

Grundlagen:

1. Gruppen

Eine Gruppe $G(M, O, +)$ ist eine Menge von Elementen und einer Verknüpfung \circ , welche folgende Eigenschaften erfüllt:

1. Es existiert ein **neutrales Element O** : $\forall a \in M: O + a = a$
 (Ein Element ohne Auswirkung auf das Ergebnis: $8+0=8$)

2. Es existiert ein **inverses Element $-x$** : $\forall a \in M \exists -a \in M: -a + a = O = a + (-a)$
 (Ein Element, bei welchem das neutrale Element als Ergebnis herauskommt)

3. Die Gruppe ist **abgeschlossen**: $\forall a, b \in M: a + b \in M$
 (Das Ergebnis jeder Operation muss wieder ein Element der Gruppe sein)

4. Die Operationen sind **assoziativ**: $\forall a, b, c \in M: a + (b + c) \stackrel{?}{=} (a + b) + c$
 (Die Reihenfolge von Operationen muss egal sein)

Wenn die Gruppe **abelsch** ist, muss außerdem gelten:

5. Die Operationen sind **kommutativ**: $\forall a, b \in M: a + b = b + a$
 (Die Reihenfolge von Elementen in einer Operation muss egal sein)

2. Ringe

Ein Ring $R(M, O, +, \cdot)$ erweitert eine Gruppe um eine weitere Operation (meist Multiplikation).

3. Körper

Ein Körper $K(M, O, +, \cdot)$ ist die Erweiterung eines **abelschen** Rings, welche folgendes hinzufügt:

6. Es existiert ein **multiplikatives inverses Element x^{-1}** : $\forall a \in M \exists a^{-1} \in M: a^{-1} \cdot a = 1$
 (Ein Element, bei welchem das neutrale Element als Ergebnis herauskommt)

Ein Körper mit $0-255$ Elementen kann man mit einer Primzahl p und einer natürlichen Zahl m darstellen als: $p^m \Rightarrow 2^8$

Wenn $m = 1$ ist der Körper ein **Primkörper**.

Wenn $m > 1$ ist der Körper ein **Erweiterungskörper**.

Charakteristik: Die Charakteristik $\text{char}(K)$ ist die kleinste Zahl $n \in \mathbb{N}$ für die gilt: $n \cdot 1 = 0$

Bsp: $\text{char}(\mathbb{Z}_7) = 7$, da $7 \cdot 1 = 0 \pmod 7$

Kardinalität: Die Kardinalität $\text{card}(K)$ ist die Anzahl der Elemente eines Körpers.

Bsp: $\text{card}(\mathbb{Z}_7) = 0, 1, 2, 3, 4, 5, 6 = 7$

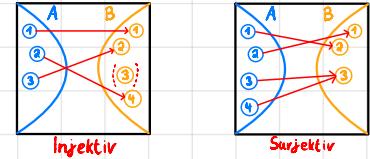
4. Endliche Körper

Ein endlicher Körper K ist ein Körper mit $\text{card}(K) < \infty$.

Charakteristik: Die kleinste Primzahl der Primfaktorzerlegung ist die Charakteristik eines endlichen Körpers.

Isomorphie: Zwei Strukturen A, B sind isomorph, wenn gilt:

A ist bijektiv (injektiv + surjektiv) zu B



Division: Nach dem Lemma von Bézout lässt sich in einem Körper K_n eine Division mit dem multiplikativen Inversen durchführen:

$$\mathbb{F}_{79}: 7 \div 40 \Rightarrow \text{ggT}(79, 40) = 2 \cdot 40 - 79 = 7 \cdot 2 = 14$$

Fundamentalsatz der Arithmetik: Für $N > 1$ gibt es eindeutige Primfaktorzerlegung.

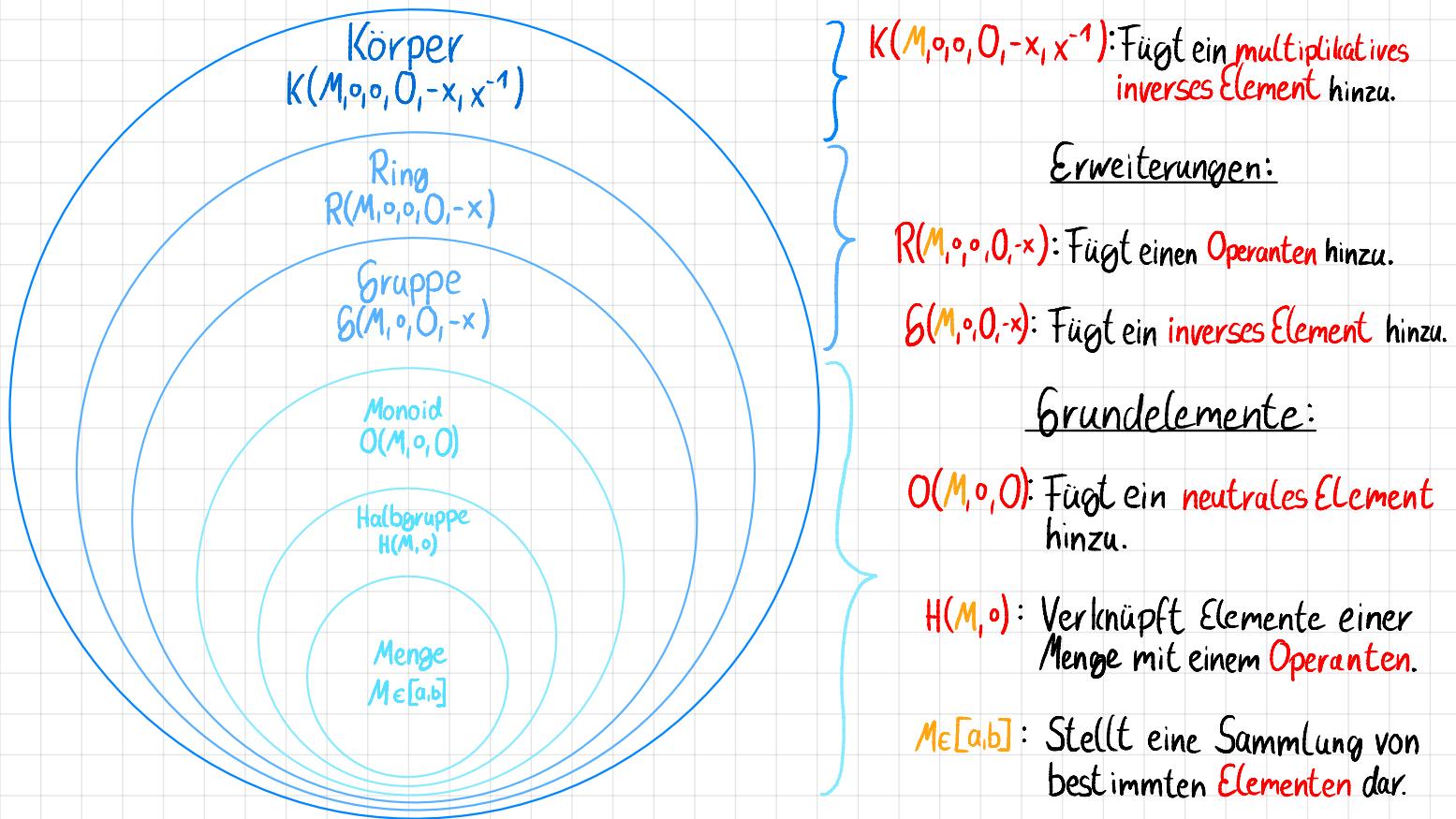
Bei einem endlichen Körper K mit $\text{char}(K) = p$ und q Elementen gilt:

$$q = p^l \quad \text{für } l \in \mathbb{N} \quad \Rightarrow \quad \mathbb{F}_q$$

So kann \mathbb{F}_q als \mathbb{F}_{p^l} geschrieben werden.

Eulersche φ -Funktion: Für alle $n \in \mathbb{N} > 1$: $\varphi(n) := \text{card}(\mathbb{Z}_n^*) / |\mathbb{Z}_n^*|$

$$\varphi(6) = \frac{4,3,2,1}{\text{ggT}(6, n)-1} = 2$$



Satz von Euler: Es sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}_n^*$:

$a^{n(n)} \equiv 1 \pmod{n} \Rightarrow$ Ein multiplikatives Inverse hoch die Anzahl der Inversen in $\mathbb{Z}_n = 1$

Chinesischer Restsatz: Es existieren $a \in \mathbb{Z}_n$ und $b \in \mathbb{Z}_m$ mit $m, n \in \mathbb{N}$; $\text{ggT}(m, n) = 1$, so gilt:

Es gibt ein $x \in \mathbb{Z}_{m \cdot n}$ mit $m \cdot a \equiv x \equiv n \cdot b$

Bsp: $x \equiv 5 \pmod{7}$
 $x \equiv 3 \pmod{4}$

$$4 \cdot x_1 \equiv 1 \pmod{7} \Rightarrow x_1 \equiv 2$$

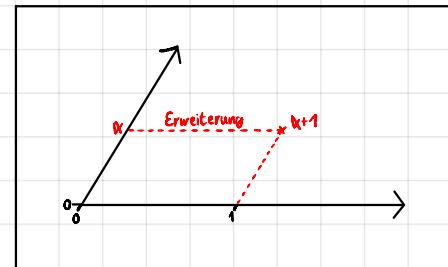
$$7 \cdot x_2 \equiv 1 \pmod{4} \Rightarrow x_2 \equiv 3$$

$$2 \cdot 5 \cdot 4 + 3 \cdot 3 \cdot 7 = 103 \pmod{7 \cdot 4} = \underline{\underline{19}}$$

5. Erweiterungskörper

In dem endlichen Körper \mathbb{F}_4 gibt es für den Wert 2 kein multiplikatives Inverse. Der Erweiterungskörper \mathbb{F}_{4^2} mit $\{0, 1, \alpha, \alpha+1\}$ hat weiterhin die Ordnung 4, erfüllt aber nun auch das multiplikative Inverse mit $\alpha \cdot (\alpha+1) = 1$

.	0	1	2	3	.	0	1	α	$\alpha+1$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	1	0	1	α	$\alpha+1$
2	0	2	0	2	α	0	α	$\alpha+1$	1
3	0	3	2	1	$\alpha+1$	0	$\alpha+1$	1	α
					\mathbb{F}_4				



Relationen: Eine Körpererweiterung vom Grad L ist nur mittels einer Relation möglich:

$$\alpha^L = r_0 + r_1 \cdot \alpha + r_2 \cdot \alpha^2 + \dots + r_{L-1} \cdot \alpha^{L-1} \xrightarrow{\text{zu B}} \mathbb{F}_3: \alpha^3 = \alpha^2 + 1$$

Diese kann einen Körper definieren.

Rechnung: Gegeben ist \mathbb{F}_8 mit $\alpha^3 = \alpha^2 + 1$:

1. Addition/Multiplikation:

$$\begin{aligned} & \alpha^3 \cdot (\alpha^2 + \alpha + 1) \\ &= \alpha^6 + \alpha^4 + \alpha^3 \\ &= \cancel{\alpha^3} \cdot \alpha^3 + \alpha^3 \cdot \alpha + \alpha^3 \\ &= \alpha \cdot (\alpha^2 + 1) + \alpha^2 + 1 \\ &= 1 \end{aligned}$$

2. Division:

$$\begin{aligned} & 1 : (\alpha + 1) \\ &= \alpha^3 : \alpha^3 \\ &= \alpha^0 \\ &= \alpha^2 + \alpha \end{aligned}$$

Relationstabelle:

α^0	=	α^0
α^2	=	α^2
α^3	=	$\alpha + 1$
α^4	=	$\alpha^3 \cdot \alpha = \alpha^2 + \alpha$
α^5	=	$\alpha^4 \cdot \alpha = \alpha^3 + \alpha = \alpha + 1$
α^6	=	$\alpha^5 \cdot \alpha = \alpha^2 + 1$
α^7	=	$\alpha^6 \cdot \alpha = \alpha$
α^8	=	$\alpha^7 \cdot \alpha = \alpha$

Minimalpolynom: Ein Minimalpolynom ist eine Funktion, die eine definierende Relation in ein Polynom umwandelt, wenn es keine Polynome $g(x)$ und $h(x)$ min. Grad 1 gibt, für die gilt: $F(x) = g(x) \cdot h(x)$

$$F(x) = X^L - r_{L-1} \cdot X^{L-1} - r_{L-2} \cdot X^{L-2} - \dots - r_1 \cdot X - r_0 \in \mathbb{F}_p$$

Für $x^3 = x + 1$ gilt $F(x) = x^3 + x + 1$, da $F(0) = 1 \neq 0$; $F(1) = 1 \neq 0$ ✓

6. Elliptische Kurven

Kryptografische Verfahren brauchen komplexe mathematische Probleme, um einen Angriff mittels Hochleistungscomputern zu erschweren. Aus diesem Grund betrachtet man elliptische Kurven in beliebigen Körpern k .

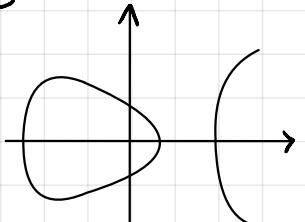
Definition: Elliptische Kurven sind eine Art von Polynomen in beliebigen Körpern k mit:

$$y^2 = x^3 + ax + b; \quad x, y \in k \text{ und } 4a^3 + 27b^2 \neq 0$$

$\Leftrightarrow F(x, y) = y^2 - x^3 - ax - b \bmod k \Rightarrow$ Tupel $(r, s) \in k^2$ ist nur ein Punkt, wenn k ein Quadrat und s eine Wurzel ist. $k > 3$

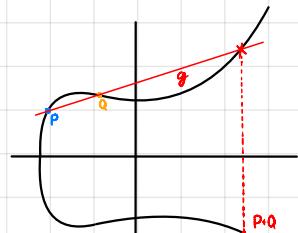
Jede Elliptische Kurve ist symmetrisch zur y -Achse:

$$E(r, s) = E(r, -s)$$



Rechnung: 1. Addition: $F(X, Y) = Y^2 - X^3 + 3X - 3$ ($a=10, b=3$) in \mathbb{F}_{11}
 $P(5, 3)$ und $Q(8, 6)$

1. Steigung von θ bestimmen:
 $m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{6-3}{8-5} = 1$

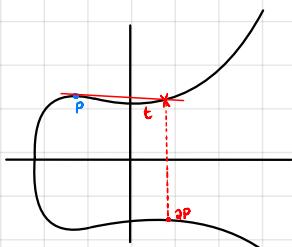


2. Schnittpunkt von θ und F bestimmen:
 $u = m^2 - x_1 \cdot x_2 = 1^2 - 5 \cdot 8 = 1$
 $v = m \cdot (u - x_1) + y_1 = 1 \cdot (1 - 5) - 3 = 12$

$$P+Q(u, -v) = P+Q(1, -12)$$

2. Verdopplung: $F(X, Y) = Y^2 + 18X^3 + 12X + 6$ ($a=7$) in \mathbb{F}_{19}
 $P(7, 5)$

1. Steigung von t bestimmen:
 $m = \frac{3 \cdot x_1^2 + a}{2 \cdot y_1} = \frac{3 \cdot 7^2 + 7}{2 \cdot 5} = \frac{1}{5} = 4$



2. Schnittpunkt von t und F bestimmen:
 $u = m^2 - 2 \cdot x_1 = 4^2 - 2 \cdot 7 = 2$
 $v = m \cdot (u - x_1) + y_1 = 4 \cdot (2 - 7) + 5 = 4$

$$2P(u, -v) = 2P(2, 15)$$

7. Punktmultiplikation:

Eine Multiplikation eines Punktes g und einer Zahl 5 bestimmt man mit:

$$5 \cdot 2^3 + 2^0 \hat{=} (101)_2 \Rightarrow L = 2 \quad \text{in } F(X, Y) = Y + XY + X^3 + aX + b$$

$$i=2: h_2 = g$$

$$i=1: \tilde{h}_1 = 2 \cdot h_2 = 2 \cdot g: \quad m: \frac{3 \cdot x_1^2 + a}{2 \cdot y_1}$$
$$\left. \begin{array}{l} u: m^2 - 2 \cdot x_1 \\ v: m \cdot (u - x_1) + y_1 \end{array} \right\} (u, v)$$
$$\tilde{h}_1 = 0 \Rightarrow h_1 = \tilde{h}_1$$

$$i=0: \tilde{h}_0 = 2 \cdot h_1: \quad m: \frac{3 \cdot x_0^2 + a}{2 \cdot y_0}$$
$$\left. \begin{array}{l} u: m^2 - 2 \cdot x_0 \\ v: m \cdot (u - x_0) + y_0 \end{array} \right\} (u, v)$$

$$\tilde{h}_0 = 1 \Rightarrow h_0 + g: \quad m: \frac{y_0 - y_1}{x_0 - x_1}$$
$$\left. \begin{array}{l} u: m^2 - x_0 - x_1 \\ v: m \cdot (u - x_0) - y_1 \end{array} \right\} (u, v)$$

$$h_0 = 5 \cdot g$$

8. Square and Multiply:

Für eine Zahl a^n kann man n in Binärfaktoren zerlegen:

- Bei $n[i] = 0$ quadriert man den Therm
- Bei $n[i] = 1$ quadriert man den Therm und multipliziert mit a

Bsp: $a^{37} \Rightarrow (100101)_2$

$$\begin{array}{ll} 1: & a \\ 0: & (a)^2 \\ 0: & ((a)^2)^2 \\ 1: & (((a)^2)^2)^2 \cdot a \\ 0: & (((((a)^2)^2)^2 \cdot a)^2)^2 \\ 1: & ((((((a)^2)^2)^2 \cdot a)^2)^2) \cdot a \end{array}$$

9. Satz von Lagrange:

Wenn für die zyklische Gruppe G eine Untergruppe H existiert gilt:

$|H|$ teilt die Gruppenkardinalität $|G|$

Bsp: Für \mathbb{Z}_{10}^* mit $|\mathbb{Z}_{10}^*| = 10 = 1 \cdot 2 \cdot 5$

\Rightarrow Die Untergruppen haben die Kardinalitäten: 1, 2, 5, 10

$$H_1 = \{1\} \quad \text{mit } \alpha = 1$$

$$H_2 = \{1, 10\} \quad \text{mit } \alpha = 10$$

$$H_3 = \{1, 3, 4, 5, 9\} \quad \text{mit } \alpha = 3, 4, 5, 9$$

10. ECDH (Elliptic Curve Diffie-Hellmann key exchange)

Vorbereitung:

- 1: Wähle eine Primzahl $p \neq 3$
 - ↳ Falls $p = 2$: $l > 1 \} q = p^l$
 - ↳ Falls $p > 3$: $l = 1 \} q = p$
- 2: Eine elliptische Kurve E über \mathbb{F}_q :
 - ↳ Falls $p = 2$: $F(X, Y) = Y^2 + XY + X^3 + aX^2 + b \in \mathbb{F}_q$
 - ↳ Falls $p > 3$: $F(X, Y) = Y^2 - X^3 - aX - b \in \mathbb{F}_q$
- 3: Wähle $g = (u, v) \in E$ mit $\text{ord}(g) = r$; wobei r eine Primzahl ist.
Die Untergruppe U mit $U_g = \langle g \rangle \subseteq E$

Schlüsselaustausch: 1: Alice wählt $k_{pr,A} = a \in \{2, \dots, r-1\}$

- 1: Alice wählt $k_{pr,A} = a \in \{2, \dots, r-1\}$
 - ↳ $k_{pub,A} = a \cdot g \in U$
 - ↳ Alice schickt $k_{pub,A}$ an Bob
- 2: Bob wählt $k_{pr,B} = b \in \{2, \dots, r-1\}$
 - ↳ $k_{pub,B} = b \cdot g \in U$
 - ↳ Bob wählt $k_{pub,B}$ an Alice

Schlüsselbestimmung: 1: Alice bestimmt $T_A = a \cdot k_{pub,B}$
2: Bob bestimmt $T_B = b \cdot k_{pub,A}$

11. Elliptische Kurven in Charakteristik 2

1. Addition: $F(X, Y) = Y^2 + XY + X^3 + aX^2 + bX \in \mathbb{F}_2$

1. Steigung bestimmen: $m = \frac{y_2 - y_1}{x_2 - x_1}$

2. Schnittpunkt bestimmen: $u = m^2 + m + a + x_1 + x_2$
 $v = m \cdot (x_1 + u) + u + y_1$

$P + Q(u, v)$

2. Verdopplung: $F(X, Y) = Y^2 + XY + X^3 + aX^2 + bX \in \mathbb{F}_2$ $P(x, y)$

1. Steigung bestimmen: $m = x_1 + \frac{y_1}{x_1}$

2. Schnittpunkt bestimmen: $u = m^2 + m + a$
 $v = m \cdot (x_1 + u) + u + y_1$

$2P(u, v)$

12. Primzahltests:

Höhe Primzahlen können nicht berechnet werden, sondern sind mit bestimmten Tests nur wahrscheinlich:

1. Probdivision: Eine Zahl n wird durch alle $k \in \{1, 2, \dots, n-1\}$ geteilt

→ Beim ersten gefundenen Teiler k wird aufgehört

2. Sieb des Erasthenes: Systematisches bestimmen von Primzahlen in einer Liste:

2	3	4	5	6	7	8	X	10	11
12	13	14	X	16	17	18	19	20	X
22	23	24	X	26	X	28	29	30	31
32	X	34	X	36	37	38	X	40	41

4. Fermat-Test: Eine ungerade Zahl n und eine Zahl a müssen für $a^{n-1} \bmod n = 1$ ergeben, damit eine Primzahl in Frage kommt:

$$n=17; a \in \{1, 2, \dots, n-1\} \wedge a^{n-1} \bmod n = 1$$

$$y = a^{n-1} \bmod n \begin{cases} \neq 1 \Rightarrow \text{Zusammengesetzt} \\ = 1 \Rightarrow \text{Kann eine Primzahl sein} \end{cases}$$

3. Miller-Rabin-Test: Eine ungerade Zahl $n > 3$ und eine Rundenzahl k ist mit der Wahrscheinlichkeit $\leq \frac{1}{4^k}$ nicht Prim, wenn:

$$n=289$$

$$n-1=288 = 2 \cdot 144$$

$$2 \cdot 2 \cdot 72$$

$$2 \cdot 2 \cdot 2 \cdot 36$$

$$2 \cdot 2 \cdot 2 \cdot 2 \cdot 18$$

$$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 9 = s=5; d=9$$

} Wir bestimmen s und d aus $n-1$.

$$a=131; 131^9 \bmod 289 = 158, \text{ da } \neq 1, -1$$

$$r=1: x=158^2 \bmod 289 = 110$$

$$r=2: x=110^2 \bmod 289 = 251$$

$$r=3: x=251^2 \bmod 289 = 288 \quad \checkmark$$

$$\Rightarrow a^{s+d} = 131^{2^3 \cdot 9} \text{ "wahrscheinlich Prim"}$$

1. Ein Zeuge a wird gewählt

2. Es wird $s-1$ mal: $x \equiv x^2 \bmod n$

3. Wenn ein Ergebnis 1 oder -1 ist, wird abgebrochen ⇒ "wahrsch. Prim"

(Nur ein falsches Ergebnis widerlegt Aussage)

(5. Das quadratische Sieb:)

6. Carmichael-Zahlen: Einige Zahlen sind zwar zusammengesetzt, werden jedoch nicht durch Primzahltests erkannt.

$$561 = 3 \cdot 11 \cdot 17$$

⇒ Diese nennt man Carmichaelzahlen/Pseudoprimezahlen.

13. Diskreter Logarithmus:

Diskretes Logarithmusproblem:

In einer zyklischen Gruppe $G(0, 0)$ betrachten wir $\alpha, \beta \in G$ und ein $x \in \mathbb{Z}$ mit $1 \leq x \leq \text{card}(G)$, sodass:

$$\beta = \alpha \circ \alpha \circ \dots \circ \alpha = \alpha^x$$

Einführung

1. Überblick

Grundlegende Frage: Ein **Sender A** (meist Alice) möchte einem **Empfänger B** (meist Bob) eine Nachricht senden. Ein **Angreifer C** (meist Catherine) versucht:

- 1: Die Nachricht zu lesen (passiver Angriff)
- 2: Die Nachricht zu verändern (aktiver Angriff)

Um solchen Angriffen entgegenzuwirken versucht man:

- 1: Zu verhindern, dass Daten korrekt interpretiert werden.
- 2: Sicherzustellen, das Manipulationen erkannt werden.

2. Caesar-Verschlüsselung

Die Verschlüsselung erfolgt durch eine Verschiebung jedes Buchstabens im Alphabet um eine vorgegebene Anzahl.

Alice: Klartext $m \Rightarrow$ Zahlenfolge (m_1, m_2, \dots, m_t)
 $n = [1, t]; k \in [1, 25]$
 $y = e_k(m_n) = m_n + k \bmod 26$

Bob: $y = (y_1, y_2, \dots, y_t)$
 $m_n = d_k(y_n) = y_n - k \bmod 26$

\Rightarrow Nur 25 mögliche Schlüssel.

Alice: 1: Schlüssel $k \in [1, 25] = 3$
2: Klartext $p = \boxed{H} \boxed{a} \boxed{L} \boxed{l} \boxed{o}$

H	a	l	l	o	\Rightarrow	7	0	11	11	14
					$\uparrow -3$	$\downarrow +3$				
k	d	o	o	r	\Leftarrow	10	3	14	14	17

Bob: 1: Chiffrat: $\boxed{k} \boxed{d} \boxed{o} \boxed{o} \boxed{r}$
2: Schlüssel: 3

3. Monoalphabetische Substitution

Die monoalphabetische Substitution ersetzt den Klartext durch eine vorgegebene Buchstabenfolge.

Alice: Klartext $m \Rightarrow$ Zahlenfolge (m_1, m_2, \dots, m_t)
Schlüssel $k = \sigma \in S_{26}; n = [1, t]$
 $y_n = e_k(m_n) = \sigma(m_n)$

Bob: $y = (y_1, y_2, \dots, y_t)$
 $m_n = d_k(y_n) = \sigma^{-1}(y_n)$

\Rightarrow Häufigkeitsverteilung der Buchstaben führen zur schnellen Entschlüsselung.

3. Vignére - Verschlüsselung

Die Verschlüsselung erfolgt durch ein sich immer wiederholendes Wort (Rhythmus)

Alice: Klartext $m \Rightarrow$ Zahlenfolge (m_1, m_2, \dots, m_t)
Schlüssel $k = \text{Wort}$; $n = [1, t]$; $i = n \bmod \text{len}(k)$
 $y_n = e_k(m_n) = m_n + k_i \bmod 26$

Bob: $y = (y_1, y_2, \dots, y_t)$
 $m_n = d_k(y_n) = y_n - k_i \bmod 26$

⇒ Unbrechbar bis Kasiskitest 1863

Alice: 1: Schlüssel $k = abc$
2: Klartext $p = \boxed{\text{H a l l o}}$

H	a	l	l	o	7	0	11	11	14
a	b	c	a	b	1	2	3	1	2
↓					i	c	o	m	a
↓					8	2	14	12	16

Bob: 1: Chiffra: $\boxed{i \ c \ o \ m \ a}$
2: Schlüssel: abc

4. Kasiski-Test

- Ermitteln der Schlüssellänge L durch einsetzen und Häufigkeitsanalyse. Marker wie N-Gramme können ebenfalls betrachtet werden.
- Den Vorgang nun auf alle weiteren Folgen bis L anwenden.

5. One-time Pad

Ein Schlüssel wird in der Länge des Klartextes generiert. Dieser muss:

- Wirklich zufällig generiert werden.
- Nur ein einziges mal verwendet werden.

Schwächen: - Schlüssellänge unpraktisch lang
- Wiederverwendung bricht gesamte Sicherheit

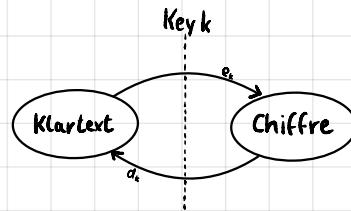
6. Ziele der Cyber Security

- Vertraulichkeit: Schutz gegen unrechtmäßigen Zugriff \Rightarrow Verschlüsselung
- Datenintegrität: Schutz gegen externe Änderungen \Rightarrow Authentisierung
- Verfügbarkeit: Schutz für größtmögliche Verfügbarkeit \Rightarrow Redundanz
- Nichtabstreitbarkeit: Schutz für legitime Herkunft \Rightarrow asymmetrische Kryptographie

Grundlagen der Kryptologie

1. Symmetrische Verschlüsselungsverfahren

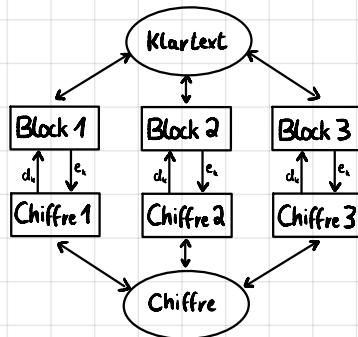
Symmetrische Verfahren benutzen einen Schlüssel k zum Ver- und Entschlüsseln. Die Verfahren sind schon eindeutig bestimmt und berechenbar.



Beispiele: Caesar- Verschlüsselung, monoalphabetische Substitution

2. Blockchiffrierung

Die Blockchiffrierung teilt einen Klartext in Blöcke der Länge r und verschlüsselt die einzelnen Blöcke nach einem eindeutigen Verfahren.

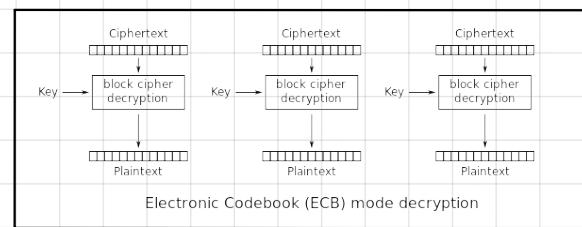


Beispiele: Vigenére - Verschlüsselung

ECB-Mode: Der electronic code book mode verschlüsselt Klartextblöcke unabhängig.

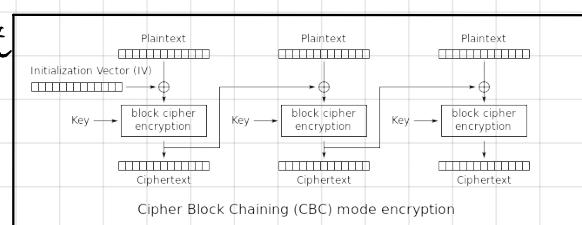
Alice: $\text{Klartext } m \Rightarrow m_1||m_2||\dots||m_t$
 $n = [1, t]$;
 $y_n = e(m_n)$

Bob: $m_n = d(y_n)$
 $m = m_1||m_2||\dots||m_t$



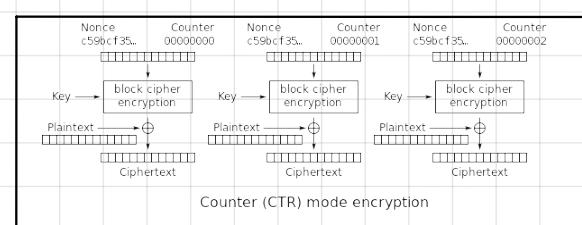
\Rightarrow Gleiche Texte werden gleich verschlüsselt (plaintext-ciphertext-attack)

CBC-Mode: Der cipher block chaining mode verketten Klartextblöcke, indem es den Cypherblock mit dem nächsten Klartextblock XOR'd.



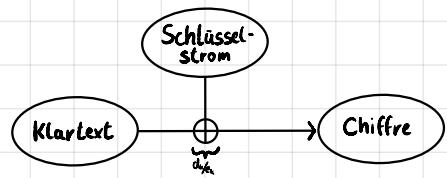
\Rightarrow Aufwendig, nicht parallelisierbar, Fehler zerstören nachfolgende Daten.

CTR-Mode: Der counter mode nutzt den Klartext nicht direkt zum verschlüsseln, sondern XOR'd ihn mit dem immer neuen init. Vector.



3. Stromchiffrierung

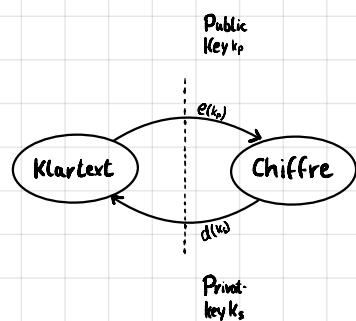
Die Stromchiffrierung teilt den Klartext nicht auf. Stattdessen wird dieser mit einem gleich langen Schlüsselstrom verrechnet.



Beispiele:

4. Assymmetrische Verschlüsselung

Assymmetrische Verfahren beruhen auf einem Schlüsselaustausch. Den öffentlichen Schlüssel können andere benutzen, um Daten zu verschlüsseln. Doch nur mit dem privaten Schlüssel kann man diese wieder entschlüsseln. Also gleicht der Verschlüsselungsalgorithmus nicht dem Entschlüsselungsalgorithmus.



Grundidee Schlüsselaustausch:

1. Alice und Bob einigen sich auf ein symmetrisches Verfahren.
2. Bob schickt Alice seinen key_{pub}
3. Alice wählt Sessionkey S und rechnet: $e_{k_{pub}}(S)$ und versendet ihn.
4. Bob entschlüsselt: $d_{k_{priv}}(S)$

5. Diffie-Hellmann Schlüsselaustausch:

Vorbereitung:

1: Alice und Bob wählen eine große Primzahl p und eine Gruppe $\mathbb{G}(\mathbb{F}_p)$

2: Alice und Bob wählen $g = (u, v) \in \mathbb{G}$ mit $\text{ord}(g) = r$; wobei r eine Primzahl ist oder einen Generator.

Schlüsselaustausch: 1: Alice wählt $k_{pr,A} = a \in \{2, \dots, r-1\}$

$$\downarrow k_{pub,A} = g^a \bmod p$$

↳ Alice schickt $k_{pub,A}$ an Bob

2: Bob wählt $k_{pr,B} = b \in \{2, \dots, r-1\}$

$$\downarrow k_{pub,B} = g^b \bmod p$$

↳ Bob schickt $k_{pub,B}$ an Alice

Schlüsselbestimmung: 1: Alice bestimmt $S = k_{pub,B}^{k_{pr,A}}$

2: Bob bestimmt $S = k_{pub,A}^{k_{pr,B}}$

5. RSA Verfahren: Gegeben: $K_{\text{pub}}(n, e)$ und Klartext x

- Schlüsselerzeugung:
- 1: Wähle zwei große Primzahlen p, q
 - 2: Berechne $n = p \cdot q$
 - 3: Berechne $\phi(n) = (p-1) \cdot (q-1)$
 - 4: Wähle öffentlichen exponenten $e \in [1; \phi(n)-1]$, sodass: $\text{ggT}(e, \phi(n)) = 1$
 - 5: Berechne $k_{\text{priv}} = d$ mit $(d \cdot e) \bmod \phi(n) = 1$

Verschlüsselung: $y = e_{k_{\text{pub}}}(x) \equiv x^e \bmod n$

Entschlüsselung: $x = y^d \bmod n$

Chinesischer Restsatz (Anwendung):

$$y_p \equiv y \bmod p$$

$$y_q \equiv y \bmod q$$

$$d_p \equiv d \bmod p$$

$$d_q \equiv d \bmod q$$

$$x_p \equiv y_p^{d_p} \bmod p$$

$$x_q \equiv y_q^{d_q} \bmod q$$

$$c_p = q^{-1} \bmod p$$

$$c_q = p^{-1} \bmod q$$

$$x = [q \cdot c_p] \cdot x_p + [p \cdot c_q] \cdot x_q \bmod n$$