Introduction to IT-Security WS 20/21

Exercise 01

Daniel Tschertkow & Eggert Jung

November 20, 2020

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

1 Security goals

2 Simple combinatorics

3 XOR cipher

Following the rule $a \oplus b = c \Leftrightarrow b = a \oplus c$ these calculations can be made:

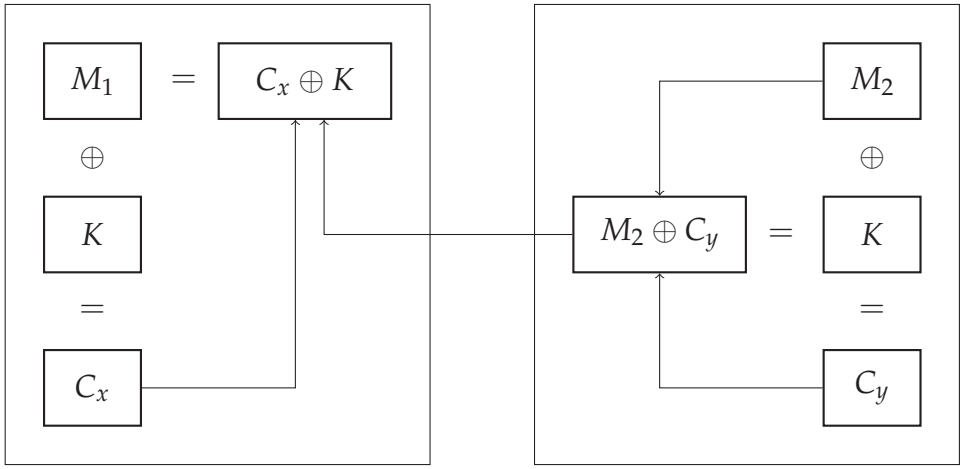

Figure 1: This Diagram shows how an attacker can calculate the key K and the message M_1. C_x, C_y and M_2 are known to the attacker.

A few requirements must be satisfied in order to get hold of K and 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.