Joud Mawad (Matrikelnummer: 5377552)

Luis Jair Gutierrez Pacheco (Matrikelnummer: 5453416)

Security goals

(a) Possible violated security goals

- Confidentiality: The attacker may have read private documents, letters, photos or looked through her computer.
- Integrity: Items could have been modified or damaged, like something in documents.
- Availability: Objects might have been stolen or left unusable, like the attacker formated the hard disk of her laptop.

(b) Security mechanisms from different classes

- prevention: security door, bars on windows, a safe for valuable items.
- detection: Alarm system, surveillance cameras.
- Analysis: evaluating the damage after the break in would help to understand what happened and help with recovery.

Simple combinatorics

(a) ROT13

ROT13 uses a fixed rotation of 13 positions. So the key space consists of exactly one elerment.

(b) Vigenère cipher with known key length n

If the alphabet consists of 26 letter. Each of the n key positions can be chosen independently from 26 possibilities so it would be 26^n.

(c) AES with a 256 bit key

An AES 256 key has length of 256 bits. Each bit can be 0 or 1, independently, so it would be 2^{256}

(d) Monoalphabetic substitution cipher with k letters

A monoalphabetic substitution over an alphabet of size k is a permutation of these k letters. so it would be k! and if the alphabet consists of 26 letters it would be 26!.

XOR

Alice sends two ciphertexts using the same XOR key k, so in other words:

$$c_0 = m_0 \oplus k, \qquad c_1 = m_1 \oplus k,$$

and Eve captures c_0 and c_1. Eve knows that one of the plaintexts m is either m_0 or m_1.

How can Eve recover the other plaintext message?

First we look at:

$$c_0 \oplus c_1 \;=\; (m_0 \oplus k) \oplus (m_1 \oplus k) \;=\; m_0 \oplus m_1,$$

and that is because $k \oplus k = 0$.

If Eve correctly guesses one plaintext (let's say m_0), she can compute the other as:

$$m_1 \;=\; m_0 \oplus (m_0 \oplus m_1) \;=\; m_0 \oplus (c_0 \oplus c_1).$$

The same goes for m1. So once one plaintext is known, the other plaintext is easy to derive without knowing the key k.

Can Eve also recover the exact key k used by Alice?

If she knows that c_0 encrypts m_0, then she can also do:

$$k = c_0 \oplus m_0.$$

So:

- With only c_0 and c_1 but she does't know which plaintext was sent, then she cannot know the correct key.
- As soon as she knows one correct plaintext/ciphertext pair (maybe from guissing), she can compute k and then decrypt any other ciphertext encrypted with the same key.