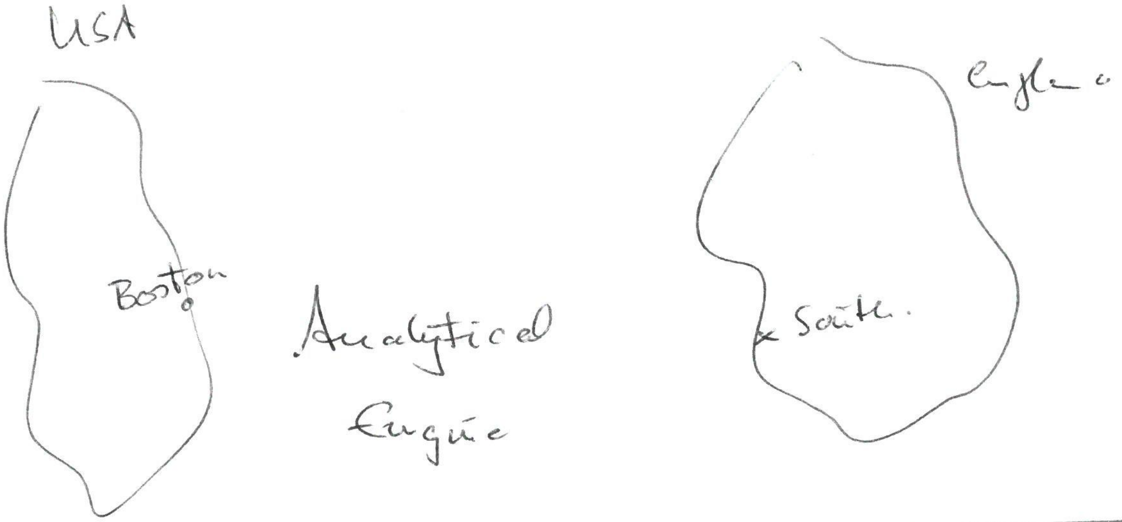
Die Vigenère - Chiffre

Eine wesentliche Eigenschaft der Shift- und Affinen Chiffre ist, dass durch die Wahl eines Schlüssels K jedes Klartextzeichen auf genau ein Chiffretextzeichen abgebildet wird, oder: das Klartextalphabet wird genau auf ein Chiffretext-Alphabet abgebildet. → monoalphabetische Chiffre.

Folge: Die statistischen Eigenschaften des Klartexts werden auf den Chiffretext übertragen.

→ Polyalphabetische Chiffren. Vigenère - Chiffre (1586).

Charles Babbage 1791 - 1871



Def: Sei m eine positive ganze Zahl und

$$M = C = K = (\mathbb{Z}_{26})^m$$

$$\underbrace{\mathbb{Z}_{26} \times \mathbb{Z}_{26} \times \ldots \times \mathbb{Z}_{26}}_{m \text{ Kopien.}}$$

Für einen Schlüssel $\vec{k} = (k_1, \dots, k_m)$ ist die Verschlüsselung eine Abb.

$$V_k : \mathbb{Z}_{26}^m \to \mathbb{Z}_{26}^m$$

$$\vec{x} \mapsto \vec{y} = [(x_1 + k_1) \bmod 26, (x_2 + k_2) \bmod 26, \dots, (x_m + k_m) \bmod 26]$$

Dech.

$$V_k^{-1} : \mathbb{Z}_{26}^m \to \mathbb{Z}_{26}^m$$

$$\vec{x} = (\vec{y} - \vec{k}) \bmod 26 = [(y_1 - k_1) \bmod 26, \dots, (y_m - k_m) \bmod 26].$$

Beispiel: Wähle ein Schlüsselwort, z. B.

$\underbrace{\text{jamesbond}}_{m=9}$.

↓ Zahlen

$(9\ 0\ 12\ 4\ 18\ 1\ 14\ 13\ 3) = \vec{k}$

Klartext: treffenummitternacht

t	r	e	f	f	e	n	u	m	m	i	t	t	e	r	n	a	c	h	t
19	17	4	5	5	4	13	20	12	12	8	19	19	4	17	13	0	2	7	19
9	0	12	4	18	1	14	13	3	9	0	12	4	18	1	14	13	3	9	0

2 17 16 9 23 5 1 7 15 21 8 5 23 22 18 1 13 5 16 19

C R Q J X F B H P V I F X W S B N F Q T

9 = Länge des Schlüssels.

Größe des Schlüsselraums: $|K| = 26^m$

$m = 5$ $\quad 26^5$ Möglichkeiten $\approx 1{,}2 \cdot 10^7$ Schlüssel

---

Die Hill-Chiffre (Lester S. Hill, 1929)

Beispiel:

① Festlegung des Schlüssels.

Man wählt eine Zahl, z.B. $n = 3$. Der Schlüssel dieses Verfahrens ist eine $n \times n$-Matrix M mit Einträgen von Zahlen mod 26.

z.B.

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}$$

[Es muss gelten

$\operatorname{ggT}[\det M, 26] = 1$]

② Verschlüsselung:

Klartext wird in Blöcke der Länge n aufgeteilt

berlin

$\rightarrow$ 1 4 17 11 8 13

Blockweise Verschlüsselung

$$(1\ 4\ 17) \circ M = (1\ 4\ 17) \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}$$

$$= (1 + 4 \cdot 4 + 17 \cdot 11,\ 2 + 20 + 17 \cdot 9,\ 3 + 24 + 17 \cdot 8)$$

$$= (204\ \ 175\ \ 163) \bmod 26$$

$$\equiv (22\ \ 19\ \ 7)$$

$$(11\ \ 8\ \ 13) \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \equiv (4\ \ 23\ \ 3)$$

berlin $\longrightarrow$ 22 19 7 4 23 3

$\longrightarrow$ W T H E X D

3 Entschlüsselung

Gesucht ist die zu M inverse Matrix, die wir N nennen, diese erfüllt:

$$M \circ N \equiv \mathbb{1}_{3\times 3} \bmod 26.$$

$$\mathbb{1}_{3\times 3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\det M = \det \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}$$

$$= 1 \cdot 5 \cdot 8 + 2 \cdot 6 \cdot 11 + 3 \cdot 4 \cdot 9$$

$$- 3 \cdot 5 \cdot 11 - 2 \cdot 4 \cdot 8 - 1 \cdot 6 \cdot 9 \quad \bmod 26$$

$$= 40 + 132 + 108 - 165 - 64 - 54$$

$$\equiv -3 \equiv 23$$

$$M^{-1} = N = 23^{-1} \cdot \begin{pmatrix} -14 & 11 & -3 \\ 34 & -25 & 6 \\ -19 & 13 & -3 \end{pmatrix}$$

$$23^{-1} \bmod 26 \equiv 17 \bmod 26$$

$$N = \begin{pmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{pmatrix}$$

Gesucht: x mit $23 \cdot x \equiv 1 \bmod 26$

$$23 \cdot 17 = 340 + 51 = 391$$

$$391 = 390 + 1$$

$$= 15 \cdot 26 + 1$$

$$\Rightarrow 23 \cdot 17 \equiv 1 \bmod 26$$

Die HILL-Chiffre hat die Eigenschaft der <u>Diffusion</u>, d.h. die Änderung ~~des~~ eines Zeichens des Klartexts hat zur Folge, dass mehrere Chiffrezeichen geändert werden.

Bsp. $(a\ a\ b) \rightarrow 0\ 0\ 1$

$$\rightarrow (0\ 0\ 1) \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}$$

$$\doteq (11 \quad 9 \quad 8) \to \underline{\underline{LjI}}$$

$$(a\,b\,b) \to 0\ 1\ 1$$

$$\to (0\ 1\ 1) \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}$$

$$\to (15 \quad 14 \quad 14) \to \underline{\underline{POO}}$$

$$(b\,a\,b) \to (1\ 0\ 1) \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}$$

$$\to (12 \quad 11 \quad 11) \Rightarrow \underline{\underline{MLL}}$$

Es gibt noch viele weitere klassische Verschlüsselungsverfahren, Ende der Fahnenstange für polyalphabetische Verschlüsselungen sind die sog. <u>Rotormaschinen</u>.

z. B. Enigma, Purple, Lorenz-Schreiber, ...

Schlüssel der Enigma:

- Anfangsstellung der 3 Rotoren
- welcher Rotor in welchem Slot
- Welche Buchstabenpaare werden durch das Steckbrett vertauscht?

1) 3 Rotoren à 26 Positionen $\hat{=}$ 26^3 Möglichkeiten

$= 17\,576$

Rotorstellungen.

2) $\binom{5}{3}$ Auswahlmöglichkeiten 3 versch. Walzen aus 5er Set auswählen

$= 10$ Möglichkeiten.

$3! = 6$ Einschubmöglichkeiten

$\rightsquigarrow$ $60 \cdot 17576$ Möglichkeiten

$= 1\,054\,560$ "

3) Hier wird's astronomisch.

Angenommen, man vertauscht 5 Buchstabenpaare

A → F (F → A)

E → L (L → E)

G → Z (Z → G)

M → P (P → M)

R → X (X → R)

1. Paar: $\binom{26}{2}$ Möglichkeiten

2. " $\binom{24}{2}$ "

5 Paaren: $\frac{1}{5!} \binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}$ Möglich.

$= 295\,269\,975$ Möglichkeiten

1) + 2) + 3) ergibt

3,113,799,048,360 000

Möglichkeiten!

Mathematische Grundlagen

Algebraische Strukturen

Betrachte eine Menge, z.B.

$$\mathbb{N} = \text{Menge der natürlichen Zahlen}$$
$$= \{0, 1, 2, \ldots\}$$

oder

$$\mathbb{Z} = \text{Menge der ganzen Zahlen}$$
$$= \{\ldots, -3, -2, -1, 0, 1, 2, \ldots\}$$

Unter einer algebraischen Struktur versteht man eine Menge M zusammen mit einer oder mehreren Operationen, die auf M definiert ist/sind.

Halbgruppen

Eine Halbgruppe ist ein Paar $(M, \circ)$, wobei M eine nichtleere Menge ist und $\circ$ ist eine auf M definierte binäre Abbildung,

$$\circ : M \times M \to M,$$ M ist abgeschlossen unter $\circ$

die assoziativ ist.

d.h. $a \circ (b \circ c) = (a \circ b) \circ c$ Assoziativgesetz

Beispiele

$(\mathbb{N}, +)$ ist Halbgruppe, $a + b \in \mathbb{N}$

$a + (b + c) = (a + b) + c$

$(\mathbb{N}, \times)$ ist ebenfalls Halbgruppe

$(\mathbb{N}, -)$ ist keine Halbgruppe ($\mathbb{N}$ ist nicht abgeschlossen, da: im allg. $a - b \notin \mathbb{N}$)

oder: $\Sigma = \{0, 1\}$, $\Sigma^* = \{0, 1\}^*$

= alle Bitstrings

$= \{\lambda, 0, 1, 00, 01, 10, 11, \ldots\}$

$\circ : \Sigma^* \times \Sigma^* \to \Sigma^*$

abgeschlossen, $w_1 \circ (w_2 \circ w_3) =$

$(w_1 \circ w_2) \circ w_3$

es gibt ein neutrales Element λ (leeres Wort)

mit $w \circ \lambda = w \quad \forall w \in \Sigma^*$

$\to$ Monoid.

Gruppe:

Eine Gruppe ist eine Halbgruppe $(M, \circ)$ mit folgenden zusätzlichen Eigenschaften

1) Es existiert ein neutrales Element $1_M \in M$ mit

$$a \circ 1_M = a \quad \forall a \in M;$$

2) $\forall a \in M \; \exists a^{-1} \in M$ (das Inverse von a)

und
$$a \circ a^{-1} = \mathbb{1}_M \quad \forall a \in M.$$

Wenn die Operation $\circ$ kommutativ ist,
$$a \circ b = b \circ a,$$
dann ist $(M, \circ)$ eine ABELsche (oder kommutative) Gruppe.

<u>Beispiele</u>: — $(\mathbb{Z}, +)$ ist eine ABELsche Gruppe,

neutrales Element: $0 \in \mathbb{Z}$

und für jedes $a \in \mathbb{Z}$ existiert das $(-a)$

und
$$a + (-a) = 0.$$

— $(\mathbb{Z} \setminus \{0\}, \times)$ ist keine Gruppe, weil

Neutr. 1 $\quad a \cdot 1 = a \quad \forall a \in \mathbb{Z}$.

$$5 \cdot x = 1 \;\Rightarrow\; x = \frac{1}{5}, \; x \notin \mathbb{Z}$$

$\rightarrow$ es gibt i.a. kein multipl. Inverses.

— $(\mathbb{Q} \setminus \{0\}, \times)$ ist eine Gruppe.

— Die Menge der Shift-Chiffren unter der Operation "Hintereinander-Ausführung" bildet eine Gruppe.

Eine weitere Struktur hat die Menge $\mathbb{Z}$ als Vorlage; auf $\mathbb{Z}$ sind zwei binäre Operationen definiert, nämlich $+$ und $\times$.

<u>Definition</u>:

Ein Ring ist ein Tripel $(A, +, \times)$ mit:

1) $(A, +)$ ist eine ABELsche Gruppe

2) $\times$ ist assoziativ

$$a \times (b \times c) = (a \times b) \times c$$

3) Es gelten die <u>Distributivgesetze</u>

$$a \times (b + c) = a \times b + a \times c$$

$$(a + b) \times c = a \times c + b \times c.$$

<u>Beispiele</u>

- $(\mathbb{Z}, +, \times)$

- Die Menge der Polynome in x mit Koeffizienten in einem Körper (kommt gleich) bilden einen Ring, das ist der <u>Polynomring</u>.

$$f(x) = x^3 + x^2 + 1$$

$$g(x) = x + 1$$

$$\begin{aligned} f(x) \times g(x) &= (x^3 + x^2 + 1)(x + 1) \\ &= x^4 + x^3 + x + x^3 + x^2 + 1 \\ &= x^4 + x + 1 \qquad (\text{über } \mathbb{Z}_2) \end{aligned}$$

Definition (wichtigste Struktur) $[(\mathbb{R}, +, \times)]$

Ein Körper (engl. field) ist eine nichtleere Menge A mit zwei binären Operationen $+$ und $\times$. Es gelten die folgenden Axiome:

A1 Assoziativgesetze

$\forall a, b, c \in A$:

$$a + (b + c) = (a + b) + c$$
$$a \times (b \times c) = (a \times b) \times c$$

A2 Kommutativgesetze

$\forall a, b \in A$: $\quad a + b = b + a$

$$a \times b = b \times a$$

A3 Distributivgesetze

$\forall a, b, c \in A$:

$$a \times (b + c) = a \times b + a \times c$$
$$(a + b) \times c = a \times c + b \times c$$

A4 Neutrale Elemente

$\forall a \in A \quad \exists\, 0_A \in A$ mit

$$a + 0_A = a$$

$\forall a \in A \quad \exists\, 1_A \in A$ mit

$$a \times 1_A = a$$

A5 Inverse Elemente

$\forall a \in A \quad \exists\, -a \in A$ mit

$$a + (-a) = 0_A \qquad \text{(additives Inverses)}$$

$\forall a \in A \setminus \{0\} \; \exists\, a^{-1} \in A$ mit $\quad a \cdot a^{-1} = 1_A$

$\boxed{a^{-1}}$ heisst MULTIPLIKATIVES INVERSES

Beispiele:

$(\mathbb{R}, +, \times)$ ist ein (unendlicher) Körper

$(\mathbb{Q}, +, \times)$ „ „ — „ — „

$(\mathbb{C}, +, \times)$ „ „ „ „

$\mathbb{Z}$: $-3 \; -2 \; -1, 0, 1, 2, 3 \ldots$

5. 3. 1. 2. 4 6.

In der Kryptographie spielen sogenannte <u>endliche Körper</u> eine dominante Rolle,

Galois-Felder.

z. B. $\left(\mathbb{Z}_p, (a+b) \bmod p, (a \times b) \bmod p\right)$

$\uparrow$

Primzahl.

$\mathbb{Z}_5, \; (a+b) \bmod 5, \; (a \times b) \bmod 5$

$\{0, \ldots, 4\}, \quad \mathbb{Z}_2 = \{0, 1\}$

Einige elementare Eigenschaften von Zahlen

Definition:

Eine Zahl $b \neq 0$ heisst Teiler von $a \in \mathbb{Z}$ (oder umgekehrt, a heisst Vielfaches von b), falls

$$a = m \cdot b, \quad m \in \mathbb{Z}.$$

oder: b teilt die Zahl a ohne Rest:

$$b \mid a$$

Bsp: $a = 24$, Teiler von a: $1, 2, 3, 4, 6, 8, 12, 24$

Es gilt (einfach zu zeigen mit $a = m \cdot b$)

- Wenn $a \mid 1 \Rightarrow a = \pm 1$
- Wenn $a \mid b$ und $b \mid a \Rightarrow a = \pm b$
- Jedes $b \neq 0$ ist Teiler von 0
- Wenn $b \mid g$ und $b \mid h \Rightarrow b \mid (m \cdot g + n \cdot h)$

Anmerkung: Es gibt sog. perfekte Zahlen, das sind Zahlen, die als Summe ihrer echten Teiler geschrieben werden können.

$$6 = 1 + 2 + 3$$

$$28 = 1 + 2 + 4 + 7 + 14$$

$$496 =$$

$$8128 \quad \text{---}$$

$$33\,550\,336 \quad \text{----}$$

Offenes Problem: Gibt es ungerade perfekte Zahlen?