RWTH AACHEN UNIVERSITY

Cryptography

Rudolf Mathar, Michael Reyer

RWTH moodle & TI web pages
- announcements
- lecture notes
- handwritten lectures notes
  - fixed
  - annotatable

www.ti.rwth-aachen.de
- usr: Diffie
  passwd: Hellman

Lecture notes:
- Chap 1-8 → Cryptography
- Chap 9-14 → AMC

Examination: 19.08.2019, 14:30, PPS H2
- Written exam
- Review exercises & rehearsal exam
  26.7.19, R002, 10:30
- Extra consultation hours
  02.08.2019, 10:30, R002

[Exam on AMC : 03.09.2019, 11:30, PPS H2]

Discussion hours : Friday, 11:00, R 333
by Vimal Radhakrishnan, from 12.04.19 on.

Consultation hours RM, MR upon agreement.

1. Introduction

Objectives of cryptography:

1. Conceal data & messages from eavesdroppers, make them available only to the entitled receiver.
2. Authentication of users and messages.
3. Anonymity & privacy
4. Protocols (transmission, key management)

Before 1975: Mostly military research. Most computers were mainframes. Sparse networks.

After 1976: Distributed computers, increasing connectivity, growing public interests.

Seminal paper: Diffie & Hellman. New Direction in Cryptography. IEEE Trans. Inf. Th., 22, 1976, 644-654. (Contains the principles of public key encryption.)

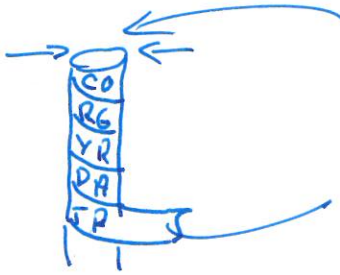
Modern application: electronic banking, electr. cash, e-commerce, automatic debiting, computer acces, VPN, mobile comm., Whatsapp, etc.

Fundamental knowledge for cryptographer :)

- A (lice), B (ob), O (ppoent) / E (ve)
  (Sender) (Receiver) (eavesdropper / intruder)
- NSA: National Security Agency, US founded 1952.
  (No Such Agency, Never Say Anything)
  (16.000 employees, many mathematicians)
- BSI, Bundesamt f. Sicherh. i.d. Inf.technik
  since 1990, ~400 employees [www.bsi.bund.de]
- IACR: Intern. Ass. for Cryptologic Research
  3 conf. per year
  Eurocrypt: 2019, Darmstadt
  Crypto: 2019, Santa Barbara
  Asiacrypt: 2019, Kobe
  [www.iacr.org]

2. Classical Cryptography

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



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 symbol / text, c: ciphertext)

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

Note: Cesar cipher is monoalphabetic, each plaintext char. is mapped to a unique ciphertext char.

2.4. Vigenère cipher (1523 – 1596)

Alphabet: $\{0, \ldots, 25\}$

Key string, keyword of length k: $(s_0, \ldots, s_{k-1})$

Plaintext: $a_0, \ldots, a_{k-1}, a_k, \ldots, a_{2k-1}, \ldots$

Key stream: $s_0, \ldots, s_{k-1}, s_0, \ldots, s_{k-1}, \ldots$

Encryption comp.wise add. mod. 26

$c_i = (a_i + s_{i \bmod k}) \bmod 26$

Note: Vigenere cipher is polyalphabetic.

- Vigenere cipher with running key
  Same as above, but ~~"no k"~~ no ~~block~~ keyword length.
  Exchange of key stream by, e.g., a book.

- Vernam cipher (1917).
  Same as Vigenere, but for each plaintext char. use a randomly generated key char. for a stream of the same length as the plaintext.