Cryptography

Rudolf Mathar
Markus Rothe
Arash Behboodii

www.ti.rwth-aachen.de
crypto@ti.rwth-aachen.de

user: Diffie
password: Hellman

Exam: 23 August 2018, 11:30

1. Introduction

Objectives of Cryptography:
1. Conceal data & messages from eavesdroppers, make it available only to entitled receivers.
2. Authentication of users & messages
3. Anonymity & privacy
4. Protocols (transmission, key management)

After 1976: Distributed computers, increasing connectivity and communications, growing public interest.

Seminal paper: Diffie & Hellman

"New directions in cryptography"

(Contains the principles of public key encryption.)

Modern applications: Whatsapp, electronic banking, electronic cash, e-commerce, computer access, VPN, mobile communication, .......

Fundamental knowledge for cryptographers: (i)

- Alice, Bob, Opponent (skar) / Eve (Sender) (Receiver) (eavesdropper / intruder)

- NSA: National Security Agency (10,000 employees)
  (No Such Agency, Never Say Anything)
- BSI: Bundesamt für Sicherheit in der Informationstechnik
  Since 1940, ~400 employees.
- IACR: Intern. Ass. for Crypt. Research
  3 conferences per year
  2018 Eurocrypt, Tel Aviv (April)
  Crypto, Santa Barbara (August)
  Asiacrypt, Brisbane (Dec.)
  (www.iacr.org)

2. Classical Cryptography

2.1. Ancient system used by the Spartans (400 BC)

- wand/rod (σκούταλυ)
- stripe of parchment wrapped around the wand
2.2. Cesar Cipher (100 - 44 BC)

\{ \text{A, B, \ldots, Z} \} \leftrightarrow \{0, 1, \ldots, 25\} = \mathbb{Z}_{26}

arithmetik \mod 26

Select a key \( k \in \mathbb{Z}_{26} \)

Encryption: \( e(i) = (i + k) \mod 26 = c \)

plain text symbol \hspace{1cm} ciphertext

Decryption: \( d(c) = (c - k) \mod 26 = \)

\( = (c + 26 - k) \mod 26 = i \)

Mature by Leon Battista Alberti (1404 - 1472)

Note: Cesar cipher is \textit{monoalphabetic}.
Each plaintext char. is encrypted by a unique ciphertext char.