RWTH AACHEN UNIVERSITY

SS 2018

Cryptography

Rudolf Mathar
Markus Rothe
Arash Behboodi

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

usr: Diffie
passwd: Hellman

Exam: 23 August 2018, 11:30 (CHECK!)

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)

Before 1975: Mostly mainframes.
Mostly military research. Sparse networks.

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

Seminal paper: Diffie & Hellmann
"New directions in cryptography"
IEEE Trans. Inf. Th., 22, 1976, 644-654.
(Contains the principles of public key encryption.)

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

Fundamental knowledge for cryptographers: (:)

- Alice, Bob, Opponent (Spy) / Eve
  (Sender) (Receiver) (eavesdropper / intruder)
- NSA: National Security Agency (16'000 employees)
  (No Such Agency, Never Say Anything)

- BSI: Bundesamt für Informationstechnik Sicherheit in der

  Since 1990, ~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 (~~skytale~~ σκυτάλη)

stripe of parchment wrapped around the wand

2.2. Cesar Cipher (100 – 44 BC)

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

arithmetic mod 26

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

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

(i: plain text symbol, c: ciphertext)

Decryption: $d(c) = (c - k) \bmod 26 =$

$= (c + 26 - k) \bmod 26 = i$

Madame by Leon Battista Alberti (1404 – 1472)

Note: Cesar cipher is monoalphabetic.

Each plaintext char. is encrypted by a unique ciphertext char.