
Kryptologie, Kryptographie: *die Lehre von der Geheimschrift*

Ziel der Kryptologie: geheime Kommunikation (Diplomatie, Militär, persönliche Beziehungen, Online-Banking etc.)

1. Transpositions-Chiffren: DI IHT ISNEE ET GIX SE EMT

Idee: Die Nachricht kräftig durchschütteln!

Genauer: Die Buchstaben des Textes werden nach einem geheimen Muster neu angeordnet.

Begriffserklärung:

- Transposition = Vertauschung
- Chiffrierung = Verschlüsselung

Eine mögliche Transpositions-Chiffre könnte folgendermaßen aussehen:

- Wähle eine Zahl m.
- Schreibe den Klartext in Zeilen mit je m Buchstaben.
- Fülle die letzte Zeile beliebig auf.
- Geheiminformation = Spaltenlänge, d.h. die Anzahl der Buchstaben pro Spalte
- Geheimtext = die Buchstaben spaltenweise geschrieben

Beispiel:

Zeilenlänge: 3 Buchstaben

Klartext: BALD SIND FERIEN $\rightsquigarrow$

B	A	L
D	S	I
N	D	F
E	R	I
E	N	J

Geheiminformation: 5 Buchstaben pro Spalte

Geheimtext: BDNEEASDRNLIFIJ

Entschlüsselung dieser Transpositions-Chiffre:

- benötigte Geheiminformation: Spaltenlänge n (eine Zahl)
- Teile den Geheimtext fortlaufend in Gruppen von n Buchstaben auf.
- Schreibe die Gruppen spaltenweise nebeneinander.
- Klartext: die Buchstaben zeilenweise gelesen

Aufgabe: Entschlüssele den Text ganz oben! Geheiminformation: Spaltenlänge 5.

Anordnungsmöglichkeiten für einen Text aus n Buchstaben: $n! = 1 \cdot 2 \cdot \ldots \cdot n$ ("n-Fakultät")

Beispiel ganz oben: 20 Buchstaben, also 20! Anordnungsmöglichkeiten

Wieviel ist das ungefähr? Stirling'sche Formel: $n! \approx \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n$

Im Fall $n = 20$: $20! \approx \sqrt{40\pi} \cdot \left(\frac{20}{e}\right)^{20} \approx \sqrt{120} \cdot 10^{20}$, da $\pi \approx 3$ und $e \approx 2$ (sehr grob!)

$\approx 11 \cdot 10^{20}$ (stimmt bis auf einen Faktor von 452)

2. Monoalphabetische Chiffrierung: JRON UHMKO AYMH HYN

Idee: Ersetze das Alphabet *ABCD...* durch ein Geheimalphabet *SXUF...* durch festgelegte Vertauschung aller Buchstaben.

Methode der Schlüsselwörter:

- Wähle ein Wort ohne mehrfache Buchstaben (= Schlüsselwort).
- Wähle einen Buchstaben des Alphabets (= Geheimbuchstabe).
- Schreibe das gewöhnliche Alphabet komplett in eine Zeile.
- Schreibe das Schlüsselwort in die Zeile darunter. Beginne unter dem Geheimbuchstaben.
- Fülle die zweite Zeile mit den noch fehlenden Buchstaben des Alphabets in ihrer üblichen Reihenfolge auf. Beginne dabei rechts vom Schlüsselwort und springe am Ende der Zeile zurück an ihren Anfang.

Beispiel: Schlüsselwort = James Bond

Geheimbuchstabe = G

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	J	A	M	E	S	B	O	N	D	C	F	G	H	I	K	L	P	Q	R	T

Aufgabe: Entschlüssele den Text ganz oben!

Beobachtungen:

- Jeder Buchstabe wird immer gleich verschlüsselt (mono = eins).
- Daher sind monoalphabetische Chiffrierungen statistisch leicht zu knacken.

Relative Häufigkeit der Buchstaben im Deutschen:

E	17,4%
N	9,8%
I	7,6%
S	7,3%
R	7,0%
⋮	
Q	0,02%

3. Polyalphabetische Chiffrierung: HFYHZ EYDY?

Idee: Jeder Buchstabe kann auf verschiedene Weisen verschlüsselt werden (poly = viele).

Ziel: Verschleierung der statistischen Häufigkeiten

Beispiel: die Vigenère-Verschlüsselung

- Lege ein Codewort fest.
- Schreibe das Codewort fortlaufend über den Klartext.
- Verschlüsselung von $\begin{array}{|c|}\hline X \\ \hline Y \\ \hline \end{array}$ zum Buchstaben in Zeile X und Spalte Y des Vigenère-Quadrats.

Aufgabe: Verschlüssele das Wort *Quadrat* mit dem Codewort *Kreis* nach der Vigenère-Methode.

K	R	E	I	S	K	R
Q	U	A	D	R	A	T

wird zum Geheimtext

A	L	E	L	J	K	K

Beobachtungen:

- Der Buchstabe A wird einmal zu E und einmal zu K verschlüsselt.
- Die Buchstaben U und D werden beide zu L verschlüsselt.
- Der Buchstabe T und das zweite A werden beide zu K verschlüsselt.

Dechiffrierung des Geheimtextes:

- Schreibe das Codewort fortlaufend über den Geheimtext.
- Für die Entschlüsselung von $\begin{array}{|c|}\hline X \\ \hline Y \\ \hline \end{array}$ betrachte Zeile X im Vigenère-Quadrat, suche darin den Buchstaben Y und entschlüssele zum Buchstaben der zugehörigen Spalte.

Aufgabe: Entschlüssele den Geheimtext am Anfang des Abschnitts mit dem Codewort *Hund*!

H	U	N	D	H	U	N	D	H
H	F	Y	H	Z	E	Y	D	Y

wird zu

A	L	L	E	S	K	L	A	R

Beobachtungen:

- Der Buchstabe H wird einmal zu A und einmal zu E entschlüsselt.
- Der Buchstabe F und das erste Y werden beide zu L entschlüsselt.

Erklärung:

- Die Buchstaben werden mit verschiedenen Geheimalphabeten ver- und entschlüsselt.
- Der jeweils oben stehende Buchstabe entscheidet, welches Geheimalphabet das ist.

4. Das RSA-Verfahren:

- entwickelt 1977 durch **R**ivest, **S**hamir und **A**dleman
- eines der sichersten Verfahren, die wir heute kennen
- die Verschlüsselung beruht auf der Verwendung von Primzahlen

Primzahl: eine natürliche Zahl $p \geq 2$, die nur durch 1 und sich selbst teilbar ist

Beispiele: 2, 3, 5, 7, 11, 13, ...

Wissenswertes über Primzahlen:

- Jede natürliche Zahl ist ein Produkt von Primzahlen (eindeutige Primfaktorzerlegung).
- Es gibt unendlich viele Primzahlen, aber nur endlich viele sind derzeit bekannt.
- Die größte derzeit bekannte Primzahl ist $2^{74.207.281} - 1$ (ca. 22 Millionen Stellen).

Grundidee: Heutige Computer brauchen zu lange, um die Primfaktorzerlegung einer großen Zahl zu finden!

Wie funktioniert das RSA-Verfahren?

1. Schlüsselerzeugung:

- Wähle zwei verschiedene Primzahlen p und q.
- Berechne $n = p \cdot q$ und $n' = (p-1) \cdot (q-1)$.
- Wähle eine beliebige zu n' teilerfremde Zahl e.
- Veröffentliche e und n auf Deiner Homepage (*öffentlicher Schlüssel*).
- Halte p und q geheim (*geheimer Schlüssel*).

2. Verschlüsselung:

- Wandle den Klartext in eine Zahl $m < n$ um (z.B. mit Hilfe von ASCII: A = 01000001).
- Eventuell muss man dafür den Klartext in Portionen aufteilen.
- Berechne m^e und teile mit Rest durch n.
- Geheimtext = der entstandene Rest r

3. Entschlüsselung:

- Wenn man p und q kennt, kann man leicht eine Zahl d berechnen, sodass $e \cdot d - 1$ durch $n' = (p-1) \cdot (q-1)$ teilbar ist.
- Ist r der Geheimtext, so berechne r^d und teile mit Rest durch n.
- Man kann zeigen, dass dieser Rest gerade m ist!
- Nun wandle m mit Hilfe von ASCII wieder in Text um.

kleines Zahlenbeispiel:

- $p = 3$ und $q = 5$
- $n = p \cdot q = 3 \cdot 5 = 15$ und $n' = (p-1) \cdot (q-1) = (3-1) \cdot (5-1) = 8$
- $e = 7$ ist teilerfremd zu $n' = 8$
- $d = 7$ erfüllt $e \cdot d - 1 = 7 \cdot 7 - 1 = 48$, ist also durch $n' = 8$ teilbar

Beobachtungen:

- Es gibt zwei Schlüssel: Die Information (e, n) ist öffentlich und wird zum verschlüsseln gebraucht. Einen Text *verschlüsseln* kann also jeder.
- Die Information (p, q) ist nur Dir bekannt und wird zum *entschlüsseln* gebraucht. Nur Du kannst n' und d berechnen und damit einen Text entschlüsseln.
- In diesem Sinne ist das RSA-Verfahren asymmetrisch.
- Zwar ist n öffentlich zugänglich, aber heutige Computer sind zu langsam, um daraus die geheimen Informationen p und q zu berechnen. Dafür genügt es schon, dass die Primzahlen p und q jeweils etwa 100 Stellen haben.

Literaturempfehlung:

A. Beutelspacher, *Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*, 10. Auflage, Springer Spektrum, 2015