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

1 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.

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

3 GLOSSARY

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