Introduction to IT-Security WS 20/21

Exercise 01

Daniel Tschertkow & Eggert Jung

November 19, 2020

GITZ Kennung:	y0058800	**GITZ Kennung:**	y0085044
Matrikelnr.:	4200606	**Matrikelnr.:**	4839284
Studiengang:	Informatik Bachelor	**Studiengang:**	IST Bachelor
Prüfungsordnung:	BPO2015	**Prüfungsordnung:**	5

1 Security goals

a)

Concerning her home, Alice might have the following security goals which Mallory violated by physically breaking in:

- **Confidentiality**: Mallory might have stolen *private data*, like a love letter, which is now at risk of being disclosed.
- **Integrity**: Mallory might have manipulated a number of things in Alice's home, like the router configuration or the fire alarm. Depending on Mallory's intentions all things (including *private* and *valuable* data) inside her home and Alice's life itself might be at risk.
- **Availibility**: Some of Alice's things, like household appliances or jewelry, might be missing.

b)

- Alice could have *prevented* the breaking by having a stronger door, a better lock, or a guard outside her home. She also could have kept the location of her home private.
- Alice could have had alarms inplace to *detect* the break-in when it was happening and intervene.
- Additionally, Alice might have have had security cameras which might have captured the break-in for later *analysis* to prevent break-ins in the future.

2 Simple combinatorics

3 XOR cipher

A few requirements must be satisfied in order to get hold of the K and the M_1:

- M_2 must be longer than M_1 or K, so that the key can be calculated in at least the needed length.
- A successfully decoded message must be distinguishable from an unsuccessfully decoded message, so that the cipher texts C_x and C_y can be exchanged if necessary.

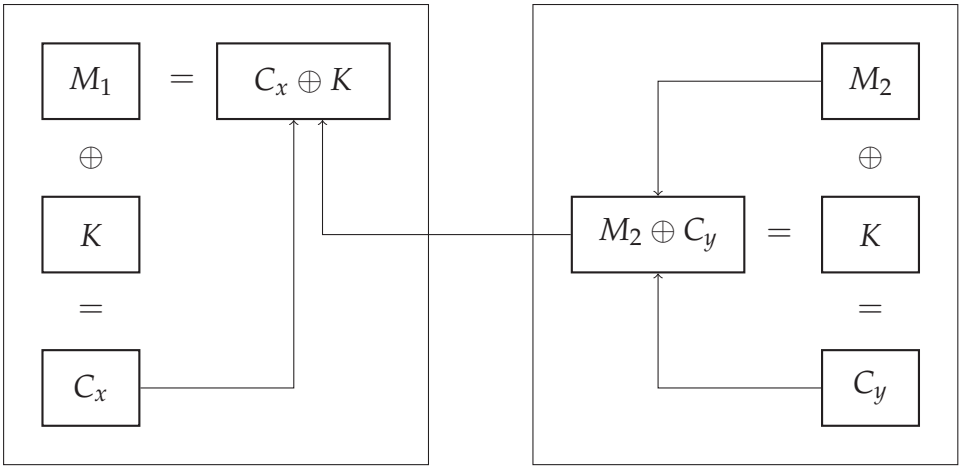

Figure 1: This Diagram shows how an attacker can calculate the key K and the message M_1. C_x, C_y and M_2 are known to the attacker.