



Technische
Universität
Braunschweig

Introduction to IT-Security WS 20/21

Exercise 01

Daniel Tschertkow & Eggert Jung

November 18, 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

2 Simple combinatorics

3 XOR cipher

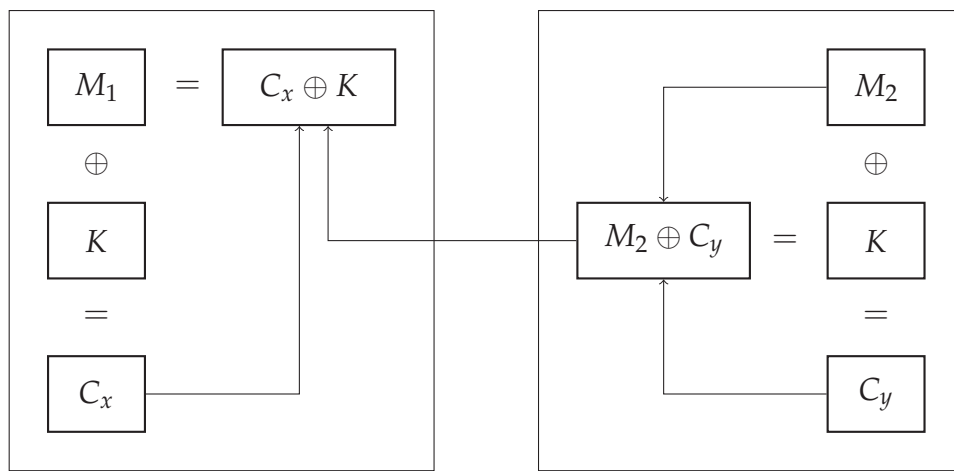


Figure 1: This Diagram shows how an Attacker can calculate the Key K and the Message M_1 .

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.