Die Mathematik als Grundlage der Kryptographie

Joachim Rosenthal
Universität Zürich

Winterthur, 10. November, 2017.

Vortragsübersicht:

1. Historische Bemerkungen

2. Chiffrierungen mit geheimen Schlüsseln

3. Chiffrierungen mit öffentlichen Schlüsseln

4. Neue Mathematik für neue Kryptographie

Vortragsübersicht:

1. Historische Bemerkungen

2. Chiffrierungen mit geheimen Schlüsseln

3. Chiffrierungen mit öffentlichen Schlüsseln

4. Neue Mathematik für neue Kryptographie

1. Historische Bemerkungen

Caesar benützte einfache *monoalphabetische Verschlüsselungen*. Dazu identifiziere die Buchstaben mit der Menge $\mathbb{Z}_{26}$:

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
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Caesar benützte einfache *monoalphabetische Verschlüsselungen*. Dazu identifiziere die Buchstaben mit der Menge $\mathbb{Z}_{26}$:

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
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Eine Caesar Verschlüsselung hat dann die Form:

$$\begin{array}{rcl} \mathbb{Z}_{26} & \longrightarrow & \mathbb{Z}_{26} \\ x & \longmapsto & x+k \end{array}$$

wobei k der geheime Schlüssel ist, $1 \leq k \leq 25$.

Beispiel:

Caesar schickt seinen Generälen in Gallien die Meldung:
YWLPQNA WOPANET WJZ KXAHET DEY AP JQJY FQHEQO YWAOWN
Ein Test aller 25 Möglichkeiten ergibt sofort die Entschlüsselung:

Entschlüsselung

Verschlüsselung	Code
$x \mapsto x + 1$	ZXMQROB ...

Entschlüsselung

Verschlüsselung	Code
$x \mapsto x+1$	ZXMQROB ...
$x \mapsto x+2$	AYNRSPC ...

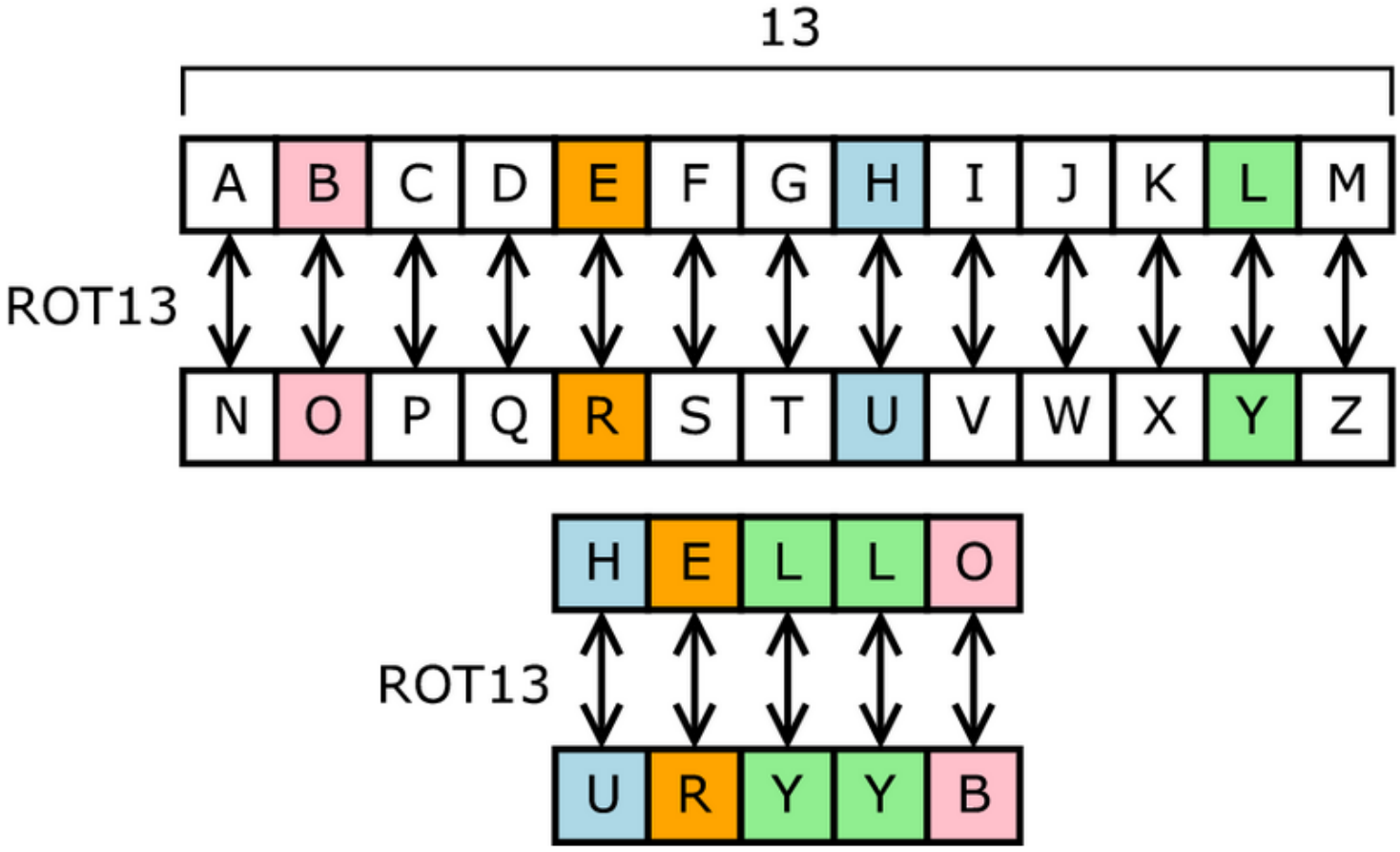
Entschlüsselung

Verschlüsselung	Code
$x \mapsto x+1$	ZXMQROB ...
$x \mapsto x+2$	AYNRSPC ...
$x \mapsto x+3$	BZOSTQD ...

Entschlüsselung

Verschlüsselung	Code
$x \mapsto x+1$	ZXMQROB ...
$x \mapsto x+2$	AYNRSPC ...
$x \mapsto x+3$	BZOSTQD ...
$x \mapsto x+4$	CAPTURE ASTERIX AND OBELIX
	HIC ET NUNC JULIUS CAESAR

Das Rot13 Verschiebechiffre System



Quelle: Wikipedia

3. Monoalphabetische Substitutionen

Anstatt eine Caesar-Verschiebung kann man beliebige Permutationen als Verschlüsselung angeben:

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

3. Monoalphabetische Substitutionen

Anstatt eine Caesar-Verschiebung kann man beliebige Permutationen als Verschlüsselung angeben:

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

Bemerkung: Es gibt

$$26! = 403'291'461'126'605'635'584'000'000$$

Möglichkeiten, dies sind 403 Quatrillionen verschiedene geheime Schlüssel. Kein Computer kann alle Schlüssel testen.

Frequenzanalyse

Kompliziertere monoalphabetische Verschlüsselungen können mittels Frequenzanalysen dechiffriert werden. Z.B. die sechs häufigsten Buchstaben in der Deutschen Sprache sind:

E	N	I	S	R	A
17,40%	9,78%	7,55%	7,27%	7,00%	6,51%

Frequenzanalyse

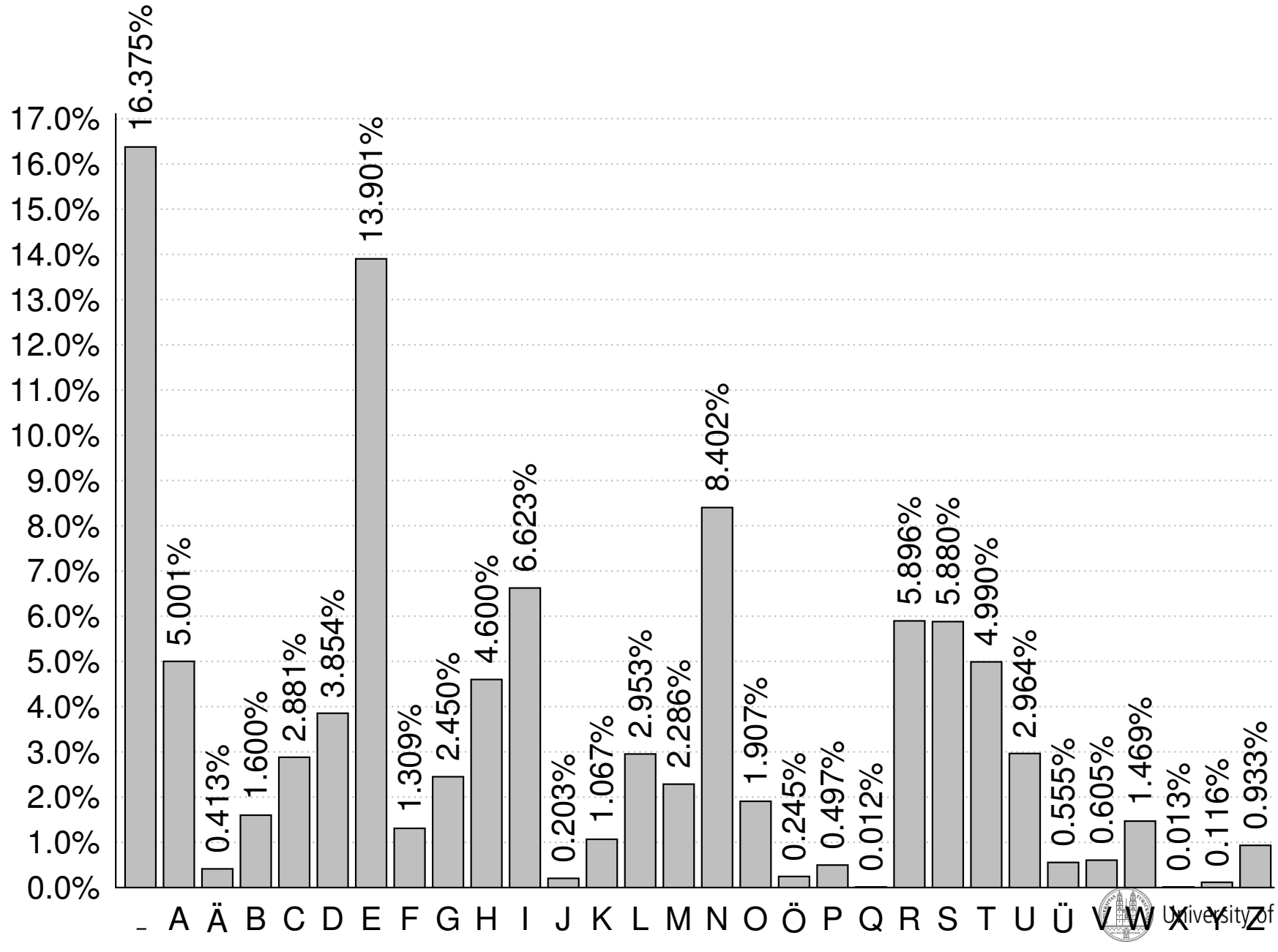
Kompliziertere monoalphabetische Verschlüsselungen können mittels Frequenzanalysen dechiffriert werden. Z.B. die sechs häufigsten Buchstaben in der Deutschen Sprache sind:

E	N	I	S	R	A
17,40%	9,78%	7,55%	7,27%	7,00%	6,51%

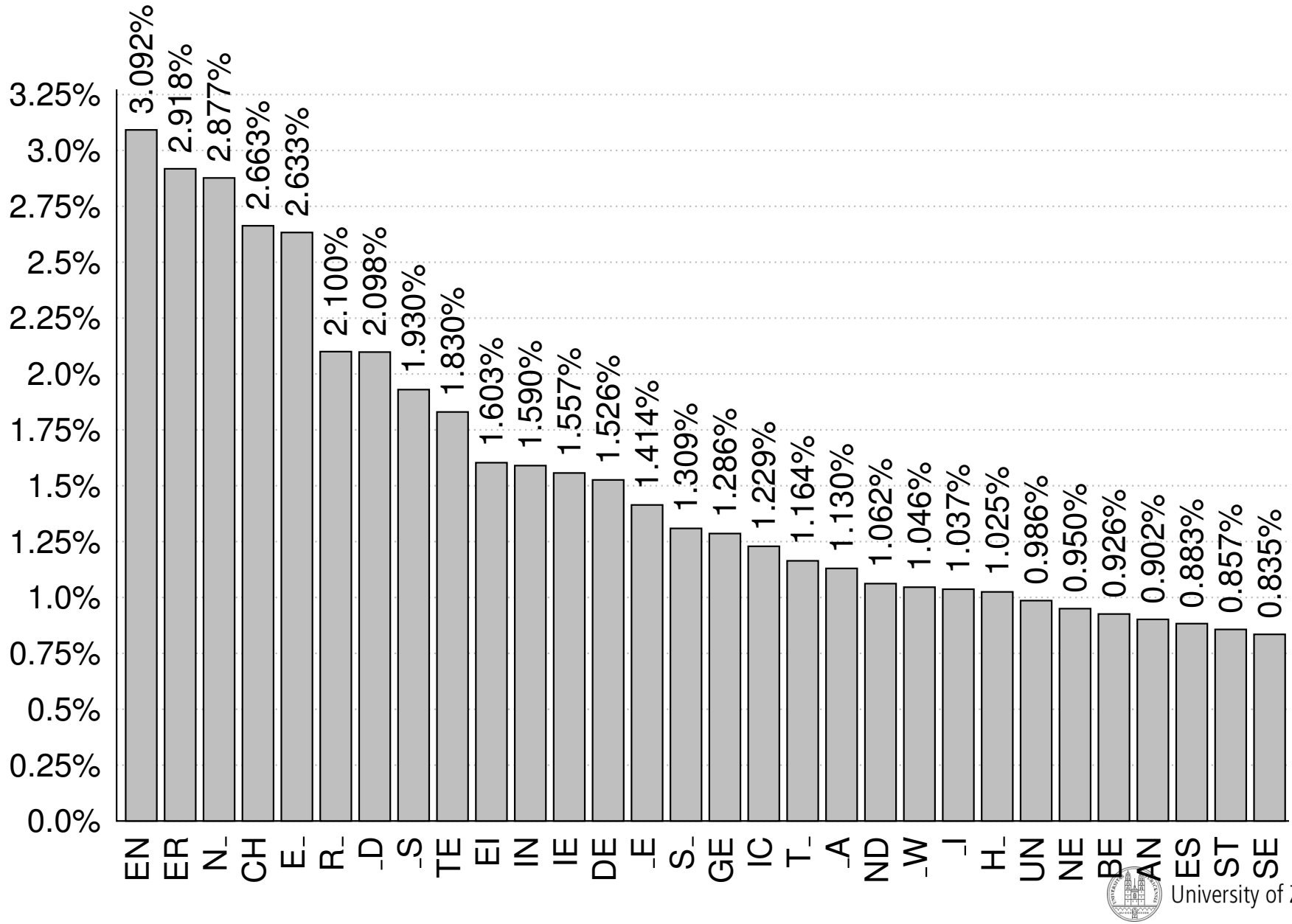
die sechs seltensten Buchstaben in der Deutschen Sprache sind:

P	V	J	Y	X	Q
0,79%	0,67%	0,27%	0,04%	0,03%	0,02%

Buchstabenhäufigkeit in der deutschen Sprache



Digrammhäufigkeit in der deutschen Sprache



Vigenère Chiffre

Im 17. Jahrhundert führte Vigenère eine Vektorversion der Caesar Verschlüsselung ein. Dazu betrachte die Abbildung:

$$(\mathbb{Z}_{26})^n \longrightarrow (\mathbb{Z}_{26})^n$$

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \longmapsto \begin{pmatrix} x_1 + k_1 \\ x_2 + k_2 \\ \vdots \\ x_n + k_n \end{pmatrix}$$

Vigenère Chiffre

Im 17. Jahrhundert führte Vigenère eine Vektorversion der Caesar Verschlüsselung ein. Dazu betrachte die Abbildung:

$$(\mathbb{Z}_{26})^n \longrightarrow (\mathbb{Z}_{26})^n$$

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \longmapsto \begin{pmatrix} x_1 + k_1 \\ x_2 + k_2 \\ \vdots \\ x_n + k_n \end{pmatrix}$$

Vigenère Chiffres können einfach mit Frequenzanalyse gebrochen werden.

Redundanz der Deutschen Sprache

Die Bcuhstbaenrehenifloge in eneim Wrot ist eagl
Ncah enier nueen Sutide, die uetnr aerdnem von der Cmabirdge Uinertvisy dührruchgeft wrdoen sien slol, ist es eagl, in wlehcer Rehenifloge Bcuhstbaen in eneim Wrot sethen, Huaptschae, der esrte und ltzete Bcuhstbae snid an der rhcitgien Setlle. Die rsetclhien Bshcuteban kenönn ttoal druchenianedr sien, und man knan es tortzedm onhe Poreblme lseen, wiel das mneschilhce Gherin nhcit jdeen Bcuhstbaen enizlen leist, snodren das Wrot als gnazes. Mti dme Pähonemn bchesfätgein shci mherere Hhcochsluen, acuh die aerichmkianse Uivnäseritt in Ptstbigurh. Esrtmlas üebr das Tmeha gchseibren hat aebr breteis 1976 - und nun in der rgchitien Bruecihhsetnafoelngbe - Graham Rawlinson in sieenr Dsiestraiton mit dem Tetil *The Significance of Letter Position in Word Recognition* an der egnlsicehn Uitneivrsy of Ntitongahm.

Hill Chiffre

Um Frequenzanalysen zu erschweren führte Lester S. Hill 1929 eine Chiffrierung mittels affin linearen Transformationen ein. Sei A eine invertierbare $n \times n$ Matrix mit Einträgen in $\mathbb{Z}_{26}$ und k ein n-dimensionaler Vektor: Die Chiffrierung ist dann mittels der Abbildung:

$$\begin{array}{ccc} (\mathbb{Z}_{26})^n & \longrightarrow & (\mathbb{Z}_{26})^n \\ x & \longmapsto & Ax + k = y. \end{array}$$

Hill Chiffre

Um Frequenzanalysen zu erschweren führte Lester S. Hill 1929 eine Chiffrierung mittels affin linearen Transformationen ein. Sei A eine invertierbare $n \times n$ Matrix mit Einträgen in $\mathbb{Z}_{26}$ und k ein n-dimensionaler Vektor: Die Chiffrierung ist dann mittels der Abbildung:

$$\begin{array}{ccc} (\mathbb{Z}_{26})^n & \longrightarrow & (\mathbb{Z}_{26})^n \\ x & \longmapsto & Ax + k = y. \end{array}$$

Hill Chiffres können mittels plaintext Angriffen entschlüsselt werden.

Beispiel eines Hill Chiffre

Alice und Bob benützen den Hill Chiffre:

$$\begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} \longmapsto \begin{bmatrix} 4 & 18 & 21 \\ 24 & 3 & 7 \\ 11 & 0 & 3 \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} + \begin{bmatrix} 11 \\ 0 \\ 20 \end{bmatrix}.$$

Beispiel eines Hill Chiffre

Alice und Bob benützen den Hill Chiffre:

$$\begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} \longmapsto \begin{bmatrix} 4 & 18 & 21 \\ 24 & 3 & 7 \\ 11 & 0 & 3 \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} + \begin{bmatrix} 11 \\ 0 \\ 20 \end{bmatrix}.$$

Alice schickt an Bob die Meldung:

$$\begin{bmatrix} 22 \\ 12 \\ 10 \end{bmatrix}, \begin{bmatrix} 16 \\ 12 \\ 20 \end{bmatrix}, \begin{bmatrix} 19 \\ 0 \\ 21 \end{bmatrix}, \begin{bmatrix} 11 \\ 9 \\ 19 \end{bmatrix}.$$

Beispiel Hill Chiffre

Bob benützt die folgende Formel um einen verschlüsselten Vektor $x := \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$ zu dechiffrieren:

Beispiel Hill Chiffre

Bob benützt die folgende Formel um einen verschlüsselten Vektor $x := \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$ zu dechiffrieren:

$$\begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} = A^{-1} \begin{bmatrix} x_1 - 11 \\ x_2 - 0 \\ x_3 - 20 \end{bmatrix}$$

Beispiel Hill Chiffre

Bob benützt die folgende Formel um einen verschlüsselten Vektor $x := \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$ zu dechiffrieren:

$$\begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} = A^{-1} \begin{bmatrix} x_1 - 11 \\ x_2 - 0 \\ x_3 - 20 \end{bmatrix}$$

Das Resultat für Bob ist:

Beispiel Hill Chiffre

Bob benützt die folgende Formel um einen verschlüsselten Vektor $x := \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$ zu dechiffrieren:

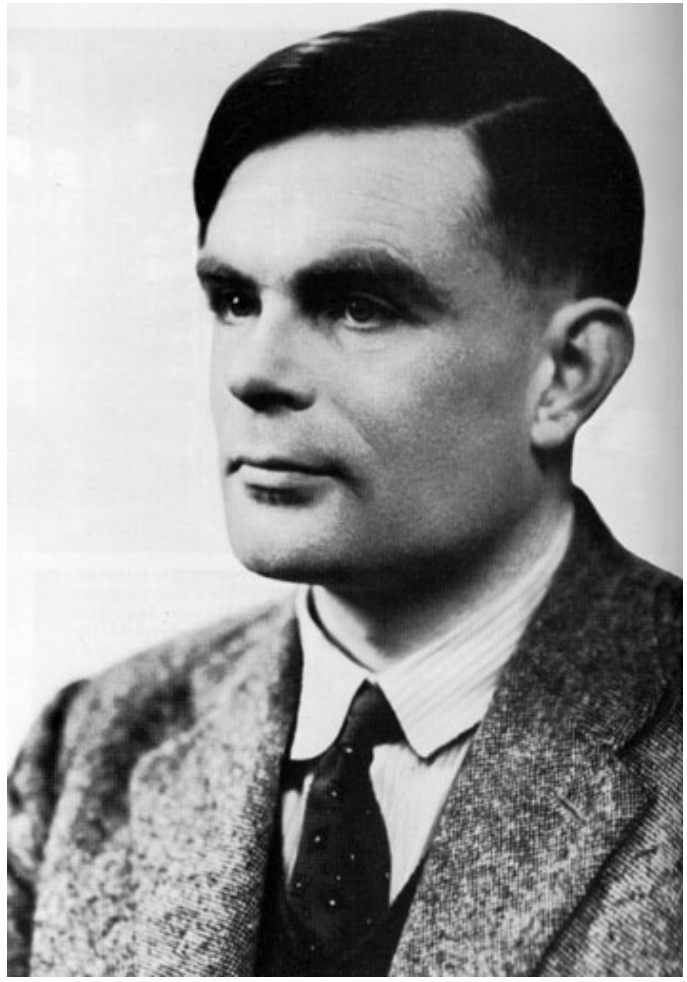
$$\begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} = A^{-1} \begin{bmatrix} x_1 - 11 \\ x_2 - 0 \\ x_3 - 20 \end{bmatrix}$$

Das Resultat für Bob ist:

“SEE” “YOU” “ATN” “OON’.

Die Enigma Maschine von Scherbius

Alan Turing (1912-1954)



Quelle: *http://aima.cs.berkeley.edu/cover.html*

Kerckhoff's Prinzip

JOURNAL
DES
SCIENCES MILITAIRES.

Janvier 1883.

LA CRYPTOGRAPHIE MILITAIRE.

« La cryptographie est un auxiliaire puissant de la tactique militaire. »
(Général LEWAL, *Études de guerre.*)

I.

LA CRYPTOGRAPHIE DANS L'ARMÉE

A. Notions historiques.

La *Cryptographie* ou l'*Art de chiffrer* est une science vieille comme le monde ; confondue à son origine avec la télégraphie militaire, elle a été cultivée, dès la plus haute antiquité, par les Chinois, les Perses, les Carthaginois ; elle a été enseignée dans les écoles tactiques de la Grèce, et tenue en haute estime par les plus illustres généraux romains [1].

Depuis la modeste scytale des Lacédémoniens et les *truces* inventés ou rapportés par Æneas-le-Tacticien [2], jusqu'au fameux

[1] C'est sous la rubrique : *Stéganographie, chiffre* ou *écritures secrètes*, que certains dictionnaires encyclopédiques donnent les renseignements qui se rapportent à la cryptographie. Les anciens auteurs l'appellent plus ou moins correctement : *ars notarum, ars ziphenarum, polygraphia, scotographia, cryptologia, steganologia, cryptomenytices*, etc. ; les Allemands disent aujourd'hui : *Geheimschrift* ou *Chiffreschrift* et les Anglais : *cryptography*.

[2] Lettres mises entre les semelles du messager, communications cachées dans un ulcère du porteur ou dans les pendants d'oreilles des femmes, dés percés de

Vortragsübersicht:

1. Historische Bemerkungen

2. Chiffrierungen mit geheimen Schlüsseln

3. Chiffrierungen mit öffentlichen Schlüsseln

4. Neue Mathematik für neue Kryptographie

Claude Shannon [Sha49] publizierte 1949 ein fundamentales Resultat:

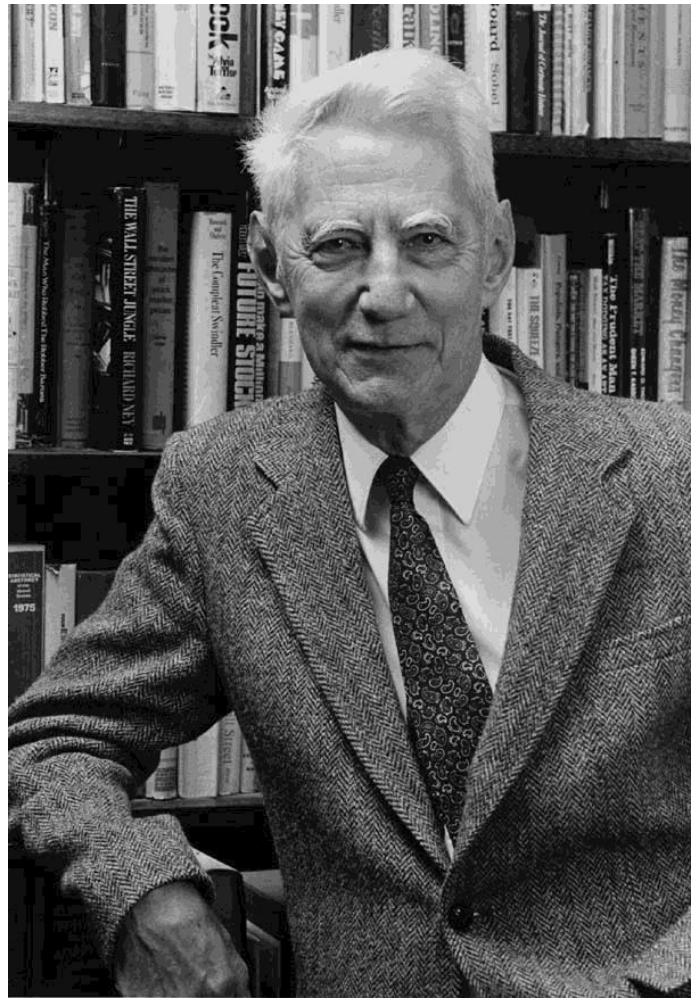
> There exist unconditionally and provable secure cryptographic protocols.

Claude Shannon [Sha49] publizierte 1949 ein fundamentales Resultat:

> There exist unconditionally and provable secure cryptographic protocols.

Die praktische Konsequenz war, dass es im Prinzip beweisbar sichere Verschlüsselungsmethoden gibt.

Claude Shannon (1916-2001)



Quelle: *http://www.bell-labs.com/*

Der ‘One Time Pad’ ist beweisbar sicher

Chiffrierung:

binärer Text:	1	0	0	1	0	1	0	0	1	0
geheimer Schlüssel:	0	0	1	0	1	1	1	1	0	0
chiffrierter Text:	1	0	1	1	1	0	1	1	1	0

Der ‘One Time Pad’ ist beweisbar sicher

Chiffrierung:

binärer Text:	1	0	0	1	0	1	0	0	1	0
geheimer Schlüssel:	0	0	1	0	1	1	1	1	0	0
chiffrierter Text:	1	0	1	1	1	0	1	1	1	0

Dechiffrierung:

chiffrierter Text:	1	0	1	1	1	0	1	1	1	0
geheimer Schlüssel:	0	0	1	0	1	1	1	1	0	0
binärer Text:	1	0	0	1	0	1	0	0	1	0

Der ‘One Time Pad’ ist beweisbar sicher

Chiffrierung:

binärer Text:	1	0	0	1	0	1	0	0	1	0
geheimer Schlüssel:	0	0	1	0	1	1	1	1	0	0
chiffrierter Text:	1	0	1	1	1	0	1	1	1	0

Dechiffrierung:

chiffrierter Text:	1	0	1	1	1	0	1	1	1	0
geheimer Schlüssel:	0	0	1	0	1	1	1	1	0	0
binärer Text:	1	0	0	1	0	1	0	0	1	0

Nachteil 1: Der geheime Schlüssel muss eine grössere Entropie haben als das Total der zukünftigen Nachrichten.

Der ‘One Time Pad’ ist beweisbar sicher

Chiffrierung:

binärer Text:	1	0	0	1	0	1	0	0	1	0
geheimer Schlüssel:	0	0	1	0	1	1	1	1	0	0
chiffrierter Text:	1	0	1	1	1	0	1	1	1	0

Dechiffrierung:

chiffrierter Text:	1	0	1	1	1	0	1	1	1	0
geheimer Schlüssel:	0	0	1	0	1	1	1	1	0	0
binärer Text:	1	0	0	1	0	1	0	0	1	0

Nachteil 1: Der geheime Schlüssel muss eine grössere Entropie haben als das Total der zukünftigen Nachrichten.

Nachteil 2: Der geheime Schlüssel darf absolut nur einmal benützt werden. ($\longrightarrow$ VENONA Projekt)

Rekursive Schlüssel

Eine Methode ‘lange Schlüssel’ mittels ‘kurzen Schlüsseln’ zu bilden ist via Rekursionsformeln:

$$s_{n+d} = f(s_{n+d-1}, \ldots, s_n),\ n = 1, 2, \ldots$$

und Anfangsbedingungen $s_1 = a_1, \ldots, s_d = a_d$.

Rekursive Schlüssel

Eine Methode ‘lange Schlüssel’ mittels ‘kurzen Schlüsseln’ zu bilden ist via Rekursionsformeln:

$$s_{n+d} = f(s_{n+d-1}, \ldots, s_n),\ n = 1, 2, \ldots$$

und Anfangsbedingungen $s_1 = a_1, \ldots, s_d = a_d$.

Beispiel

Fibonacci Reihe $s_{n+2} = s_{n+1} + s_n$ mit Anfangswerten $s_1 = 1,\ s_2 = 1$:

$$\text{über } \mathbb{F}_3\text{: } 1, 1, 2, 0, 2, 2, 1, 0, 1, 1$$

$$\text{über } \mathbb{F}_5\text{: } 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1$$

Im Folgenden seien X, Y beliebige Mengen.

Definition

Eine Einwegfunktion ist eine Abbildung $\varphi : X \longrightarrow Y$ mit der Eigenschaft, dass $\varphi(x)$ effizient berechnet werden kann für jedes $x \in X$. Gleichzeitig sollten keine praktischen Rechenverfahren existieren die es erlauben $x \in \varphi^{-1}(y)$ zu berechnen für ein gegebenes $y \in Y$.

Im Folgenden seien X, Y beliebige Mengen.

Definition

Eine Einwegfunktion ist eine Abbildung $\varphi : X \longrightarrow Y$ mit der Eigenschaft, dass $\varphi(x)$ effizient berechnet werden kann für jedes $x \in X$. Gleichzeitig sollten keine praktischen Rechenverfahren existieren die es erlauben $x \in \varphi^{-1}(y)$ zu berechnen für ein gegebenes $y \in Y$.

Anwendung für Einwegfunktionen:

- Passwort Abspeicherung
- Hashfunktionen

Einwegfunktionen mit geheimem Schlüssel

M: Klartextraum.
K: Schlüsselraum.
C: Chiffretextraum.

Definition

Eine Einwegfunktion mit geheimem Schlüssel ist eine Abbildung $\varphi : M \times K \longrightarrow C$
zusammen mit einer Abbildung $\psi : C \times K \longrightarrow M$ so dass gilt:

1. $\psi(\varphi(m,k),k) = m$ für alle $(m,k) \in M \times K$.
2. Die Abbildungen $\varphi_m : K \longrightarrow C,\ k \longmapsto \varphi(m,k)$
   $\varphi_k : M \longrightarrow C,\ m \longmapsto \varphi(m,k)$
   sind Einwegfunktionen.

Geschichte der Data Encryption Standards

1973: National Institute of Standards erfragt die Forscher um einen Standard.

Geschichte der Data Encryption Standards

1973: National Institute of Standards erfragt die Forscher um einen Standard.

1975: IBM schlägt ‘Lucipher DES’ mit einer Schlüssellänge von 128 bits vor.

Geschichte der Data Encryption Standards

1973: National Institute of Standards erfragt die Forscher um einen Standard.

1975: IBM schlägt ‘Lucipher DES’ mit einer Schlüssellänge von 128 bits vor.

1977: DES mit einer Schlüssellänge von 56 bits wird zum Standard erklärt.

Geschichte der Data Encryption Standards

1973: National Institute of Standards erfragt die Forscher um einen Standard.

1975: IBM schlägt ‘Lucipher DES’ mit einer Schlüssellänge von 128 bits vor.

1977: DES mit einer Schlüssellänge von 56 bits wird zum Standard erklärt.

1995: National Institute of Standards erfragt die Forscher wiederum um einen Standard.

Geschichte der Data Encryption Standards

1973: National Institute of Standards erfragt die Forscher um einen Standard.

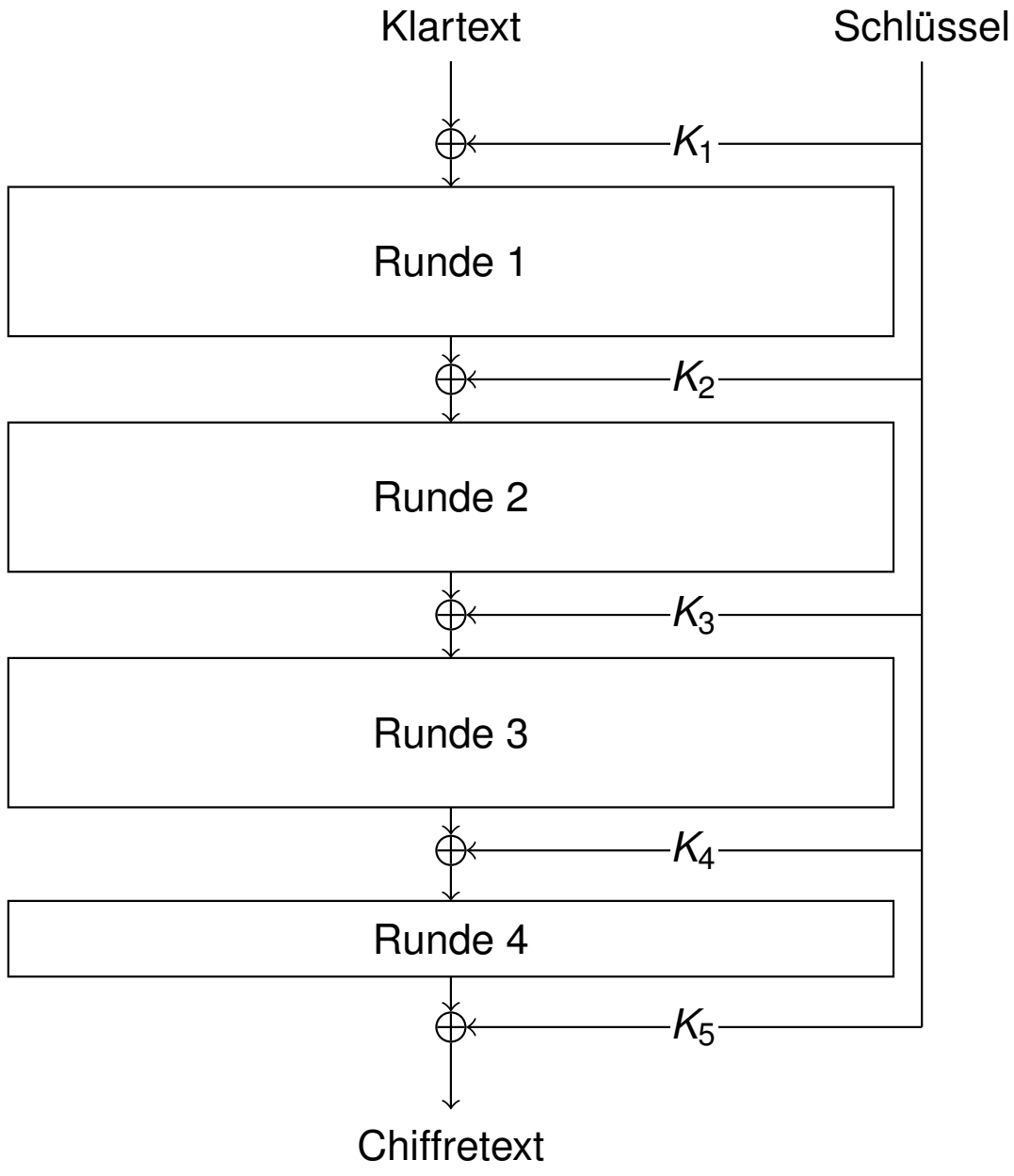
1975: IBM schlägt ‘Lucipher DES’ mit einer Schlüssellänge von 128 bits vor.

1977: DES mit einer Schlüssellänge von 56 bits wird zum Standard erklärt.

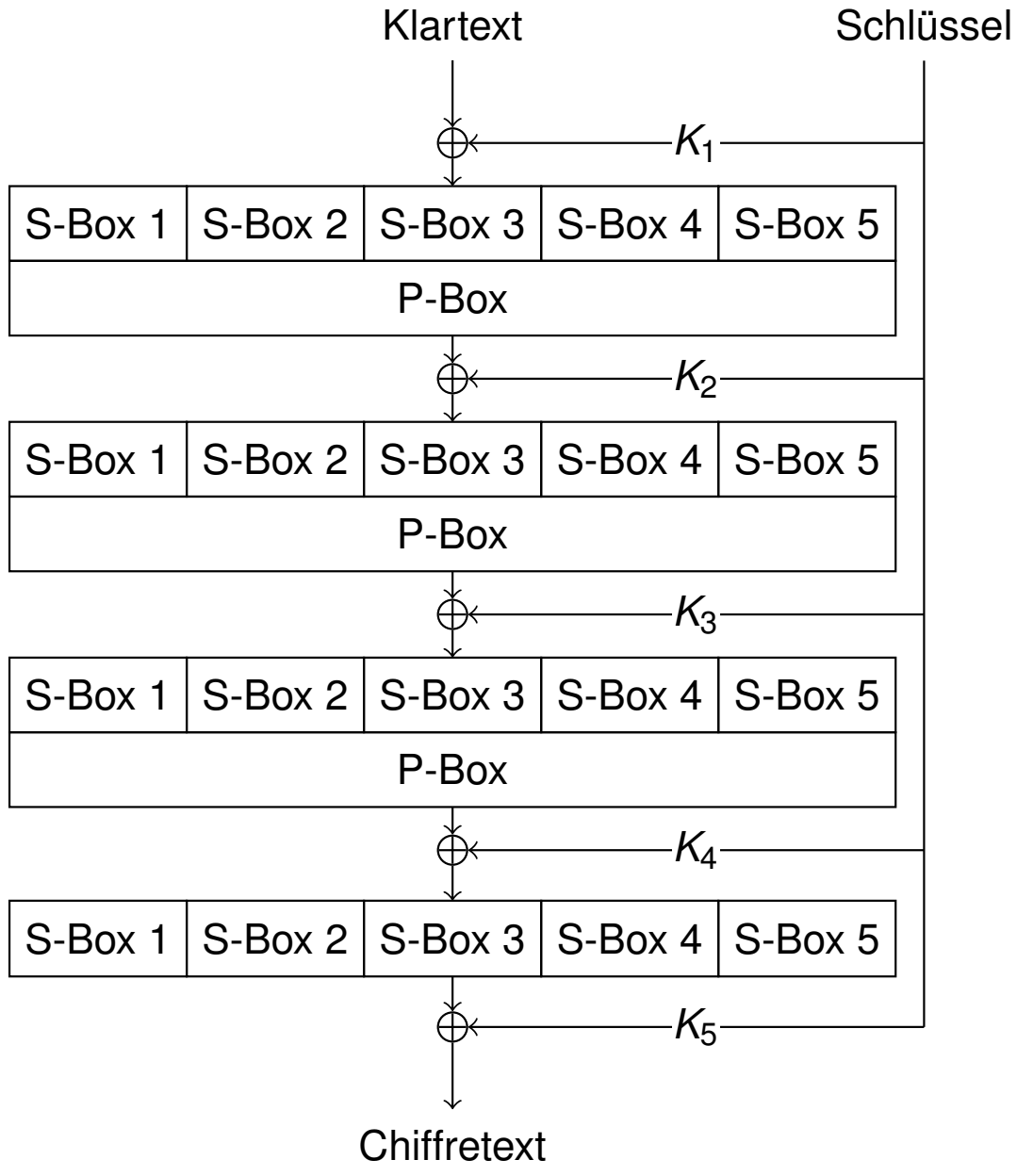
1995: National Institute of Standards erfragt die Forscher wiederum um einen Standard.

2001: Das Rijndael System wird zum Advanced Encryption Standard (AES) erklärt.

Schematische Beschreibung von AES



Schematische Beschreibung von AES



Das Rijndael System (AES)

Vergleiche mit [Ros03].

$$\mu(z) := z^8 + z^4 + z^3 + z + 1 \in \mathbb{Z}_2[z]$$

ist irreduzibel. Betrachte den endlichen Körper $\mathbb{F} := \mathbb{Z}_2[z]/\langle \mu(z) \rangle = \mathrm{GF}(256)$ und definiere das Ideal:

$$I := \langle x^4 + 1, y^4 + 1, \mu(z) \rangle \subset \mathbb{Z}_2[x, y, z].$$

Im folgenden beschreiben wir den Rijndael-Algorithmus mittels polynomialen Operationen im Ring:

$$R := \mathbb{Z}_2[x, y, z]/I = \mathbb{F}[x, y]/\langle x^4 + 1, y^4 + 1 \rangle. \tag{1}$$

Die Monome

$$\left\{ x^i y^j z^k \mid 0 \leq i,j \leq 3,\ 0 \leq k \leq 7 \right\}$$

bilden eine $\mathbb{Z}_2$-Basis des Rings (Algebra) R. Insbesondere ist $\dim_{\mathbb{Z}_2} R = 128$, d.h. $|R| = 2^{128}$.
Falls $r \in R$ definieren wir Elemente $r_{i,j} \in \mathbb{F}$ und $r_j \in \mathbb{F}[x]/\langle x^4 + 1 \rangle$ durch:

$$r = \sum_{i=0}^{3} \sum_{j=0}^{3} r_{i,j} x^i y^j = \sum_{j=0}^{3} \left(\sum_{i=0}^{3} r_{i,j} x^i \right) y^j = \sum_{j=0}^{3} r_j y^j. \qquad (2)$$

Für den Rijndael-Algorithmus definieren wir:

$$K = M = C = R.$$

Folgendes *Permutationspolynom* ist von Wichtigkeit in der Beschreibung:

$$\begin{aligned}\varphi(u) := &\left(z^2+1\right)u^{254}+\left(z^3+1\right)u^{253}+\left(z^7+z^6+z^5+z^4+z^3+1\right)u^{251}\\ &+\left(z^5+z^2+1\right)u^{247}+\left(z^7+z^6+z^5+z^4+z^2\right)u^{239}+u^{223}\\ &+\left(z^7+z^5+z^4+z^2+1\right)u^{191}+\left(z^7+z^3+z^2+z+1\right)u^{127}\\ &+(z^6+z^5+z+1)\in\mathbb{F}[u]. \quad (3)\end{aligned}$$

Angenommen Alice und Bob besitzen beide den geheimen Schlüssel $k \in R$ und Alice möchte die Meldung $m \in R$ an Bob schicken. Dazu berechnen beide 11 Elemente $k^{(t)} \in R,\ t = 0,\ldots,10$:

Key Expansion:

$$
\begin{aligned}
k^{(0)} &:= k \\
k_0^{(t+1)} &:= \left(\sum_{i=0}^{3} \varphi(k_{i,3}^{(t)}) x^i \right) x^3 + z^t + k_0^{(t)} \text{ für } t = 0, \ldots, 9. \\
k_i^{(t+1)} &:= k_{i-1}^{(t+1)} + k_i^{(t)} \text{ für } t = 0, \ldots, 9,\ i = 1, 2, 3.
\end{aligned}
$$

Beide besitzen nun 11 (geheime) Elemente

$$k^{(0)}, k^{(1)}, k^{(2)}, \ldots, k^{(10)}.$$

Im weitern definiert Rijndael das Ringelement:

$$\gamma := (z+1)x^3 + x^2 + x + z \in R.$$

Rijndael Verschlüsselungs-Algorithmus:

Alice verschlüsselt in rekursiver Weise die Meldung $m \in R$:

$$
\begin{aligned}
m^{(0)} &:= m + k^{(0)} \\
m^{(t+1)} &:= \gamma \sum_{i=0}^{3} \sum_{j=0}^{3} \varphi(m_{i,j}^{(t)}) x^i y^{3i+j} + k^{(t+1)}, t = 0, \ldots, 8. \\
m^{(10)} &:= \sum_{i=0}^{3} \sum_{j=0}^{3} \varphi(m_{i,j}^{(9)}) x^i y^{3i+j} + k^{(10)}
\end{aligned}
$$

Der Chiffretext an Bob ist das Ringelement $m^{(10)}$.

Vortragsübersicht:

1. Historische Bemerkungen

2. Chiffrierungen mit geheimen Schlüsseln

3. Chiffrierungen mit öffentlichen Schlüsseln

4. Neue Mathematik für neue Kryptographie

Fundamentale Frage:

Wie kann eine sichere Kommunikation ohne vorhergehenden Schlüsselaustausch gewährleistet werden?

Im Jahre 1976 gaben W. Diffie, M. E. Hellmann und R. C. Merkle darauf eine mathematische Antwort. [DH76]

Diffie-Hellman Schlüsselaustausch

Klassischerweise führt man Diffie-Hellman in der multiplikativen Gruppe eines endlichen Körpers durch. Man nimmt eine grosse Primzahl p (in der Grössenordnung von 2^n mit $n \in \{1024, 2048, 4096\}$, wobei $n = 1024$ heutzutage nicht mehr verwendet werden sollte) und betrachtet die Restklassen in $\mathbb{Z}_p$ ungleich 0:

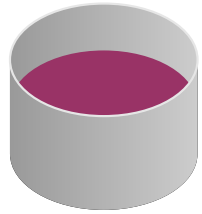
$$G := \{\overline{1}_p, \ldots, \overline{p-1}_p\}$$

Diese Gruppe $(G, \cdot)$ hat $p-1$ Elemente.

Diffie-Hellman Schlüsselaustausch

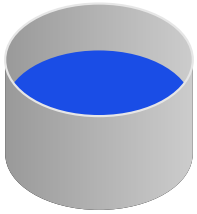
1. Alice sucht sich eine geheime Zahl $e_A \in \{2, \ldots, p-1\}$ aus. Sie berechnet $g_A := g^{e_A} \in G$ und schickt das Ergebnis g_A an Beat.
2. Beat sucht sich eine geheime Zahl $e_B \in \{2, \ldots, p-1\}$ aus. Er berechnet $g_B := g^{e_B} \in G$ und schickt das Ergebnis g_B an Antje.
3. Zu diesem Zeitpunkt kann man G, g, g_A und g_B als allgemein bekannt annehmen.
4. Alice kennt jetzt g_B und kann $g_{AB} := (g_B)^{e_A} = g^{e_A e_B}$ berechnen, ohne e_B zu kennen.
5. Beat kennt jetzt g_A und kann $g_{AB} := (g_A)^{e_B} = g^{e_A e_B}$ berechnen, ohne e_A zu kennen.
6. Alice und Beat kennen beide g_{AB}, aber niemand anders kann aus G, g, g_A und g_B den Wert g_{AB} berechnen, ohne zuerst einen diskreten Logarithmus zu bestimmen.

Diffie-Hellman-Schlüsselaustausch mit Farben

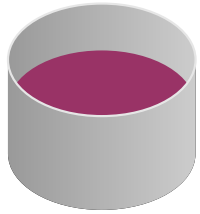


Grundfarbe

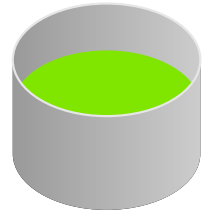
Diffie-Hellman-Schlüsselaustausch mit Farben



Alices geheime Farbe

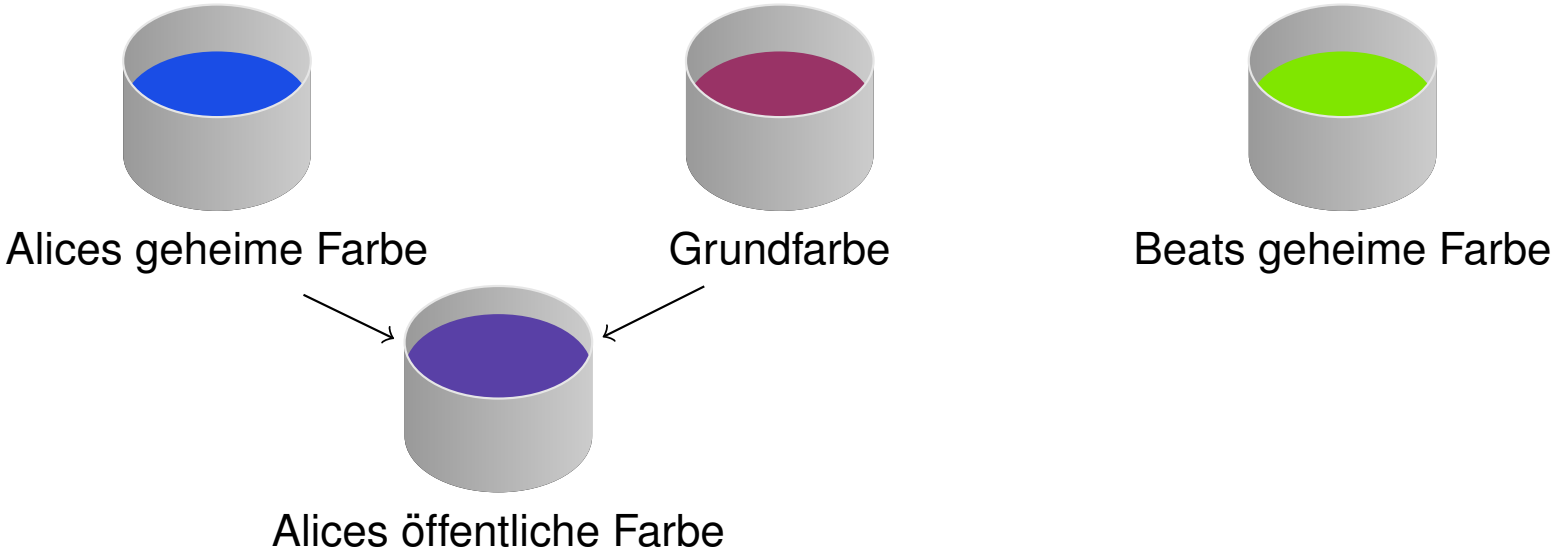


Grundfarbe

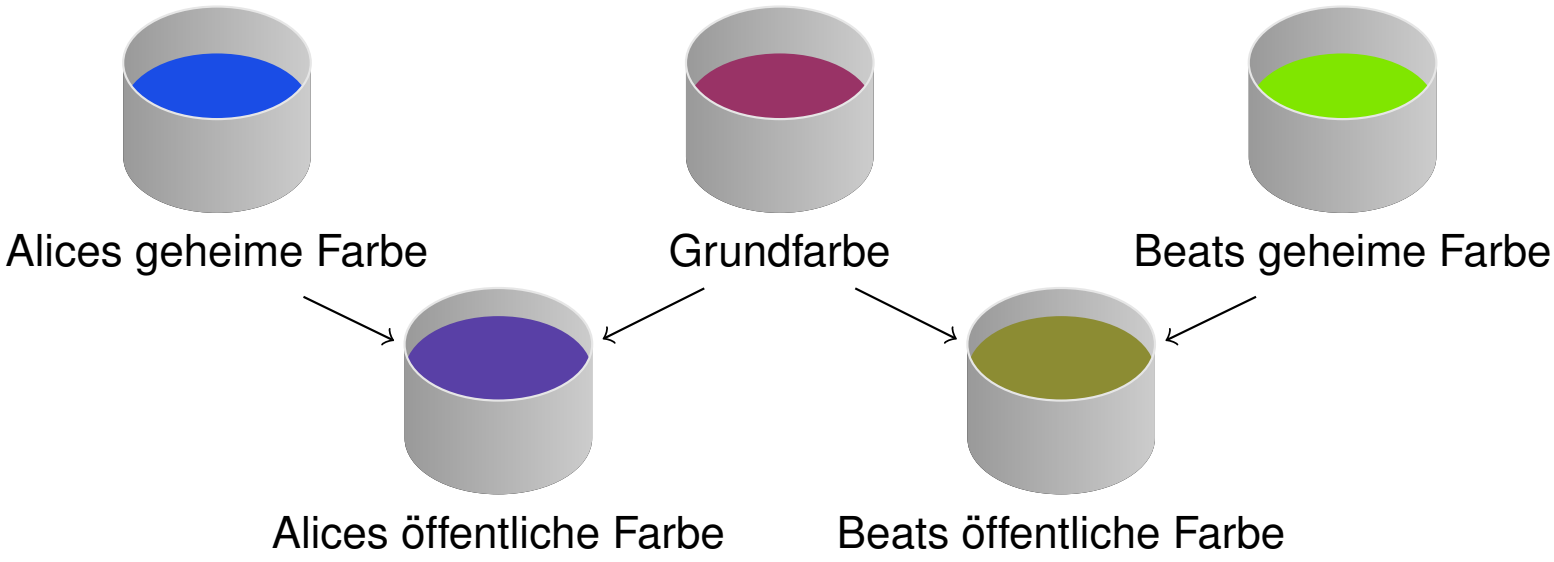


Beats geheime Farbe

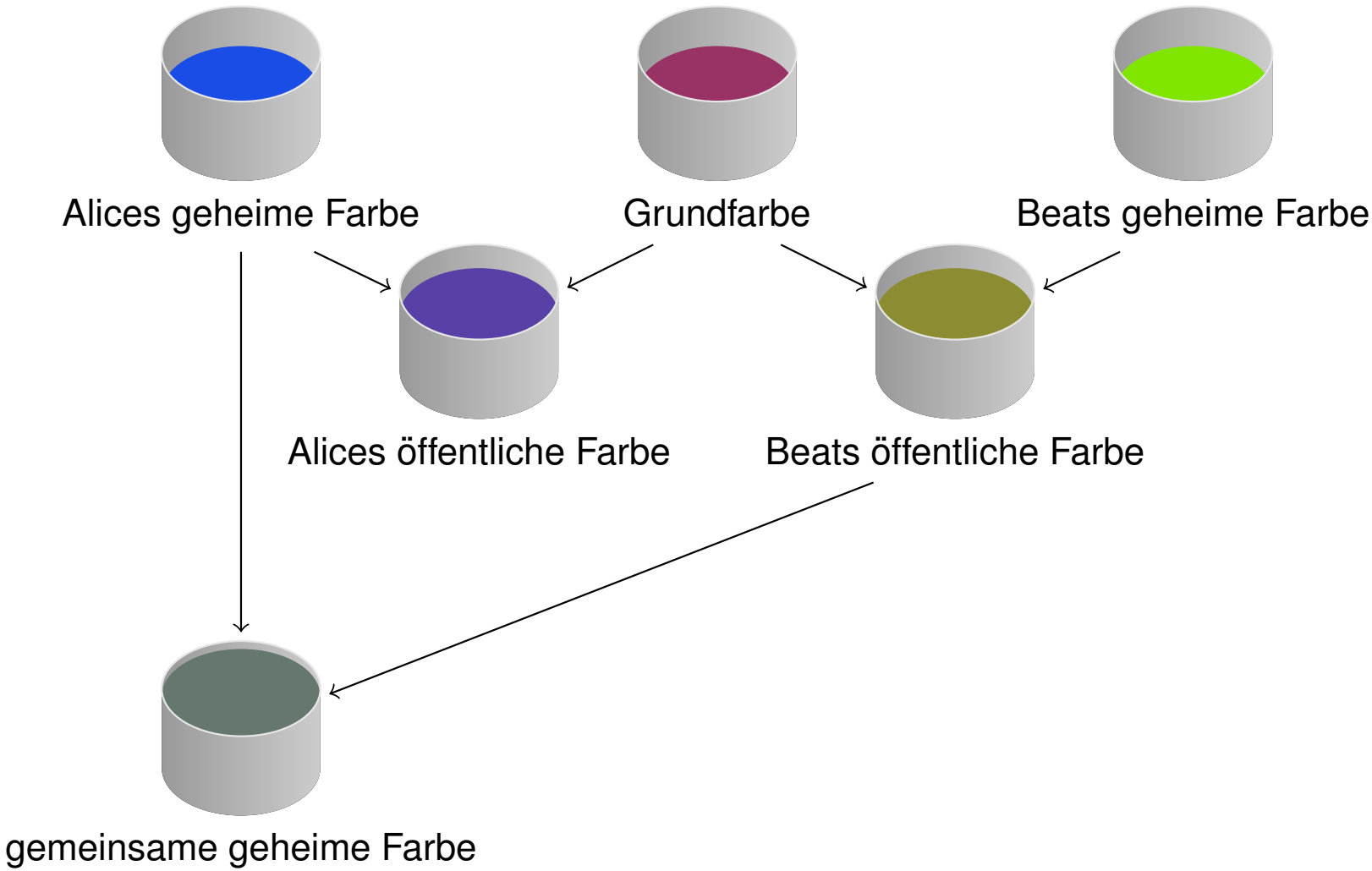
Diffie-Hellman-Schlüsselaustausch mit Farben



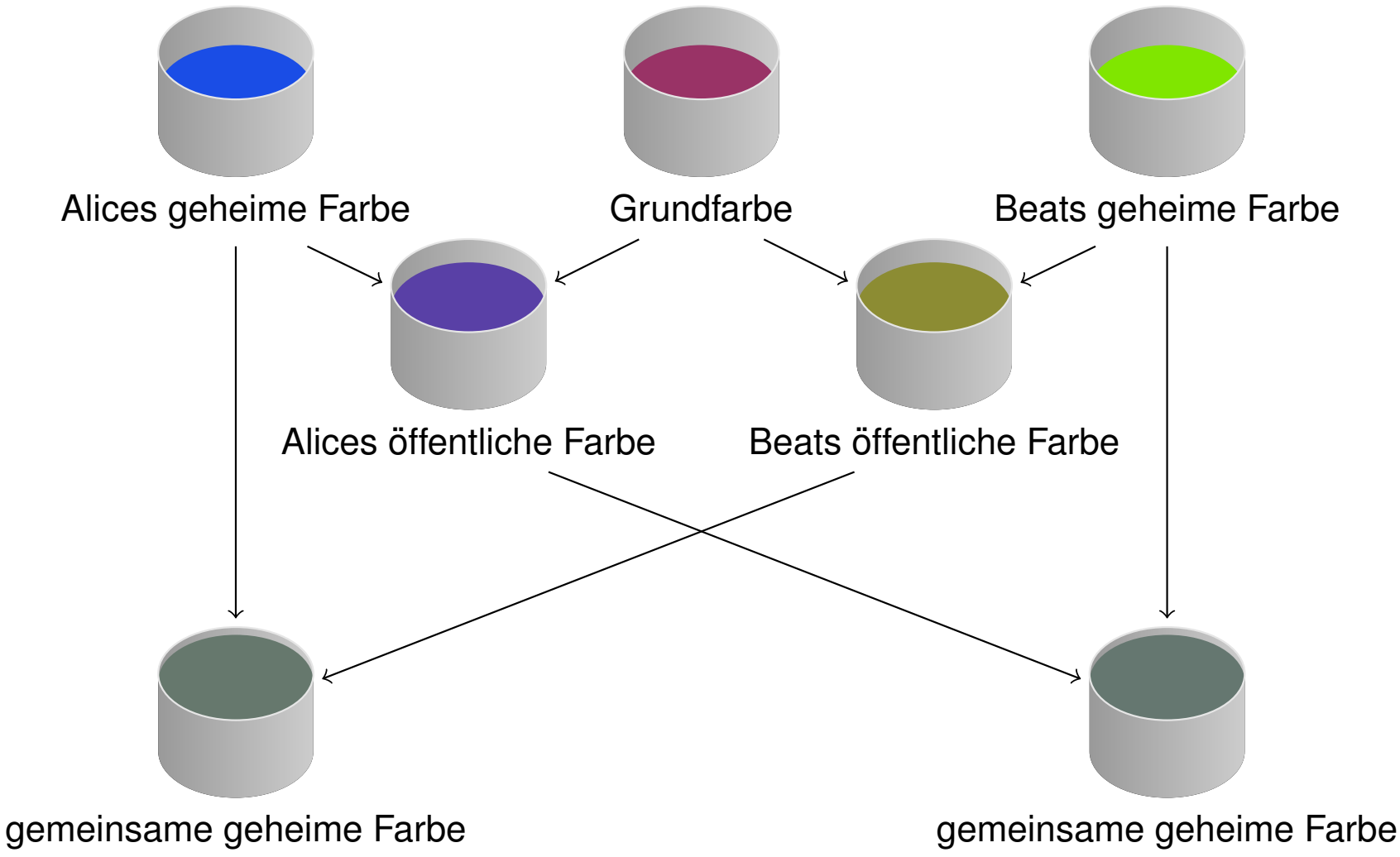
Diffie-Hellman-Schlüsselaustausch mit Farben



Diffie-Hellman-Schlüsselaustausch mit Farben



Diffie-Hellman-Schlüsselaustausch mit Farben



Sicherheit vom Diffie-Hellman Schlüsselaustausch

1. Mathematisch beruht die Sicherheit des Diffie-Hellman Schlüsselaustausch Verfahrens auf der Schwierigkeit des diskreten Logarithmus in der gewählten Gruppe G.
2. Für die Gruppe $\mathbb{Z}_p$ konnte Maurer und Wolf [Mau94] zeigen dass das Diffie-Hellman Verfahren polynomial äquivalent ist zum diskreten Logarithmus in der Gruppe.
3. Neue Forschung zeigt dass die multiplikative Gruppe in einem endlichen Körper vermieden werden sollte wenn die Charakteristik klein ist [GGMZ14].
4. Von der Informatikseite gibt es Seitenkanalangriffe auf konkrete Implementationen (Timing-Attacken);

Sendung einer Nachricht die öffentlich verschlüsselt ist

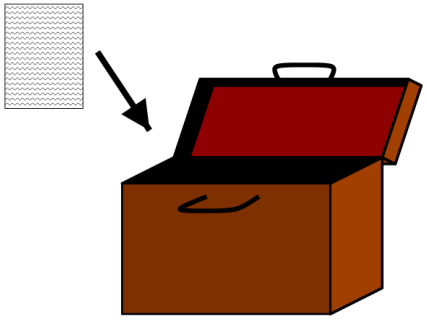
Alice

Bob

Sendung einer Nachricht die öffentlich verschlüsselt ist

Alice

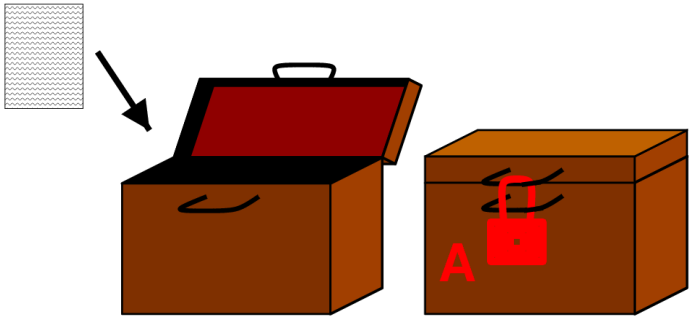
Bob



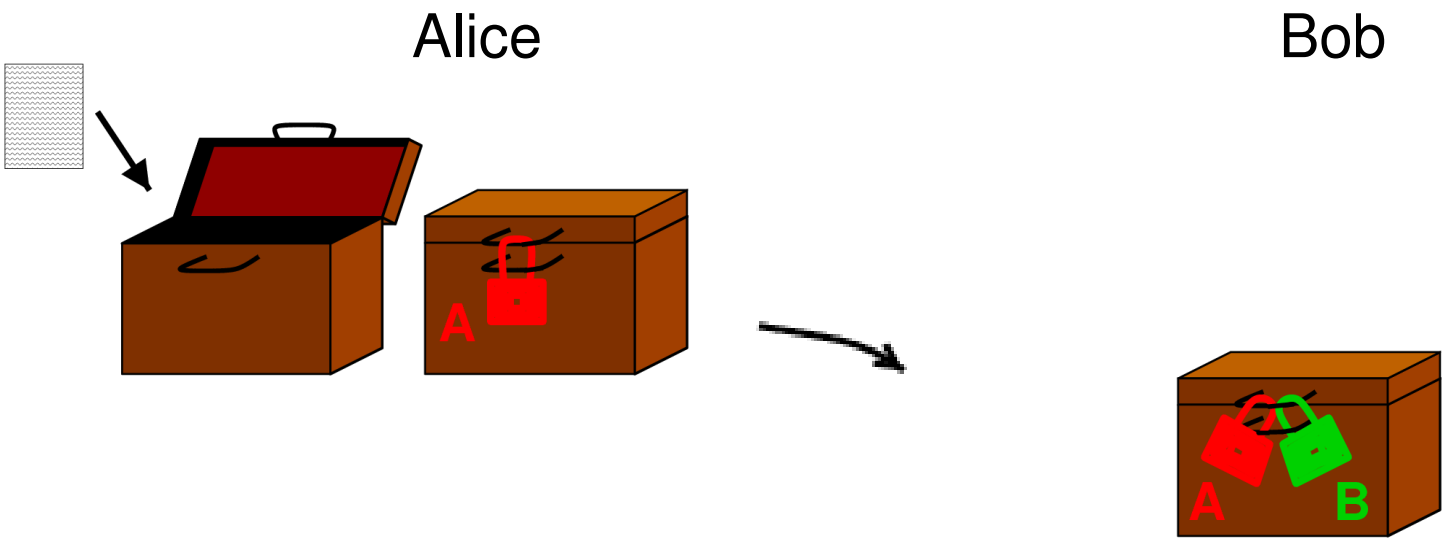
Sendung einer Nachricht die öffentlich verschlüsselt ist

Alice

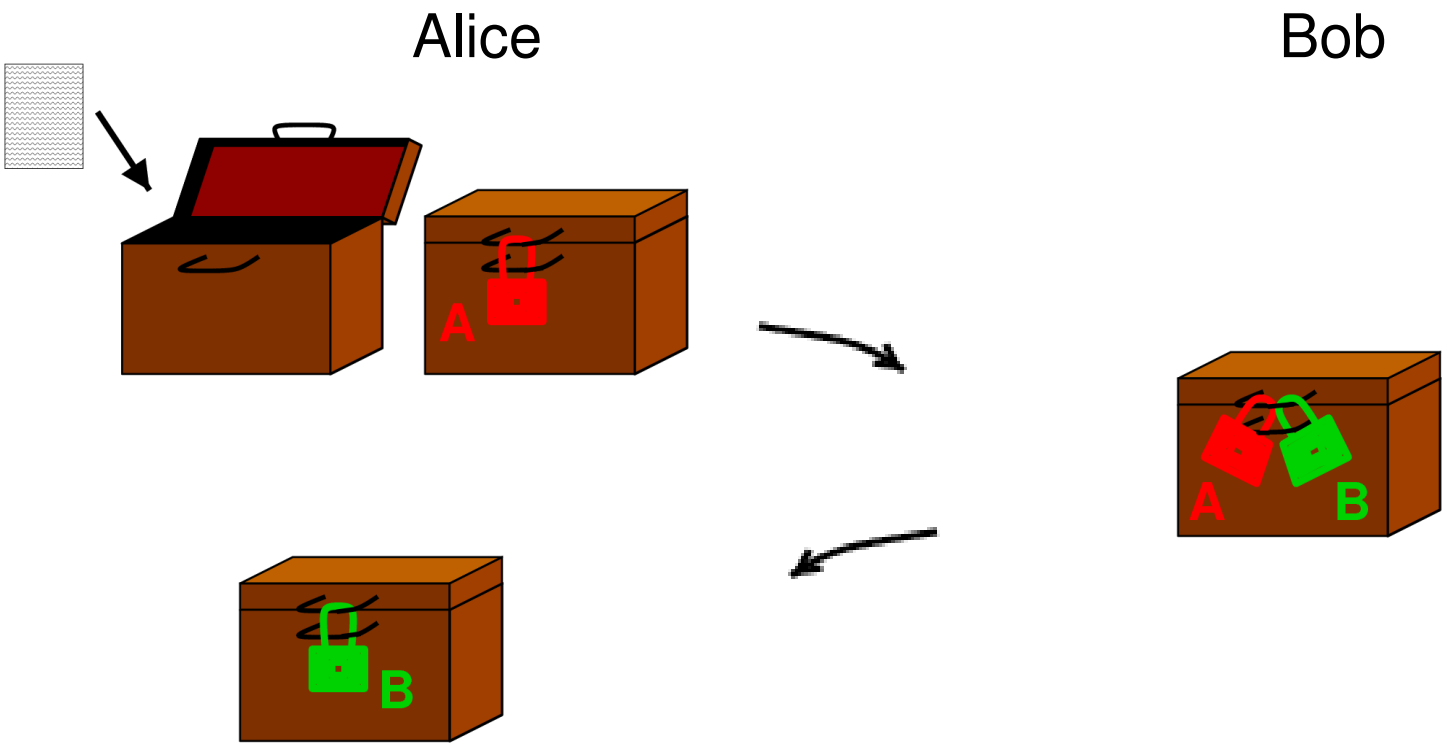
Bob



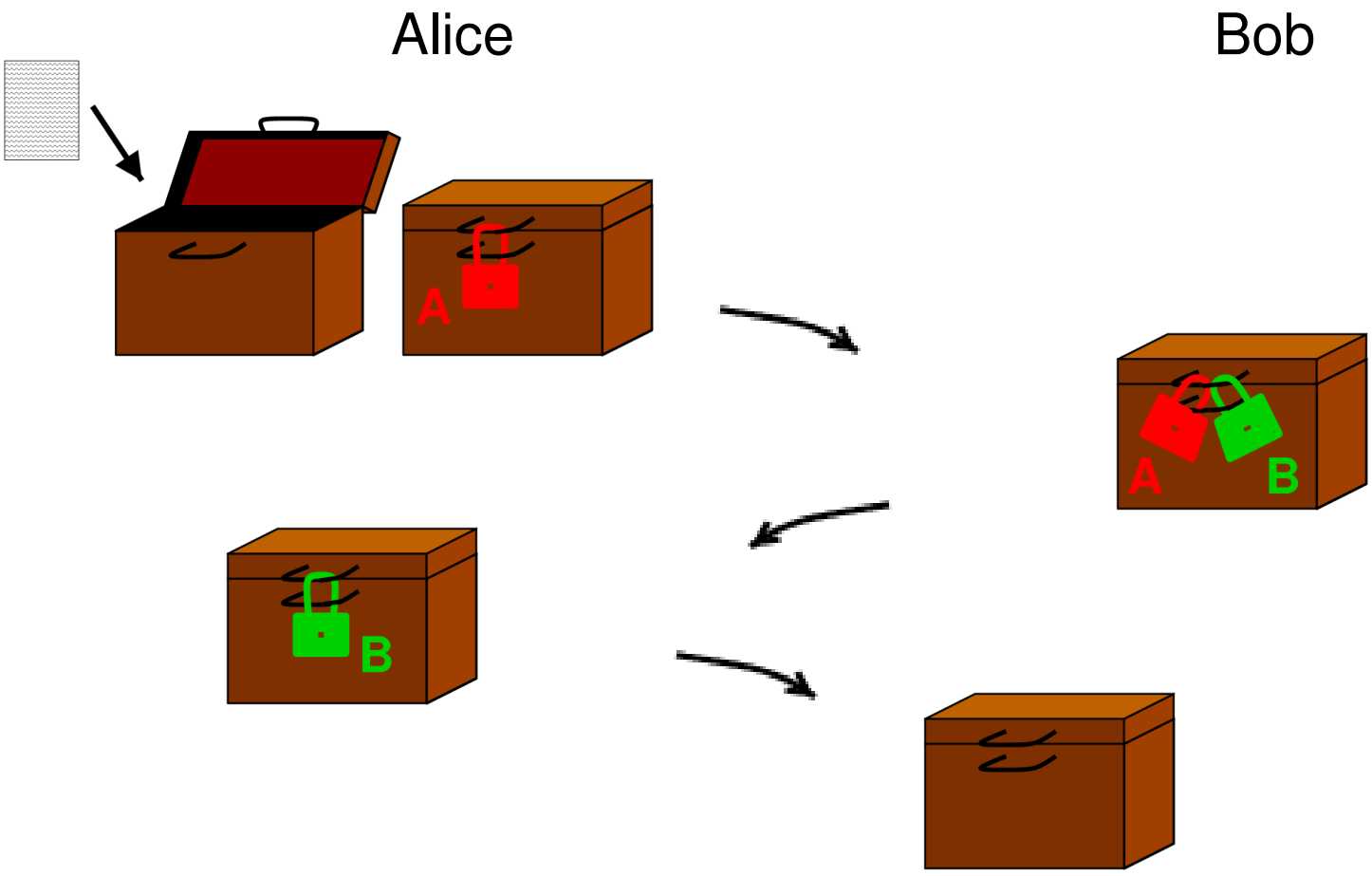
Sendung einer Nachricht die öffentlich verschlüsselt ist



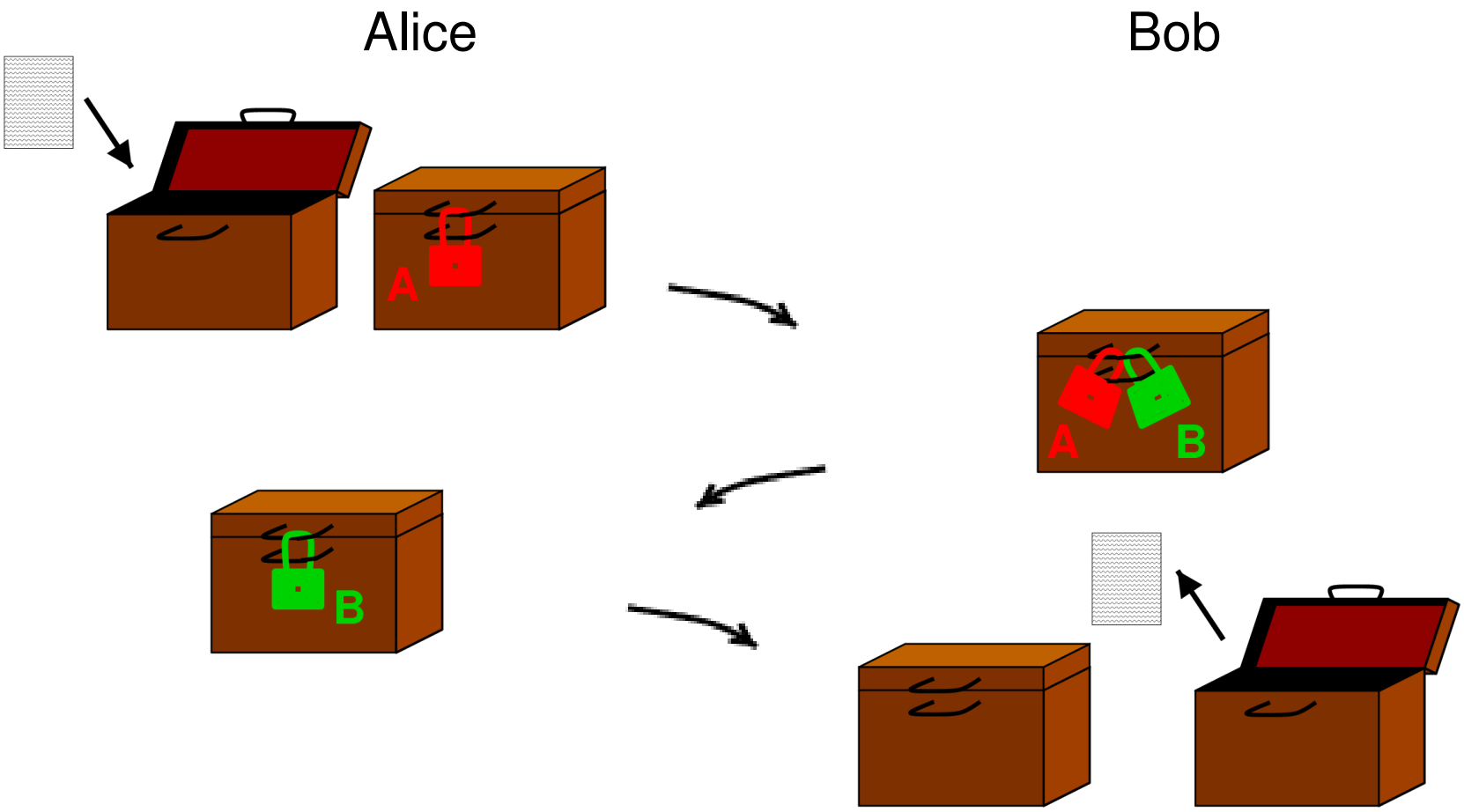
Sendung einer Nachricht die öffentlich verschlüsselt ist



Sendung einer Nachricht die öffentlich verschlüsselt ist



Sendung einer Nachricht die öffentlich verschlüsselt ist



Trapdoor Einwegfunktionen

Definition

Eine Trapdoor Einwegfunktion ist eine Abbildung $\varphi : X \longrightarrow Y$, welche die Eigenschaft besitzt:

1. φ ist injektiv
2. Mit Hilfe eines 'privaten Schlüssels' des Designers ist es möglich

$$\varphi^{-1} : \varphi(X) \longrightarrow X.$$

zu berechnen.

Prinzip der öffentlichen Verschlüsselungsverfahren

- Alice konstruiert eine Trapdoor Einwegfunktion $\varphi : X \longrightarrow Y$ und publiziert diese.
- Mit Hilfe von φ verschlüsselt Bob seine Meldung $x \in X$. Er schickt $\varphi(x) \in Y$ zu Alice.
- Nur Alice weiss $x = \varphi^{-1}(\varphi(x))$ zu berechnen.

Prinzip der öffentlichen Verschlüsselungsverfahren

- Alice konstruiert eine Trapdoor Einwegfunktion $\varphi : X \longrightarrow Y$ und publiziert diese.
- Mit Hilfe von φ verschlüsselt Bob seine Meldung $x \in X$. Er schickt $\varphi(x) \in Y$ zu Alice.
- Nur Alice weiss $x = \varphi^{-1}(\varphi(x))$ zu berechnen.

Bemerkung

In der Praxis repräsentiert $x \in X$ meist einen geheimen Schlüssel für ein symmetrisches Verschlüsselungsverfahren (z.B. Rijndael).

Prinzip der öffentlichen Verschlüsselungsverfahren

- Alice konstruiert eine Trapdoor Einwegfunktion $\varphi : X \longrightarrow Y$ und publiziert diese.
- Mit Hilfe von φ verschlüsselt Bob seine Meldung $x \in X$. Er schickt $\varphi(x) \in Y$ zu Alice.
- Nur Alice weiss $x = \varphi^{-1}(\varphi(x))$ zu berechnen.

Bemerkung

In der Praxis repräsentiert $x \in X$ meist einen geheimen Schlüssel für ein symmetrisches Verschlüsselungsverfahren (z.B. Rijndael).

Bemerkung

Die Wichtigkeit von Trapdoor Einwegfunktionen wurde von Diffie, Hellman und Merkle um 1976 erkannt.

Bemerkungen

Trapdoor Einwegfunktionen haben viele Anwendungen wie z.B.:

- geheimer Schlüsselaustausch
- Digitale Unterschriften
- Authentication protocols
- Digital Cash System
- Zero knowledge proofs
- BitCoin
- Electronic Voting

RSA Trapdoor Einwegfunktion

Alice konstruiert eine ganze Zahl $n = pq$, wobei p, q Primzahlen mit mehr als 100 Ziffern sind. Sie bestimmt $e < n$ koprim zu $\phi(n) = (p-1)(q-1)$. Ihre Trapdoor Einwegfunktion ist:

$$\begin{array}{rccc} \varphi: & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & m & \longmapsto & m^e = c \end{array}$$

Falls Bob an Alice die Nachricht m^e gesandt hat kann Alice die Meldung m wie folgt entschlüsseln:
Alice kennt die Gruppenordnung von $(\mathbb{Z}_n)^*$. Mit Hilfe des Euklidschen Algorithmus berechnet Sie $d, b \in \mathbb{Z}$ so dass $de + b\phi(n) = 1$. Die Umkehrfunktion ist dann:

$$\begin{array}{rcl} \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ c & \longmapsto & c^d = m \end{array}$$

Verifiziere:

$$c^d = (m^e)^d = m^{de} = m^{1-b\phi(n)} = m \cdot \left(m^{\phi(n)}\right)^{-b} = m$$

Bemerkungen

- Fast alle implementierten öffentlichen Verschlüsselungsverfahren sind RSA basierened.
- Wegen theoretischen Fortschritten im Bereich des Faktorisierens ist heute ein öffentlicher Schlüssel von mindestens 1000 bits absolut notwendig.
- Auf einem Quantum-Computer ist faktorisieren in polynomialer Zeit möglich [Sho99].

ROCA Attacke

- In 1996 Don Coppersmith fand eine effiziente Faktorisierungsmethode für RSA Zahlen $n = p \cdot q$ bei denen man die Hälfte der bits einer der beiden Primzahlen kannte.
- Eine Deutsche Semiconductor Firma verkaufte Geräte welche RSA Zahlen generierte wobei die Primzahlen die spezielle Form

$$p = k \cdot M + (2^{16} + 1)^a \mod M,$$

  hatten.
- Eine Gruppe von Tschechischen Forschern [NSS+17] publizierte im Oktober 2017 ein Verfahren, welches Ideen von Coppersmith übernahm und solche RSA Zahlen faktorisieren kann.

National Institute of Standards (NIST)

NIST: ([nis16]) Im Februar 2016 veröffentlichte NIST einen Report über “Post-Quantum Kryptograhie” in diesem Report liest man:

Quote: “It is unclear when scalable quantum computers will be available, however in the past year or so, researchers working on building a quantum computer have estimated that it is likely that a quantum computer capable of breaking RSA - 2048 in a matter of hours could be built by 2030 for a budget of about a billion dollars. This is a serious long - term threat to the cryptosystems currently standardized by NIST”

Vortragsübersicht:

1. Historische Bemerkungen

2. Chiffrierungen mit geheimen Schlüsseln

3. Chiffrierungen mit öffentlichen Schlüsseln

4. Neue Mathematik für neue Kryptographie

4. Neue Mathematik für neue Kryptographie

In der modernen Kryptographie werden oft Mengen eingesetzt die ‘zahlenähnliche’ Eigenschaften haben.

4. Neue Mathematik für neue Kryptographie

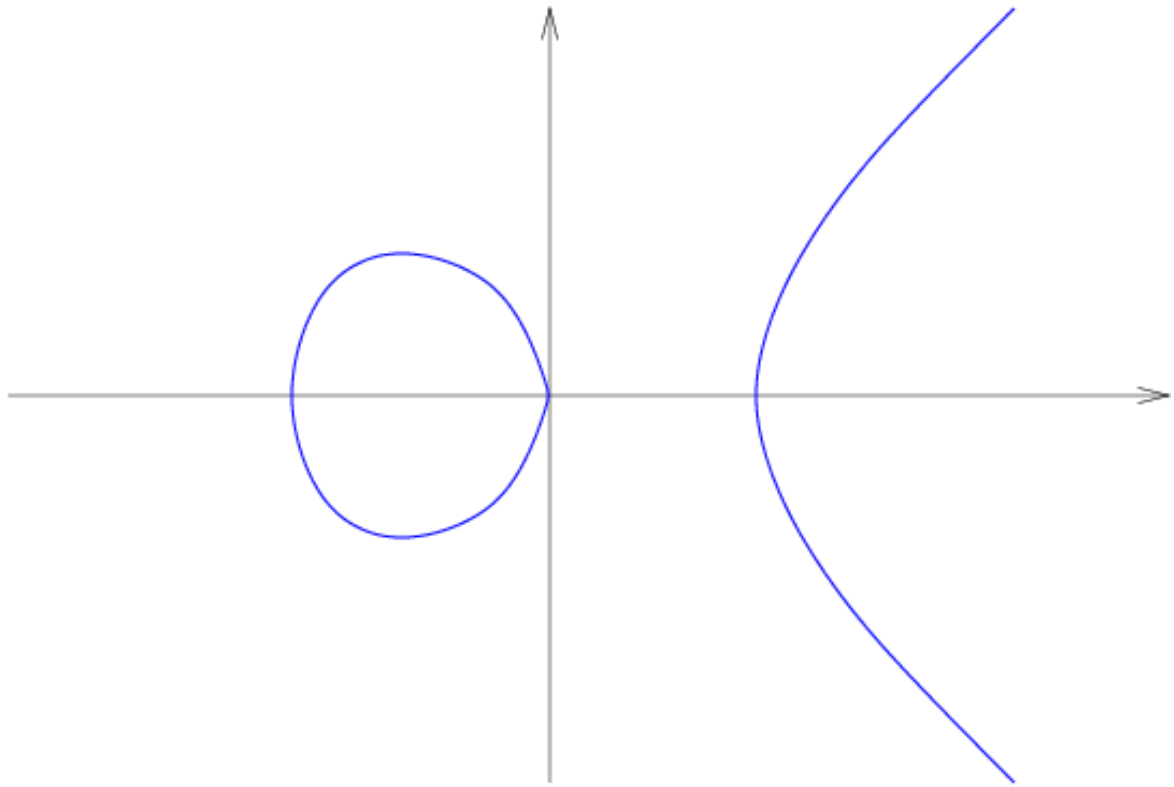
In der modernen Kryptographie werden oft Mengen eingesetzt die ‘zahlenähnliche’ Eigenschaften haben.

Beispiel: Die folgenden Additions- und Multiplikationstafeln beschreiben einen *irreduziblen Halbring* der Ordnung 6. Halbringe dieser Art wurden von Chris Monico und Jens Zumbrägel gefunden und untersucht.

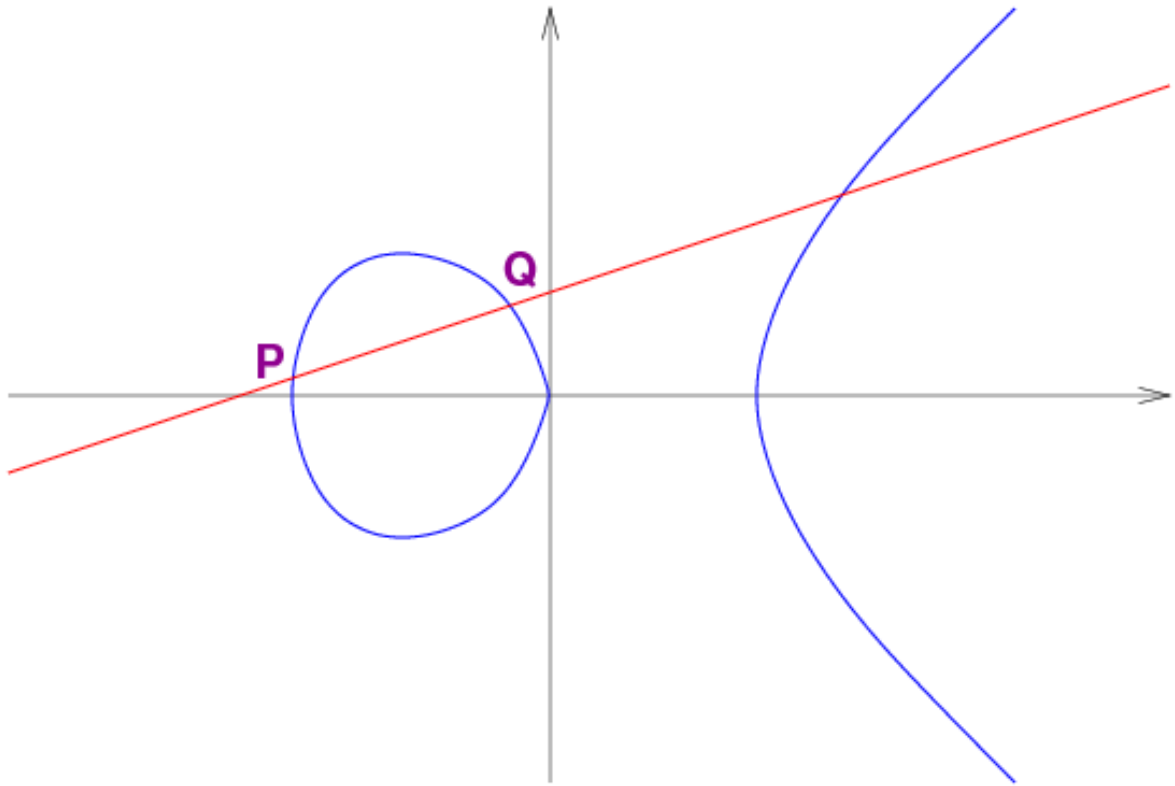
$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	1	1	1	1	5
2	2	1	2	1	2	5
3	3	1	1	3	3	5
4	4	1	2	3	4	5
5	5	5	5	5	5	5

$*$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	2	0	0	5
3	0	3	4	3	4	3
4	0	4	4	0	0	3
5	0	5	2	5	2	5

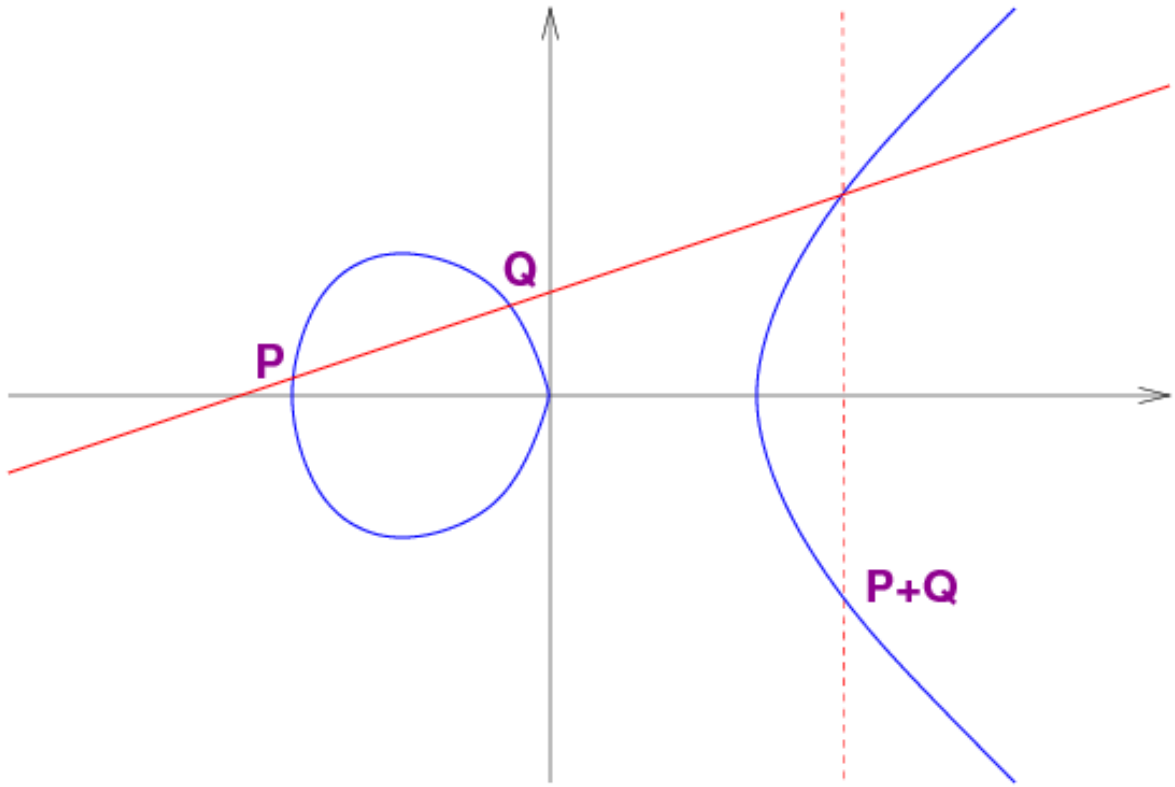
Elliptische Kurven Kryptographie



Elliptische Kurven Kryptographie



Elliptische Kurven Kryptographie



Massey-Omura Protokoll

Alice und Bob einigen sich auf eine elliptische Kurve $E(\mathbb{F}_q)$ deren Ordnung prim ist.
Alice möchte die Meldung $P \in E(\mathbb{F}_q)$ an Bob schicken.

Massey-Omura Protokoll

Alice und Bob einigen sich auf eine elliptische Kurve $E(\mathbb{F}_q)$ deren Ordnung prim ist.
Alice möchte die Meldung $P \in E(\mathbb{F}_q)$ an Bob schicken.

1. Alice wählt $a \in \mathbb{Z}$ (ihr privater Schlüssel) und schickt an Bob aP.

Massey-Omura Protokoll

Alice und Bob einigen sich auf eine elliptische Kurve $E(\mathbb{F}_q)$ deren Ordnung prim ist.
Alice möchte die Meldung $P \in E(\mathbb{F}_q)$ an Bob schicken.

1. Alice wählt $a \in \mathbb{Z}$ (ihr privater Schlüssel) und schickt an Bob aP.
2. Bob wählt $b \in \mathbb{Z}$ (Bob's privater Schlüssel) und schickt an Alice baP.

Massey-Omura Protokoll

Alice und Bob einigen sich auf eine elliptische Kurve $E(\mathbb{F}_q)$ deren Ordnung prim ist.
Alice möchte die Meldung $P \in E(\mathbb{F}_q)$ an Bob schicken.

1. Alice wählt $a \in \mathbb{Z}$ (ihr privater Schlüssel) und schickt an Bob aP.
2. Bob wählt $b \in \mathbb{Z}$ (Bob's privater Schlüssel) und schickt an Alice baP.
3. Alice berechnet $a^{-1}baP = bP$ (sie entfernt ihren Schlüssel) und schickt das Resultat an Bob.

Massey-Omura Protokoll

Alice und Bob einigen sich auf eine elliptische Kurve $E(\mathbb{F}_q)$ deren Ordnung prim ist.
Alice möchte die Meldung $P \in E(\mathbb{F}_q)$ an Bob schicken.

1. Alice wählt $a \in \mathbb{Z}$ (ihr privater Schlüssel) und schickt an Bob aP.
2. Bob wählt $b \in \mathbb{Z}$ (Bob's privater Schlüssel) und schickt an Alice baP.
3. Alice berechnet $a^{-1}baP = bP$ (sie entfernt ihren Schlüssel) und schickt das Resultat an Bob.
4. Bob berechnet $b^{-1}bP = P$ (er entfernt seinen Schlüssel) und erhält die Meldung von Alice.

Danke für Ihre Aufmerksamkeit!

Spezieller Dank an:

Marco Baldi, Josep Climent, Michele Elia, Felix Fontein, Elisa Gorla, Anna-Lena Horlemann, Karan Kathuria, Christine Kelley, Juan Antonio Lopez Ramos, Kyle Marshall, Felice Manganiello, Giacomo Micheli, Gérard Maze, Chris Monico, Alina Ostafe, Davide Schipani, Reto Schnyder, Urs Wagner, Violetta Weger, und Jens Zumbrägel.


W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory **IT-22** (1976), no. 6, 644–654.


Faruk Göloğlu, Robert Granger, Gary McGuire, and Jens Zumbrägel, *Solving a 6120 -bit DLP on a Desktop Computer*, pp. 136–152, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.


U. M. Maurer, *Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms*, Advances in cryptology—CRYPTO '94 (Santa Barbara, CA, 1994), Springer, Berlin, 1994, pp. 271–281.


Report on Post-Quantum Cryptography, Tech. report, National Institute of Standards and Technology, February 2016, NISTIR 8105.


M. Nemec, M. Sys, P. Svenda, D. Klinec, and V. Matyas, *The return of coppersmith's attack: Practical factorization of widely used RSA moduli*, Preprint, October 2017.


J. Rosenthal, *A polynomial description of the Rijndael advanced encryption standard*, J. Algebra Appl. **2** (2003), no. 2, 223–236.


C. E. Shannon, *Communication theory of secrecy systems*, Bell System Tech. J. **28** (1949), 656–715.


P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Rev. **41** (1999), no. 2, 303–332 (electronic).