

Cryptography – Mini-script

Contents

1 Introduction	1
2 Notation	1
3 Historical ciphers	1
4 Kerckhoffs' principle	2
5 Perfect secrecy	2
6 Computational security	3
7 Pseudorandom generators	3
8 References	4

This document collects the definitions and theorems of the lecture, so that you have the precise formulations at hand. It contains no explanations, examples, or proofs: for those, see the lectures and the reading material. Each section ends with optional further reading (not exam-relevant beyond what was covered in the lecture).

It contains only material that has appeared already in the lecture or some assignments. So you don't need to scan it for new material but can use it as a reference.

1 Introduction

Further reading (what is cryptography): [1, §1.1] “Cryptography and Modern Cryptography” and §1.4 “Principles of Modern Cryptography” – how cryptography turned from an art into a science with definitions and proofs. Video: C. Paar, Lecture 1: Introduction to Cryptography. Outlook – proving your age without revealing your birth date is a *zero-knowledge proof* (later in the course): Wikipedia, Zero-knowledge proof.

2 Notation

Game notation (see the reading material on probability, section “Game notation”). $x \xleftarrow{\$} S$: x is chosen uniformly at random from the set S . $x \leftarrow A(e_1, \dots, e_n)$: the algorithm A is run on the values of $e_1, \dots, e_n$, and x is its output. $x \leftarrow e$: x is the value of e . $\Pr[B : G]$ is the probability of the event B when the values of the variables are chosen as described by the game G .

Adversaries are probabilistic algorithms (they may use randomness). A *t-time* algorithm runs at most t steps.

Unless said otherwise, any adversary has memory between executions. That is, in a game such as $(m_0, m_1) \leftarrow A(), \dots, b \leftarrow A(c)$, the call $A(c)$ remembers what $A()$ did.

Bitstrings. $\{0, 1\}^n$ is the set of bitstrings of length n . $x \oplus y$ is the bitwise XOR of two bitstrings of the same length.

3 Historical ciphers

Letters are identified with numbers: $A = 0, B = 1, \dots, Z = 25$; $+$ is addition modulo 26. A message is a sequence of letters $m_0 m_1 m_2 \dots$, the ciphertext $c_0 c_1 c_2 \dots$.

Definition 1 (Shift cipher). The key is a number $k \in \{0, \dots, 25\}$. Encryption: $c_i := m_i + k$. (The *Caesar cipher* is the shift cipher with $k = 3$; *ROT13* the one with $k = 13$.)

Definition 2 (Substitution cipher). The key is a permutation π of the alphabet (one of $26!$). Encryption: $c_i := \pi(m_i)$.

Definition 3 (Vigenère cipher). The key is a sequence of letters $k = k_0 \dots k_{|k|-1}$. Encryption: $c_i := m_i + k_{i \bmod |k|}$.

Further reading.

- *Shift and substitution cipher*: [1, §1.3] “Historical Ciphers and Their Cryptanalysis” (also Vigenère); [2, ch. 1] (Caesar, substitution, frequency analysis, Mary Queen of Scots); [3, ch. 2–3]. Videos: Khan Academy, The Caesar cipher and the series Journey into cryptography; C. Paar, Lecture 2: Modular Arithmetic and Historical Ciphers. Sources: Suetonius, *Life of Julius Caesar* §56 (English translation); I. A. Al-Kadi, “Origins of Cryptology: the Arab Contributions”, *Cryptologia* 16(2), 1992, doi:10.1080/0161-119291866801 (Al-Kindi, the oldest description of frequency analysis). Wikipedia: Caesar cipher, ROT13, Substitution cipher, Frequency analysis, Letter frequency.
- *Vigenère and how to break it*: [1, §1.3]; [2, ch. 2] (Babbage, Kasiski); [3, ch. 4, 6, 12] (index of coincidence). Video: Khan Academy, Polyalphabetic cipher. Sources: F. W. Kasiski, *Die Geheimschriften und die Dechiffrier-Kunst*, 1863; W. F. Friedman, *The Index of Coincidence and Its Applications in Cryptography*, 1922. Wikipedia: Vigenère cipher, Kasiski examination, Index of coincidence.
- *Enigma*: [2, ch. 3]; Crypto Museum, Enigma – How it works and Enigma I. Videos: Jared Owen, How did the Enigma Machine work?; Numberphile, 158,962,555,217,826,360,000 (Enigma Machine) and Flaw in the Enigma Code; Veritasium, The Insane Real Engineering of the Nazi Enigma Machine.

4 Kerckhoffs’ principle

Kerckhoffs’ principle (A. Kerckhoffs, 1883): the system must not require secrecy and can be stolen by the enemy without causing trouble.

Shannon’s formulation: “the enemy knows the system”.

That is, the security must rest only on the secrecy of the key, not on the secrecy of the algorithm.

Further reading.

- *Kerckhoffs’ principle, security by obscurity*: [1, §1.2] “The Setting of Private-Key Encryption” (syntax of encryption schemes, arguments for the principle); [2, ch. 1 and 3]. Sources: [4], [5]. Wikipedia: Kerckhoffs’s principle, Security through obscurity, A5/1.
- *Attack models* (ciphertext-only, known-plaintext, chosen-plaintext, chosen-ciphertext): [1, §1.4.1] “Principle 1 – Formal Definitions”. The “gardening” story: Wikipedia, Cryptanalysis of the Enigma, Gardening (cryptanalysis).

5 Perfect secrecy

Definition 4 (Perfect secrecy). Let $\mathcal{K}$ be the set of keys, $\mathcal{M}$ the set of messages, $\mathcal{C}$ the set of ciphertexts, and *Enc* the encryption algorithm (possibly randomized) of an encryption scheme. The encryption scheme has *perfect secrecy* iff for all $m_0, m_1 \in \mathcal{M}$ and for all $c \in \mathcal{C}$:

$$\Pr[Enc(k, m_0) = c : k \xleftarrow{\$} \mathcal{K}] = \Pr[Enc(k, m_1) = c : k \xleftarrow{\$} \mathcal{K}].$$

Definition 5 (One-time pad). Let $\mathcal{K} := \mathcal{M} := \mathcal{C} := \{0, 1\}^n$. The *one-time pad* encrypts a message $m \in \mathcal{M}$ under a key $k \in \mathcal{K}$ as $Enc(k, m) := k \oplus m$, and decrypts as $Dec(k, c) := k \oplus c$.

Theorem 1. *The one-time pad has perfect secrecy.*

Theorem 2. *There is no encryption scheme that has the following three properties:*

- *Perfect secrecy.*
- $|\mathcal{K}| < |\mathcal{M}|$, where $\mathcal{K}$ is the key space and $\mathcal{M}$ the message space.
- *Decrypting the encryption of a message always gives the original message back.*

Further reading.

- *Definition:* [1, §2.1] “Definitions” – their Definition 2.3 is the “a-priori = a-posteriori” view; the formulation above is their Lemma 2.5; Definition 2.6 and Lemma 2.7 give the game-based view (the adversary guesses which of two messages was encrypted). [5, §10] “Perfect Secrecy” – the original definition.

6 Computational security

Definition 6 (IND-EAV security). An encryption scheme (Enc, Dec) with key space $\mathcal{K}$ and message space $\mathcal{M}$ has (t, ε) -IND-EAV security iff for all probabilistic t -time algorithms A that output $m_0, m_1 \in \mathcal{M}$ and $b \in \{0, 1\}$:

$$\left| \Pr[b = 1 : k \xleftarrow{\$} \mathcal{K}, (m_0, m_1) \leftarrow A(), c \leftarrow Enc(k, m_0), b \leftarrow A(c)] \right. \\ \left. - \Pr[b = 1 : k \xleftarrow{\$} \mathcal{K}, (m_0, m_1) \leftarrow A(), c \leftarrow Enc(k, m_1), b \leftarrow A(c)] \right| \leq \varepsilon.$$

(IND = indistinguishability, EAV = eavesdropper.)

7 Pseudorandom generators

Definition 7 (Pseudorandom generator). A (deterministic) function $G : \{0, 1\}^n \rightarrow \{0, 1\}^\ell$ is a (t, ε) -PRG (pseudorandom generator) iff for all probabilistic t -time algorithms A that output $b \in \{0, 1\}$:

$$\left| \Pr[b = 1 : s \xleftarrow{\$} \{0, 1\}^n, r \leftarrow G(s), b \leftarrow A(r)] \right. \\ \left. - \Pr[b = 1 : r \xleftarrow{\$} \{0, 1\}^\ell, b \leftarrow A(r)] \right| \leq \varepsilon.$$

Definition 8 (Pseudo one-time pad). Let $G : \{0, 1\}^n \rightarrow \{0, 1\}^\ell$ be a pseudorandom generator. The *pseudo one-time pad* has key space $\mathcal{K} := \{0, 1\}^n$, message space $\mathcal{M} := \{0, 1\}^\ell$, and ciphertext space $\mathcal{C} := \{0, 1\}^\ell$, and is defined by

$$Enc(k, m) := m \oplus G(k), \quad Dec(k, c) := c \oplus G(k).$$

8 References

- [1] J. Katz, Y. Lindell: *Introduction to Modern Cryptography*, 3rd ed., CRC Press 2020.
- [2] S. Singh: *The Code Book*, 1999. RWTH library: print (German: *Geheime Botschaften*).
- [3] D. Kahn: *The Codebreakers*, revised ed., Scribner 1996.
- [4] A. Kerckhoffs: “La cryptographie militaire”, *Journal des sciences militaires* IX, 1883. Scans and English translation: petitcolas.net/kerckhoffs.
- [5] C. E. Shannon: “Communication Theory of Secrecy Systems”, *Bell System Technical Journal* 28(4), 1949. RWTH library: print, e-copy.