Grundlagen der Kryptographie

Prof. Dr. Christoph Saatjohann

14.10.2024 - 28.10.2024

1 Aufgabe 1: Substitutionschiffren

1.1 Implementierung eines Substitutions-Knacker

In der Vorlesung wurden Substitutions-Chifferen und ein Angriff mittels Buchstaben-Frequenz-Analyse dagegen vorgestellt. Implementieren Sie einen entsprechenden Angriff (z.B. in Python oder C).

Bitte verzichten Sie hierbei auf zuviele if/else Kombinationen, sondern nutzen eine andere Methode.
Tipp: Sie können davon ausgehen dass alle Texte die Sie entschlüsseln möchten in deutscher Sprache sind und nur aus Großbuchstaben bestehen. Sonderzeichen wurden NICHT verschlüsselt.

1.2 Entschlüsseln der Nachricht

Sie haben folgende geheime Nachricht abgefangen und möchten diese gerne entschlüsseln. Streng nach dem Kerckhoffs'sche Prinzip hat der Sender der Nachricht Ihnen erklärt dass er eine Substitutionschiffre nutzt, möchte Ihnen aber natürlich nicht das Passwort geben.

Probieren Sie mit Ihrer Implementierung die Nachricht zu entschlüsseln. Falls das nicht funktionieren sollte, erläutern Sie warum und nutzen Sie eine andere Möglichkeit, bspw. das in der Vorlesung gezeigte CryptTool.

```
VPY YPLNPN GE GQFPN CJYKS UFKSN JUC VLUC?
PG LGN CPY ZFNPY WLN GPLUPW HLUC;
PY SFN CPU HUFDPU VESO LU CPW FYW,
PY IFGGN LSU GLKSPY, PY SFPON LSU VFYW.

WPLU GESU, VFG DLYBGN CJ GE DFUB CPLU BPGLKSN?
GLPSGN ZFNPY, CJ CPU PYOHEPULB ULKSN?
CPU PYOPUHEPULB WLN HYEU JUC GKSVPLI?
WPLU GESU, PG LGN PLU UPDPOGNYPLI.

CJ OLPDPG HLUC, HEWW, BPS WLN WLY!
```

```
BFY GKSEPUP GQLPOP GQLPO LKS WLN CLY;
WFUKS DJUNP DOJWPU GLUC FU CPW GNYFUC,
WPLUP WJNNPY SFN WFUKS BJPOCPU BPVFUC.
```

2 Aufgabe 2: Modulare Arithmetik

2.1 Berechnen Sie folgende Gleichungen per Hand:

- $15 * 29 \mod 13$
- $2 * 29 \mod 13$
- $2 * 3 \mod 13$
- $-11 * 3 \mod 13$
- $1/5 \mod 13$
- $1/5 \mod 7$
- $3 * 2/5 \mod 7$

2.2 Restklassenringe Z_m

Wir betrachten die Restklassenringe Z_5 (Modulus = 5) und Z_6 (Modulus = 6).

- Berechnen Sie die Additions- und Multiplikationstabellen für beide Restklassenringe.
- Welche Elemente in Z_5 und Z_6 haben keine multiplikative Inversen?
- Warum haben alle Elemente, außer 0, in Z_5 eine multiplikative Inverse?

Beispiel Additionstabelle für Z_4:

+	0	1	2	3
0	0	2	3	3
1	1	2	3	.
2	2	.	.	.
3	.	.	.	.

Table 1: Additionstabelle Z_4