TECHNISCHE
UNIVERSITÄT
DARMSTADT

Technical University Darmstadt

– Department of Computer Science –

Introduction to Cryptography

A Summary of the Course Contents

Author:

Jonas Weßner

Teaching professor	:	Prof. Dr. Marc Fischlin
Semester	:	Winter semester 2022/2023

CONTENTS

LIST OF ABBREVIATIONS

INTRODUCTION

Cryptography is the science of the processes for securing information, data and systems.

Typically we talk about certain key concepts, which differ from book to book. In this course, we define them as the following:

C Confidentiality: Attackers cannot read a message.

 I Integrity: Attackers cannot modify the content of a message (in a narrow sense), cannot fake the message's sender address (authenticity) and receivers cannot claim, they have received the message (non-repudiation).

A Availability: A system is always functional (less relevant in this course)

Often in this lecture, we take a three-step approach to cryptographic processes:

1. **Abstract Object:** We define what interface our cryptographic process should work with. Often, we define one process for encryption, one for decryption and maybe others like one for key generation. We do not yet define their implementation.

2. **Security Model:** We define how our abstract object is used and in which cases our abstract object is secure. Questions to be answered are e.g. when is an attack successful and what is information the attacker is allowed to possess without introducing insecurity?

3. **Security Proof a Specific process:** When given a concrete implementation of our security model, we check the security of that model. For example, we prove that an attacker must calculate at least n hash sums to compromise the system.

Cryptographic processes can be classified in a matrix as follows:

	Private-Key	**Public-Key**
Confidentiality	Symmetric processes	Asymmetric processes
Integrity	Message Authentication Codes (MACs)	Digital signatures

Furthermore, there are elementary processes serving as building blocks to build cryptographic processes:

- Pseudo random number generators (PRNGs)

- Hash functions

- Blockcipher

- Number theory

2

PRIVATE-KEY CRYPTOGRAPHY

2.1 ONE TIME PAD

The One Time Pad works as follows:

1. Alice has a message $m \in \{0,1\}^n$ to be sent to Bob. Furthermore, Alice and Bob possess a common key $k \in \{0,1\}^n, n \in N$. n is called the security parameter.

2. Alice computes a cipher text $c \in \{0,1\}^n$ as $c = m \oplus k$ and sends it to Bob.

3. Bob reconstructs the plain message as $m = c \oplus k = m \oplus k \oplus k = m \oplus \{0\}^n$.

Therefore, the abstract object for this cryptographic process consists of the following functions[1]:

- $kGen(1^n) \rightarrow k \in \{0,1\}^n$

- $enc(m,k) \rightarrow c, \quad |m| = |k| = |c| = n$

- $dec(c,k) \rightarrow m \quad || \quad \perp$

The functional correctness is then defined as follows:
For all security parameter $n \in N$, for all messages m, for all keys $k \leftarrow kGen(1^n)$, for all keys $k \leftarrow kGen(m,k)$ and for all ciphertexts $c \leftarrow enc(m,k)$ applies $dec(c,k) = m$. That means that we must be able to decrypt all encrypted messages for all possible input parameters.

Security of Shannon's OTP

Independently of a bit m_i in the message m, the OTP flips this bit with the probability of $\frac{1}{2}$ creating a distribution of ciphtertexts c that is independent of the messages m. And because m and c are independent, it is intuitive that knowing c cannot reveal anything about m. We can also prove this mathematically because the probability for two independent events to take place is the product of the individual probabilities: $Pr[M = m|C = c] = \frac{Pr[M=m \wedge C=c]}{Pr[C=c]} = \frac{Pr[M=m] \cdot Pr[C=c]}{Pr[C=c]} = Pr[M = m]$.

---

[1] The symbol $\perp$ is indicating an error.

GLOSSARY

In this chapter, basic terms will be defined and explained.

3.1 KERCKHOFFS'S PRINCIPLE

Security should not require the system, but merely the key to be secret.

3.2 PERFECT SECURITY

A cryptographic process is perfectly secure if for all messages in the set of possibles messages $m \in M$ and all possibly producible ciphertexts $c \in C | Pr[C = c] > 0$ the probability that m occurs is equal no matter if the ciphertext is known or unknown: $Pr[M = m] = Pr[M = m|C = c]$. More simply put, this means that an attacker cannot gain any knowledge about the message when seeing its ciphertext regardless of the message's and the ciphertext's concrete values.

3.3 CONDITIONAL PROBABILITY

Conditional probability $Pr[A = a|B = b]$ is the probability that the event $a \in A$ occurs if it is already known that the event $b \in B$ occurs. It is calculated as $Pr[A = a|B = b] = \frac{Pr[A=a] \wedge Pr[B=b]]}{Pr[B=b]}$. An example is a probability rolling a 6-sided dice results in the number 6 if it is already known that the result is an even number: $Pr[is6|iseven] = \frac{Pr[is6] \wedge Pr[iseven]}{iseven} = \frac{\frac{1}{6}}{\frac{1}{2}} = \frac{1}{3}$.

Perfect security can only be reached for processes with deterministic a decryption function if the key space is at least as big as the message space $|K| \geq |M|$. This is because then a given ciphtertext c could be decrypted to $|K|$ different messages m (determinism), which minimizes the search space for an attacker from $|M|$ possibilities to $|K|$ possibilities and therefore also decrease the attacker's uncertainty..

Completely hiding the length of a message is impossible if the length of possible messages is unlimited. Hiding messages' lengths would require changing their length for transmission. The message length cannot be decreased because this would result in data loss. Therefore, messages would have to be increased up to the maximum message size to make all appear to have the same length. If the message size is unlimited, we cannot expand messages to that nonexisting limit.

3.5   INSECURITY OF SHIFT-CIPHERS

Shift-ciphers, like Ceasar, are not perfectly secure, which can be shown by contraposition: If the possible messages are defined as $M = aa, ab$, a shift cipher shifting each character by some number of characters in an alphabet would always create ciphertexts as follows $Dec(aa) \rightarrow c_0c0$ and $Dec(ab) \rightarrow c_0c_1 \quad | \quad c_0 \neq c_1$ Therefore, an attackers probability when seeing the ciphertexts to guess the correct message $m \in M$ is equal to 1 and greater than the initial probability, which was $\frac{1}{2}$. A concrete example would be: $Pr[M = aa|C = c_0c_0] = 1 \neq Pr[M = aa] = \frac{1}{2}$. We see that limiting the set of possible messages can be a helpful method for contradictions of perfect correctness.