



Technische
Universität
Braunschweig

Introduction to IT-Security WS 20/21

Exercise 01

Daniel Tschertkow & Eggert Jung

November 19, 2020

GIT'Z Kennung: y0058800
Matrikelnr.: 4200606
Studiengang: Informatik Bachelor
Prüfungsordnung: BPO2015

GIT'Z Kennung: y0085044
Matrikelnr.: 4839284
Studiengang: IST Bachelor
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.
- **Availability:** 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 in place to *detect* the break-in when it was happening and intervene.
- Additionally, Alice might have had security cameras which might have captured the break-in for later *analysis* to prevent break-ins in the future.

2 Simple combinatorics

Let $\mathbb{K}$ be the keyspace K the key.

a) ROT13

ROT13 is the shift of an alphabet by 13 letters. Thereby it's a special case of the *caesar* cipher (shift of an alphabet by k letters). Thus 13 is the key and $|\mathbb{K}| = 1$.

b) Vigenère Cipher

Let k be the length of the chosen alphabet. Let $|K| = n$. Thus $\mathbb{K} = k^n$.

c) 256 bit AES

$\mathbb{K} = 2^{256}$.

d) monoalphabetic substitution cipher

We assume that k is the length of the alphabet. Thus $K = k!$.

3 XOR cipher

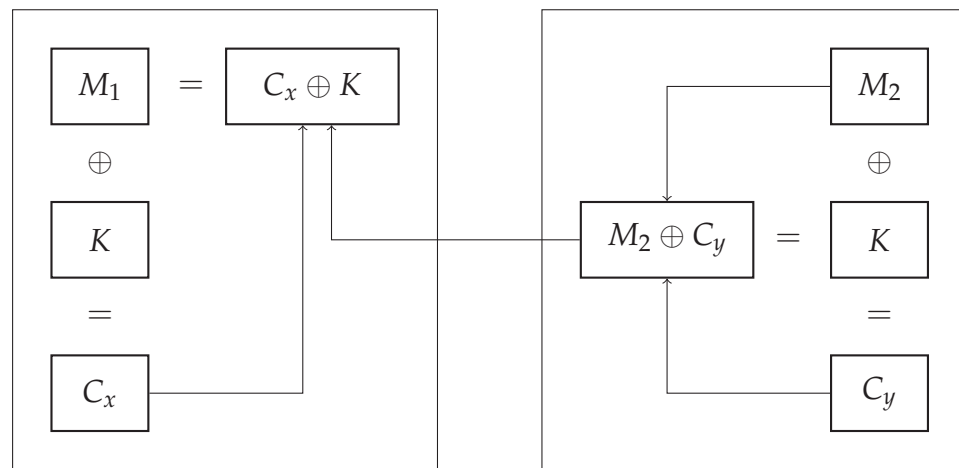


Figure 1: This Diagram shows how an attacker can calculate the key K and the message M_1 . C_x , C_y and M_2 are known to the attacker.

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.