Solutions: Sheet 2

1. Protection Goals (II)

In a simple communication model, Alice and Bob exchange messages over an insecure channel. Mallory acts as man-in-the-middle, as shown in figure 1.

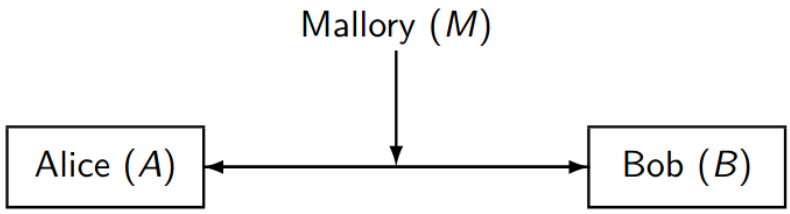

Figure 1: Communication Model

(a) Name and briefly describe three different attacks on three different protection goals that Mallory could carry out and explicitly state which protection goal is violated with the respective attack.

- Listen to the communication $\rightarrow$ Confidentiality
- Cut the line $\rightarrow$ Availability
- Manipulate the communication $\rightarrow$ Integrity

(b) Name for each protection goals a cryptographic method that is suitable for the implementation of this protection goal.

- Listen to the communication $\rightarrow$ Encrypt message e.g via PGP, authentication methods like passwords, access control (different right, roles, ...)
- Cut the line $\rightarrow$ Redundancy, e.g backup line, more servers
- Manipulate the communication $\rightarrow$ Hash functions, digital signatures

2. Protection Goals (III)

(a) Explain the protection goals of "message authenticity" and "non-repudiation". What is their delimitation? Are there any dependencies between the two protection goals?

- **message authenticity:** Means that when sending a message the sender can be clearly identified by the recipient and it can be proven that the sender is the author of this massage. $\rightarrow$ Integrity
- **non-repudiation:** Means that a creator of a data cannot deny that he created it.

message authenticity --/--> non-repudiation

non-repudiation -----> message authenticity ???

(b) Name a cryptographic method to achieve the security objective of non-repudiation.

- Digital signatures

3. Protection Goals for Data Protection

Research the two protection goals “anonymity” and "pseudonymity" and state their definition. Explain their difference using an example.

- Anonymity means that no one can draw conclusions about the identity of a person in any way → an online chat without registration
- Pseudonymity means that the identity of a person is not known, but certain actions or information may allow conclusions to be drawn about the identity of a person by a certain group. (assignment rule, pseudonym to identity) → an online chat with registration

4. Safety vs. Security

Research the difference between the two security related terms "security" and "safety" and give their definitions. Explain their difference using an example.

- Saftey means to protect you from the consequences of natural actions, e.g measures to minimize consequences natural catastrophes.
- Security means to protect you from the consequences of unauthorized actions, e.g place police patrols in places where crimes often occur.

5. CAESAR Cipher

The ciphertext `LIPPS` was encrypted with a CAESAR cipher. Which of the following three words is the corresponding plaintext? Justify your answer without trying.

- `MAGIC`
- `HELLO` → it always shifts by the same number, so the two P's in the middle must also be two equal letters when you decode it. `k = 4`
- `SALUT`

6. Skytale

The Spartan military leader Lysander received the following message from his generals during the Peloponnesian War: `AHMLTEOYTERMANROCEORKMWNBYEIYTANTORG`

Unfortunately he had forgotten his Skytale. However, he was still able to decrypt the message. Explain how he did it and determine the message.

```
A T T A C K B Y T
H E E N E M Y T O
M O R R O W E A R
L Y M O R N I N G
```

`ATTACK BY THE ENEMY TOMORROW EARLY MORNING`