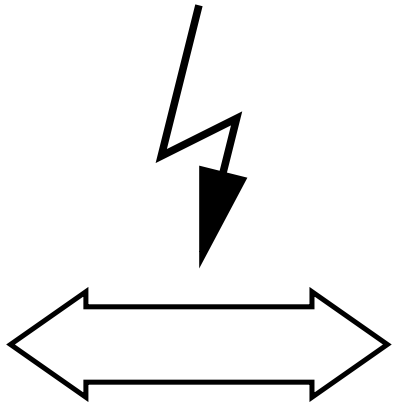
Cryptography	**Cryptanalysis**
encrypting texts and	breaking existing cryptosystems
messages such that	by determining the encryption
unauthorized decryption	keys and deciphering encrypted
is prevented	messages without authorization

Related Fields . . .

- . . . we will *not* consider:
  - Steganography
  - Coding Theory
- . . . whose notions, results, and methods will be used:
  - Complexity Theory
  - Number Theory and (Linear) Algebra
  - Probability Theory
  - Algorithmics

A Typical Cryptographic Scenario

Erich

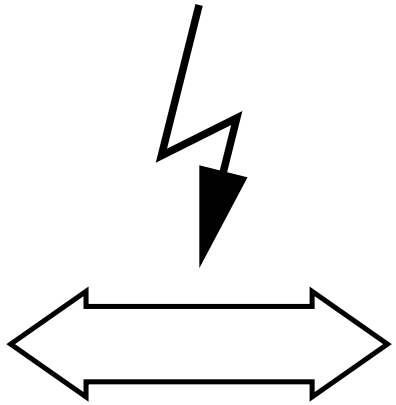


© The design of Alice and Bob is due to Crépeau.

Why Alice and Bob?

A Typical Cryptographic Scenario

Jennifer



Angelina **Brad**

Cryptosystem

Definition

A *cryptosystem* is a quintuple $S = (M, C, K, \mathscr{E}, \mathscr{D})$ such that:

1. M, C, and K are sets, where
   - M is the *message space* (or *"plaintext space"* or *"cleartext space"*),
   - C is the *ciphertext space*, and
   - K is the *key space*.
2. $\mathscr{E} = \{E_k \mid k \in K\}$ is a family of functions $E_k : M \to C$ that are used for encryption, and
3. $\mathscr{D} = \{D_k \mid k \in K\}$ is a family of functions $D_k : C \to M$ that are used for decryption.
4. For each key $e \in K$, there exists a key $d \in K$ such that for each message $m \in M$:

$$D_d(E_e(m)) = m. \tag{1}$$

Cryptosystem

Definition

- A *cryptosystem* is called *symmetric* (or *"private-key"*) if $d = e$, or if d can at least be "easily" computed from e.

- A *cryptosystem* is called *asymmetric* (or *"public-key"*) if $d \neq e$, and it is "practically infeasible" to compute d from e. Here, d is the *private key*, and e is the *public key*.

Types of Attack

- Ciphertext-Only Attack
  - Known: some ciphertexts
  - Determine: the corresponding plaintext/keys
- Known-Plaintext Attack
  - Known: $(p_1, c_1), (p_2, c_2), \ldots, (p_k, c_k)$
  - Determine: the corresponding keys/other ciphertexts
- Chosen-Plaintext Attack
  - Choose: some plaintexts at will
  - Obtain: the corresponding ciphertexts
  - Determine: the corresponding keys

Types of Attack and Kerckhoffs's Principle

- Chosen-Ciphertext Attack
  - Choose: some ciphertexts at will
  - Obtain: the corresponding plaintexts
  - Determine: the corresponding keys

- Key-Only Attack (relevant only for public-key cryptosystems)
  - Known: the public keys
  - Determine: the corresponding private keys

Kerckhoffs's Principle:

The security of a cryptosystem must not depend on the secrecy of the system used. Rather, the security of a cryptosystem may depend only on the secrecy of the keys used.

Digital Signatures and Authentication

- Digital Signatures: Alice wants to sign her (encrypted) messages to Bob such that
  (a) Bob can verify that indeed she is the sender of the message, and
  (b) also third parties (who perhaps do not trust Bob) can convince themselves of the authenticity of her signature.

  Property (a) is already achieved by symmetric authentication codes.

- Authentication codes:
  - provide a method of ensuring the integrity of a message.
  - Active Attacks:
    - *Substitution Attack*: Erich might try to tamper with (i.e., to change or replace) the messages transmitted.
    - *Impersonation Attack* (a.k.a. "*Man-in-the-middle Attack*"): Erich might try to introduce a message of his own into the channel, hoping it is accepted as authentic by Bob.

Authentication Problems

- **Message integrity**: How can one be sure that no intruder has tampered with the message received?
- **Message authentication**: How can one be sure that a message indeed originated from the sender asserted and was not introduced by an intruder?
- **User authentication**: How can one be sure of the identity of an individual?