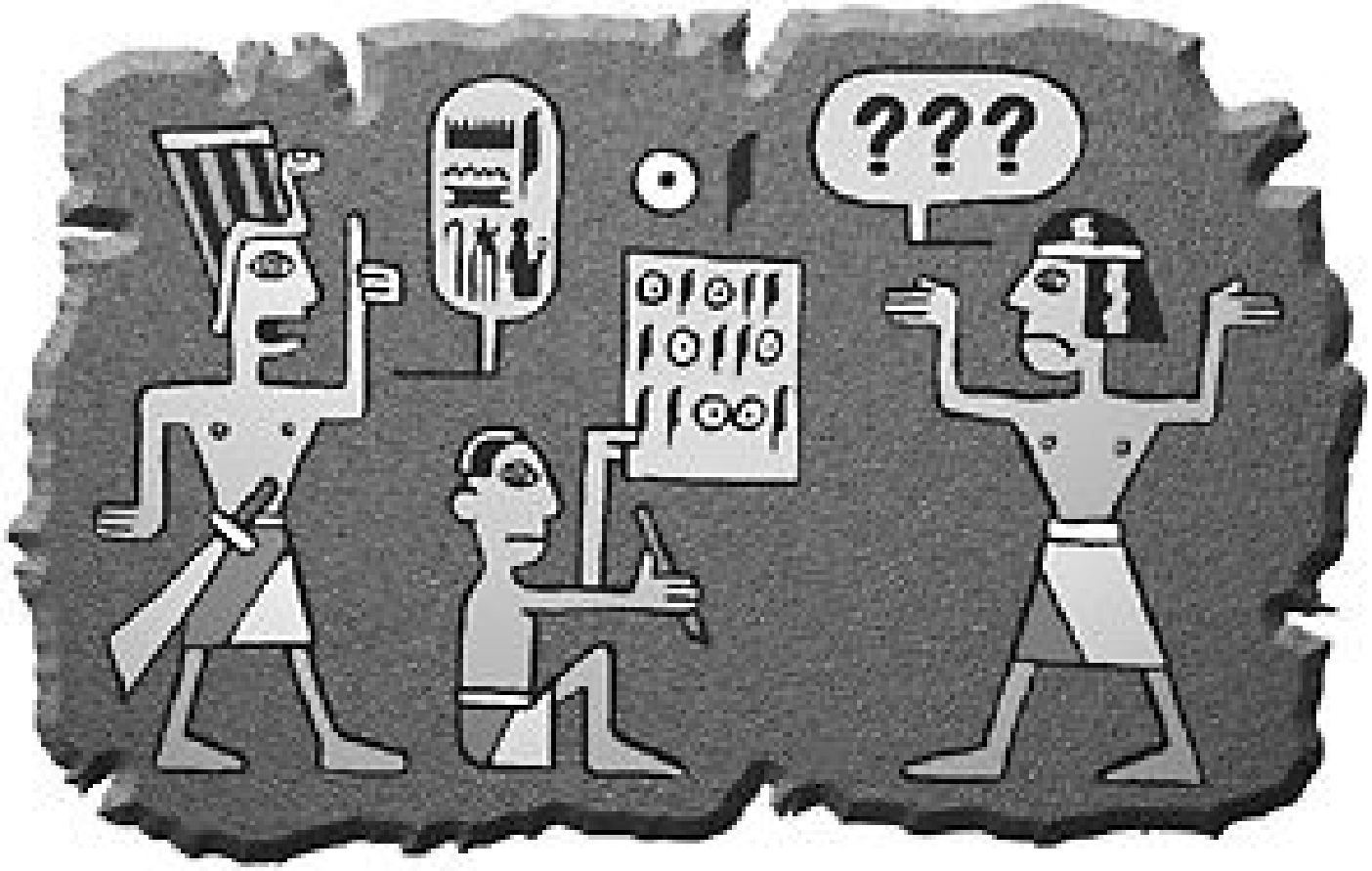
Kryptographie

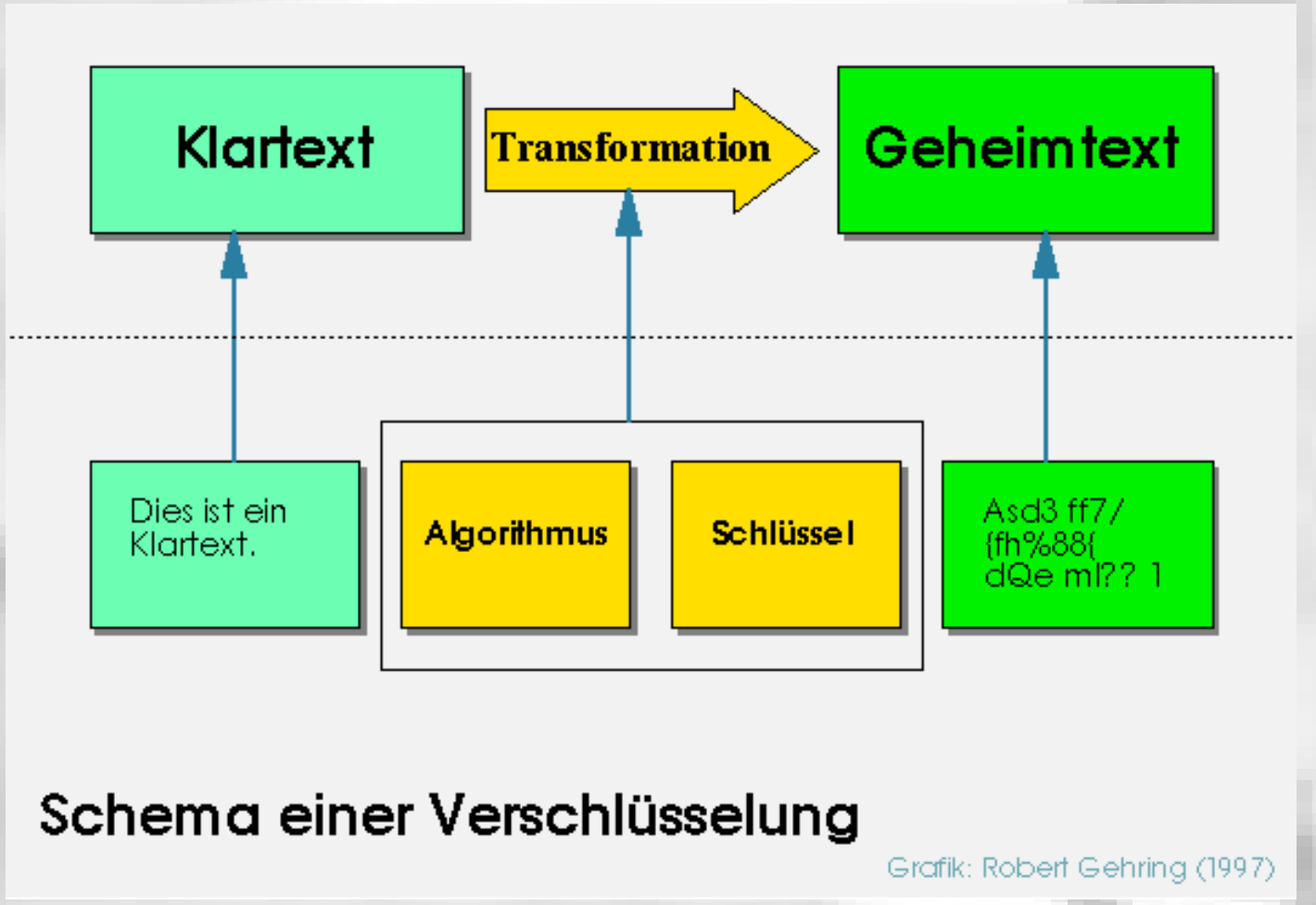


Claudia Wierskowski und Andreas Thiessen

Betreuer: Eberhard Heyne

Inhaltsverzeichnis

Einleitung



Schema einer Verschlüsselung

Grafik: Robert Gehring (1997)

Einleitung

- Einsatzgebiete
  - Sensible Daten in der Wissenschaft
  - Abwicklung von Geschäftsvorgängen
  - Vertrauliche Informationen im Privaten

Einleitung

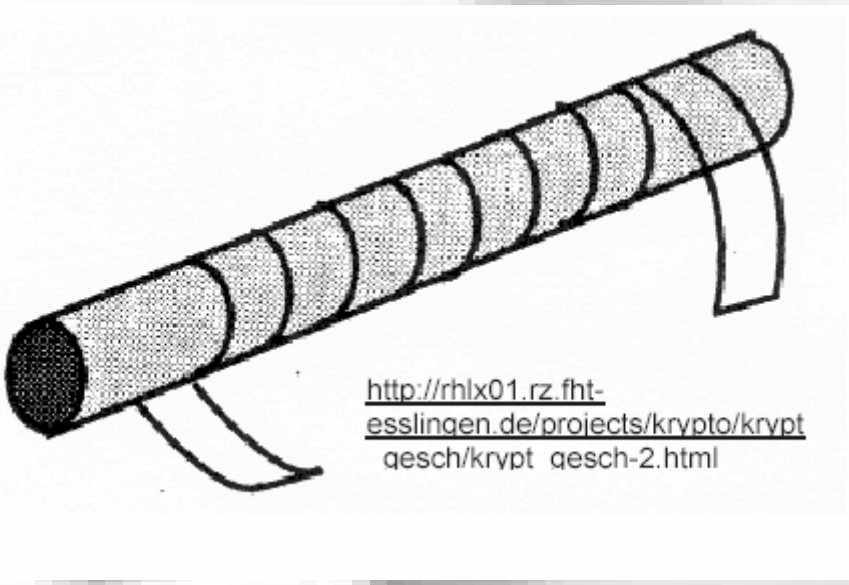
- Ziele
  - Vertraulichkeit
  - Integrität
  - Authentizität

Historisches

- Einleitung
- **Historisches**
- Blockchiffren
  - Symmetrische Verfahren
  - Asymmetrische Verfahren
  - Hybrid Verfahren
- Aktuelle Anwendung
- Politische Randbedingungen
- Ausblick

Historisches

- Skytale



- Caesar Chiffre

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

Klartext: KRYPTOGRAPHIE

Chiffretext: NUBSWRJUDSKLH

Historisches

- Vigènere Chiffre
  - Erstes Chiffrierverfahren mit Schlüssel

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

Schlüsseltext	G	E	H	E	I	M	G	E	H	E	I	M	G	E	H	E	I
Klartext	D	I	E	L	O	E	S	U	N	G	L	A	U	T	E	T	X
Chiffretext	J	M	L	P	W	Q	Y	Y	U	K	T	M	A	X	L	X	F

Historisches

- One-Time-Pad
  - einziges 100% sicheres Chiffrierverfahren
- Enigma
  - Rotormaschine eingesetzt im 2.Weltkrieg

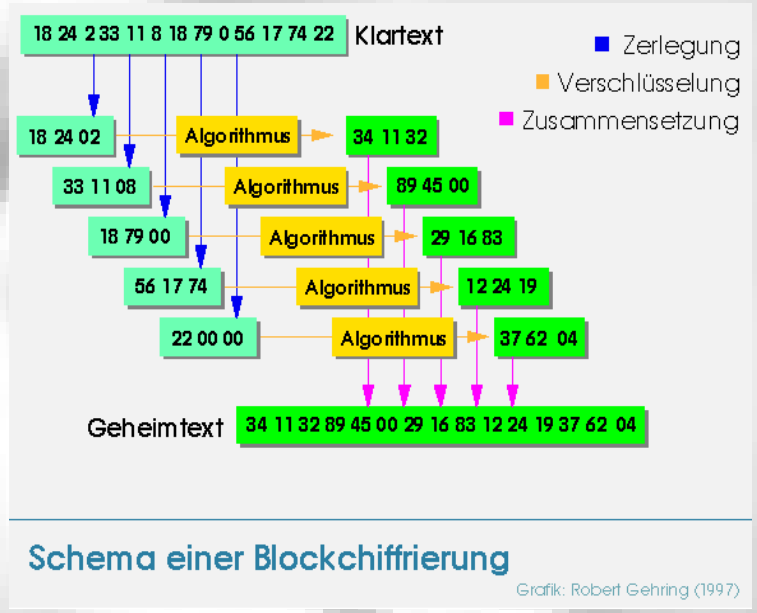
http://ed-thelen.org/comp-hist/NSA-Enigma.html

Blockchiffren

- Einleitung
- Historisches
- **Blockchiffren**
  - Symmetrische Verfahren
  - Asymmetrische Verfahren
  - Hybrid Verfahren
- Aktuelle Anwendung
- Politische Randbedingungen
- Ausblick

Blockchiffren

- Nachteile Klassische Verfahren
  - Einfache Verschlüsselung
  - Konfusion
  - Regelmäßigkeiten im Chiffretext
- Blockchiffren
  - Block fester Länge
  - Diffusion
  - Kaum Regelmäßigkeiten
  - Blocklängen 64 oder 128 Bit



Schema einer Blockchiffrierung

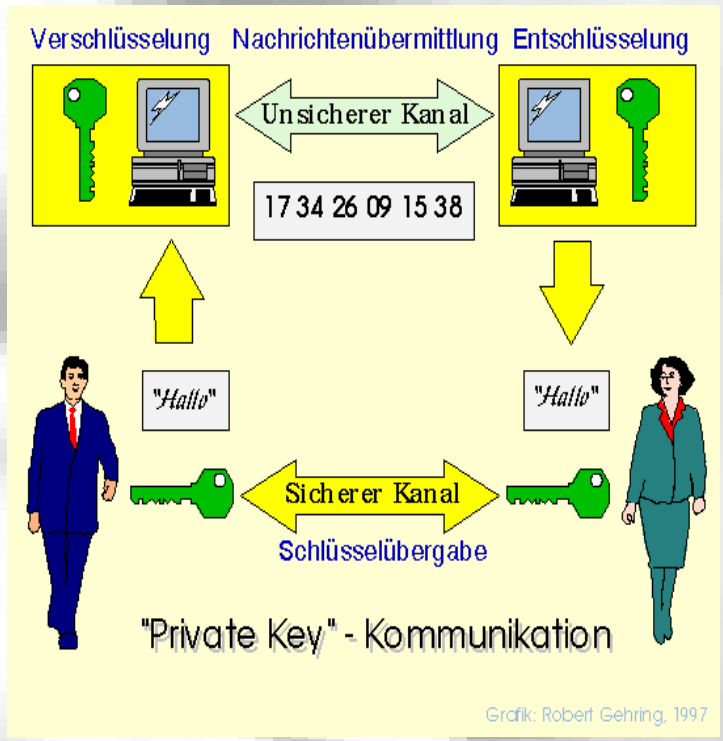
Grafik: Robert Gehring (1997)

Blockchiffren: Symmetrische Verfahren

- Einleitung
- Historisches
- Blockchiffren
  - **Symmetrische Verfahren**
  - Asymmetrische Verfahren
  - Hybrid Verfahren
- Aktuelle Anwendung
- Politische Randbedingungen
- Ausblick

Blockchiffren: Symmetrische Verfahren

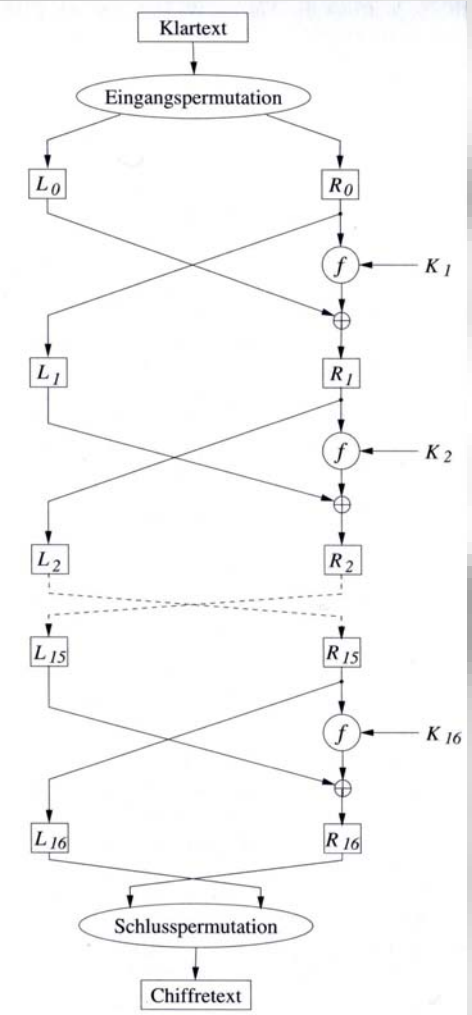
- Grundlagen
  - Symmetrischer Schlüssel
  - Einfache Chiffriervorschriften
    - XOR
    - Vertauschen
    - Shiften
  - 8–16 Verschlüsselungsrunden



Blockchiffren: Symmetrische Verfahren

- DES Data-Encryption-Standard
  - Ab 1977 USA Standard Chiffrierverfahren
  - Wurde durch Brute Force Angriff gebrochen
  - Erweiterung Triple-DES ist bis heute sicher
  - 2002 durch AES abgelöst

Blockchiffren: Symmetrische Verfahren



- DES Verfahren
  - 64-Bit Schlüssel
  - 64-Bit Blöcke
  - 16 Runden
  - Teilen des 64- Bit Blockes in eine linke und eine rechte Hälfte
  - Basiert auf gegebenen Permutationstabellen

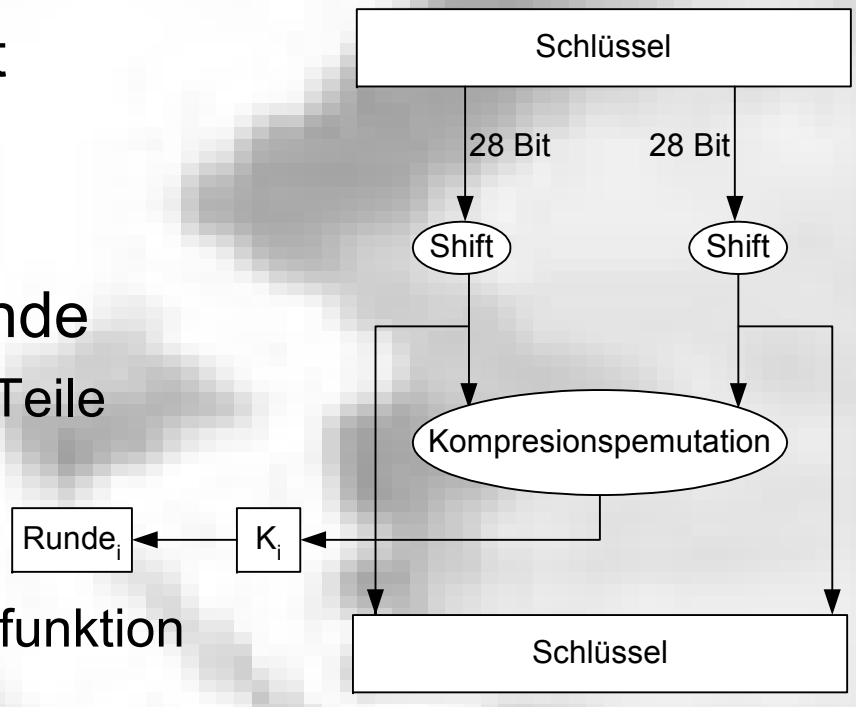
Eingangspermutation:

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Angewandte Kryptographie, W. Ertel

Blockchiffren: Symmetrische Verfahren

- Schlüsselerzeugung
  - 64-Bit Schlüssel auf 56 Bit kürzen
  - Wiederholung in jeder Runde
    - Teilen in zwei gleich große Teile
    - Shiften
    - 48 von 56 Bit auswählen
    - 48 Bit Schlüssel an Rundenfunktion geben
    - 56 Bit an nächste Runde geben



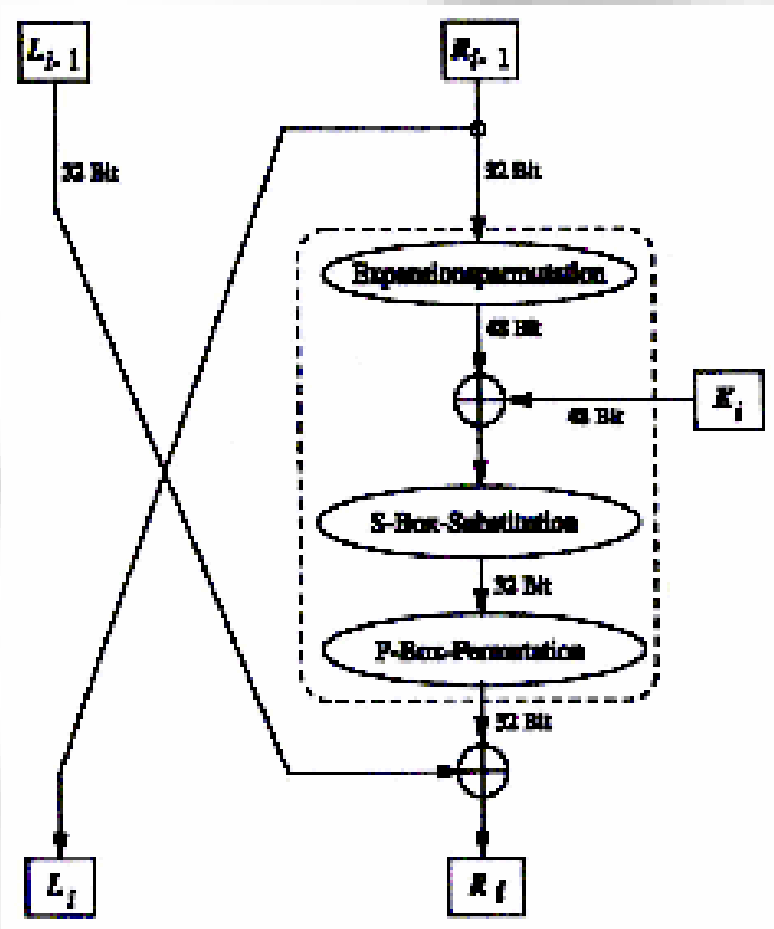
Angewandte Kryptographie, W. Ertel

Blockchiffren: Symmetrische Verfahren

- Eine Runde
  - Expansion
  - XOR- Verknüpfung mit Schlüssel

Expansionspermutation:

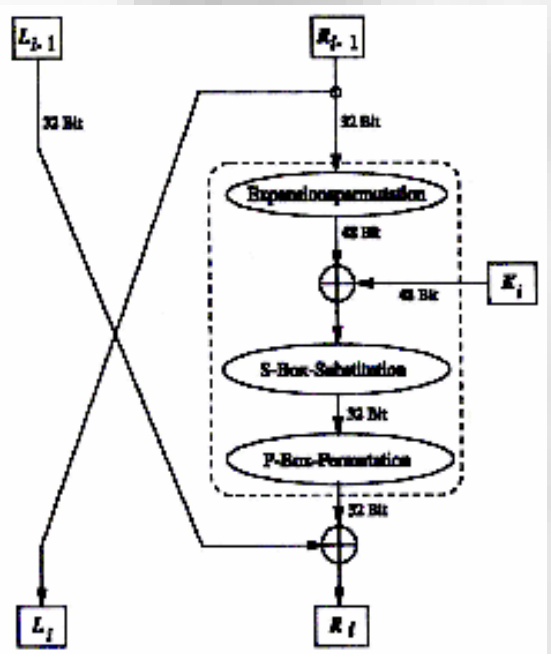
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1



Angewandte Kryptographie, W. Ertel

Blockchiffren: Symmetrische Verfahren

- S-Box Substitution
- P-Box Permutation
- XOR- Verknüpfung mit linker Hälfte



S-Box 5:

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Beispiel:

Eingabe für S-Box 5 ist binär 110100

Bits 1 und 6 sind binär 10 das ergibt den Zeilenindex 2

Bits 2 – 5 ergeben sind binär 1010 den Spaltenindex 10

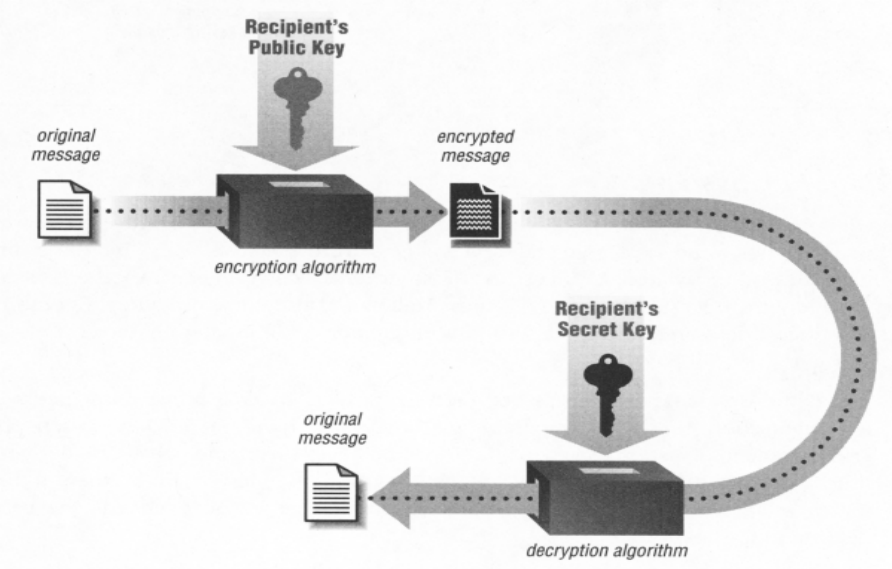
Rückgabe 12

Blockchiffren: Asymmetrische Verfahren

- Einleitung
- Historisches
- Blockchiffren
  - Symmetrische Verfahren
  - **Asymmetrische Verfahren**
  - Hybrid Verfahren
- Aktuelle Anwendung
- Politische Randbedingungen
- Ausblick

Blockchiffren: Asymmetrische Verfahren

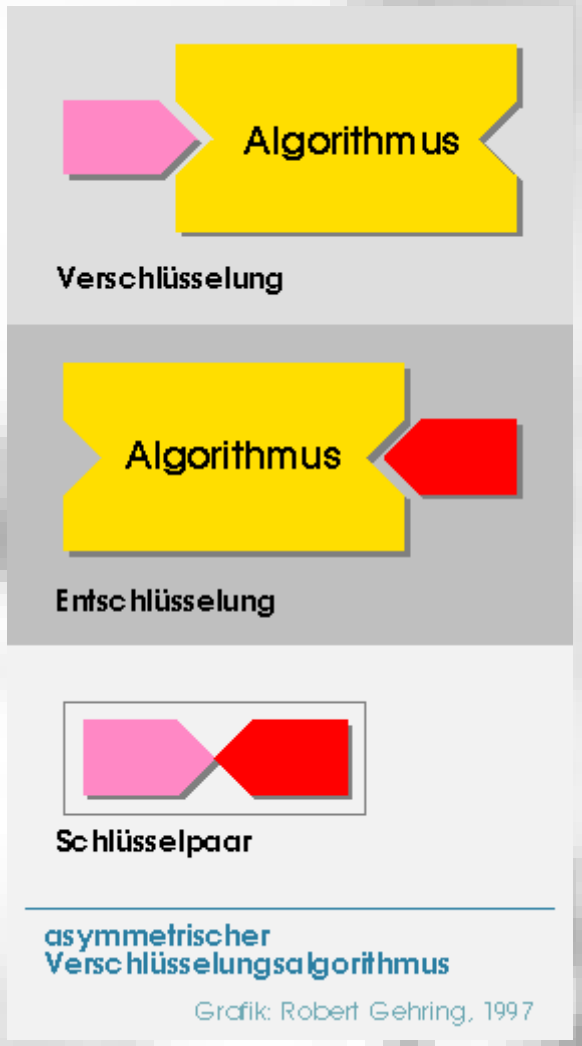
- Grundlagen
  - Idee aus 70er Jahre von Whitfield Diffie, Martin Hellmann, Ralph Merkle
  - Unterschiedliche Schlüssel zum Ver- und Entschlüsseln
  - Schlüsselpaar aus öffentlichem und privaten Schlüssel => Public Key Verfahren



http://www.ita.hsr.ch/studienarbeiten/arbeiten/WS98/SecurityTutorial/verschluesselung.html

Blockchiffren: Asymmetrische Verfahren

- Forderungen
  - Schlüsselpaar muss leicht erzeugbar sein
  - Verbindung zwischen Schlüsseln darf nicht herstellbar sein
- Lösung
  - Harte mathematische Probleme



Blockchiffren: Asymmetrische Verfahren

- RSA
  - benannt nach seinen Erfindern Ron Rivest, Adi Shamir und Len Adleman
  - 1977 und 1978 entwickelt
  - Noch heute wichtigstes Public–Key Verfahren
  - Hartes math. Problem: Primzahlfaktorisierung

Blockchiffren: Asymmetrische Verfahren

- Schlüsselerzeugung
  1. *Wähle zwei Primzahlen p und q. Die Länge der Primzahlen sollte mindestens 512 Bit betragen.*
     - Fermat–Test
     - Miller–Rabin–Test
  2. *Berechne n = pq (n hat dann eine Länge von mindestens 1024 Bit)*
     n heißt das RSA Modul

Blockchiffren: Asymmetrische Verfahren

3. *Wähle eine kleine ungerade natürliche Zahl e, die zu $\varphi(n) = (p-1)(q-1)$ relativ prim ist, d.h. es gilt $ggT(e, \varphi(n)) = 1$.*
   e heißt Verschlüsselungsexponent

4. *Berechne d als Lösung der Gleichung*
   $ed \bmod \varphi(n) = 1$
   mit Hilfe des erweiterten euklidischen Algorithmus
   d heißt Entschlüsselungsexponent

Blockchiffren: Asymmetrische Verfahren

Erweiterter euklidischer Algorithmus

- Besagt, dass es Zahlen x, y Є Z gibt, so dass $ggT(a,b) = ax + by$ ist
- Berechnet x und y durch Umkehrung des euklidischen Algorithmus
- Ist d < 0 bilde Inverse: d = $\varphi(n) + d$

Blockchiffren: Asymmetrische Verfahren

Beispiel zum erweiterten euklidischen Algorithmus:

Beispiel: a = 531, b = 93

<u>Euklidischer Algorithmus:</u>

531 = 5 * 93 + 66
93 = 1 * 66 + 27
66 = 2 * 27 + 12
27 = 2 * 12 + 3
12 = 4 * 3 => ggT(531, 93) = 3

<u>Erweiterter euklidischer Algorithmus:</u>

3 = 27 – 2 * 12
= 27 – 2 * (66 – 2 * 27) = -2 * 66 + 5 * 27
= -2 * 66 + 5 * (93 – 1 * 66) = 5 * 93 – 7 * 66
= 5 * 93 – 7 * (531 – 5 * 93)
= -7 * 531 + 40 * 93 => x = -7, y = 40

Blockchiffren: Asymmetrische Verfahren

5. *Gib das Paar P = (e,n) bekannt als öffentlichen Schlüssel.*

6. *Halte das Paar S = (d,n) geheim als geheimen Schlüssel.*

7. *p, q und φ(n) werden nicht mehr benötigt und sollten gelöscht werden*

Blockchiffren: Asymmetrische Verfahren

Beispiel zur Schlüsselerzeugung:

1. ***Als Primzahlen wählt man die Zahlen p = 11 und q = 23.***
2. ***Also ist n = pq = 253***
3. ***φ(n) = (p-1)(q-1) = 220, dazu das kleinstmöglichste e ist e = 3.***
4. ***Der erweiterte euklidische Algorithmus:***

1) 220 = 73 * 3 + 1
3 = 3 * 1 + 0 => ggT(220, 73) = 1
2) 1 = 220 – 73 * 3

Unser d' ist also -73 => d = 220 – 73 = 147

5. ***Öffentlicher Schlüssel P = (3,253)***
6. ***Geheimer Schlüssel S = (147, 253)***

Blockchiffren: Asymmetrische Verfahren

- Verschlüsselung
  - Alphabet dargestellt durch die Zahlen *0* bis *N-1*

1. *Man setze* $k = [\log_N n]$
   k ist die Länge der Klartextblöcke

2. *Verwandle Block* $m_1 \ldots m_k$ *in die Zahl*
   $m = \sum_{i=1}^{k} m_i * N^{k-i}$

Blockchiffren: Asymmetrische Verfahren

3. *Diese Zahl m wird nun durch* $\boldsymbol{c = m^e \bmod n}$ *chiffriert.*

4. *Schreibe die Zahl c wieder zur Basis N*
   Man erhält einen Schlüsselblock $c_1 \ldots c_{k+1}$

Blockchiffren: Asymmetrische Verfahren

Beispiel zur Verschlüsselung:

Das verwendete Alphabet lautet:

0	*a*	*b*	*c*
0	1	2	3

e = 3, n = 253, N = 4 ***Klartext: abb => 122***

1. $k = [\log_4 253] = 3$

2. $m = \sum_{i=1}^{k} m_i * N^{k-i} = 1 * 4^2 + 2 * 4^1 + 2 * 4^0 = 26$

3. $c = 26^3 \bmod 253 = 119$

4. c zur Basis N = 4: $c = 119_{10} = 1 * 4^3 + 3 * 4^2 + 1 * 4^1 + 3 * 4^0 = 1313_4$

Der chiffrierte Text lautet also: acac

Blockchiffren: Asymmetrische Verfahren

- Entschlüsselung

1. *Man setze* $k = [\log_N n]$

   k+1 ist die Länge der Geheimtextblöcke

2. *Verwandle Block* $c_1 \ldots c_{k+1}$ *in die Zahl*

   $$c = \sum_{i=1}^{k+1} c_i * N^{k-i}$$

Blockchiffren: Asymmetrische Verfahren

3. *Diese Zahl c wird nun durch* $\boldsymbol{m = c^d \bmod n}$ *dechiffriert*

4. *Schreibe die Zahl m wieder zur Basis N*
   Man erhält einen Schlüsselblock $m_1 \ldots m_k$

Blockchiffren: Asymmetrische Verfahren

Beispiel zur Entschlüsselung:

Das verwendete Alphabet lautet:

0	*a*	*b*	*c*
0	1	2	3

d = 147, e = 3, n = 253, N = 4 ***Geheimtext: acac => 1313***

1. $k = [\log_4 253] = 3$

2. $c = \sum_{i=1}^{k+1} c_i * N^{k-i} = 1 * 4^3 + 3 * 4^2 + 3 * 4^1 + 1 * 4^0 = 119$

3. $m = 119^{147} \bmod 253 = 26$

4. m zur Basis N = 4: $m = 26_{10} = 1 * 4^2 + 2 * 4^1 + 2 * 4^0 = 122_4$

Der dechiffrierte Text lautet also: abb

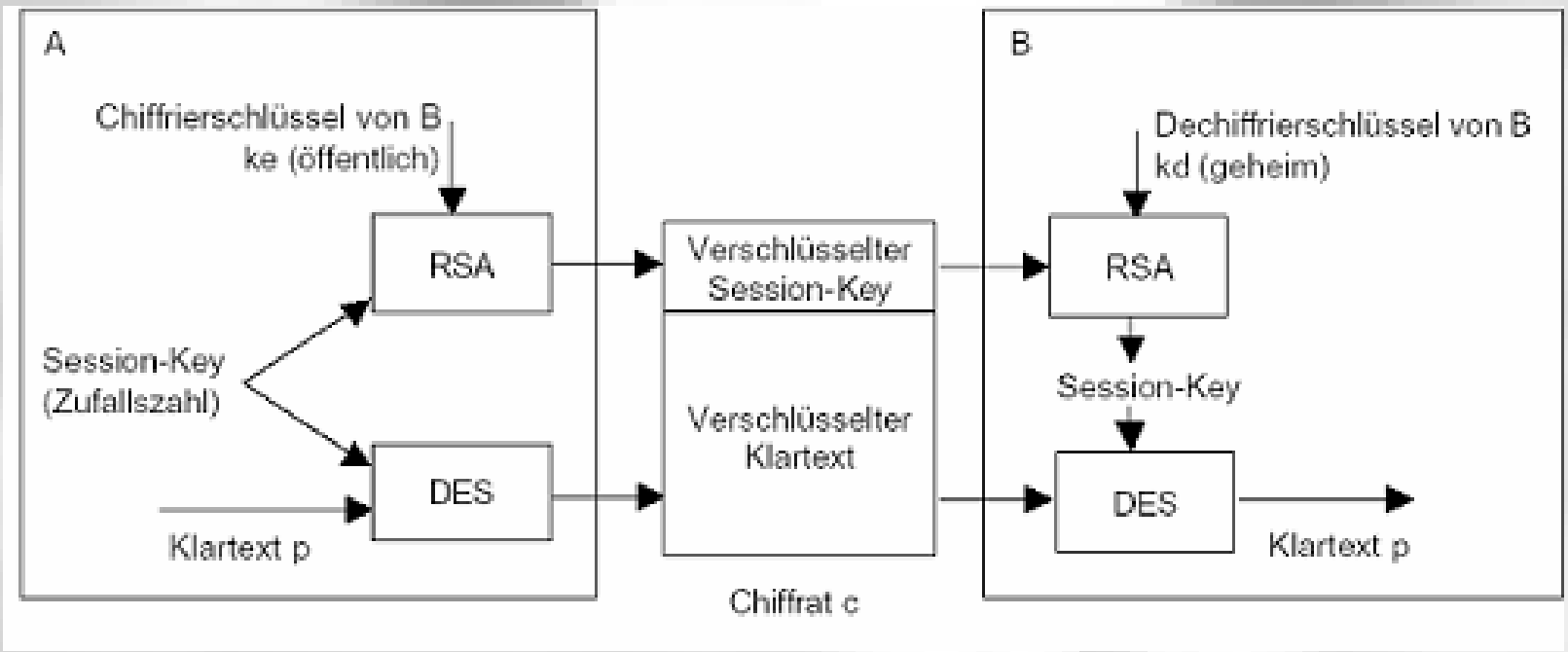
Blockchiffren: Hybrid Verfahren

- Einleitung
- Historisches
- Blockchiffren
  - Symmetrische Verfahren
  - Asymmetrische Verfahren
  - **Hybrid Verfahren**
- Aktuelle Anwendung
- Politische Randbedingungen
- Ausblick

Blockchiffren: Hybrid Verfahren

	symmetrisch	asymmetrisch	
Vorteil	• kurze Schlüssel • Einwegschlüssel • einfache Verfahren • sehr schnell	• lange Schlüssel • Mehrwegschlüssel • komplexe Verfahren • sehr langsam	Nachteil
Nachteil	• Schlüsselübertragung • n(n-1)/2 Schlüssel • feste Schlüssellänge	• Sicherheit • 2n Schlüssel • Skalierbarkeit	Vorteil

Blockchiffren: Hybrid Verfahren



http://wwwfl.ebs.de/Lehrstuehle/Wirtschaftsinformatik/Lehre/IKS/buch18.pdf

Aktuelle Anwendungen

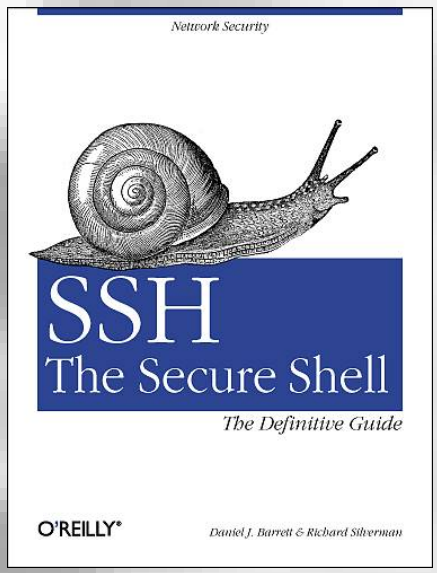
- Einleitung
- Historisches
- Blockchiffren
  - Symmetrische Verfahren
  - Asymmetrische Verfahren
  - Hybrid Verfahren
- **Aktuelle Anwendung**
- Politische Randbedingungen
- Ausblick

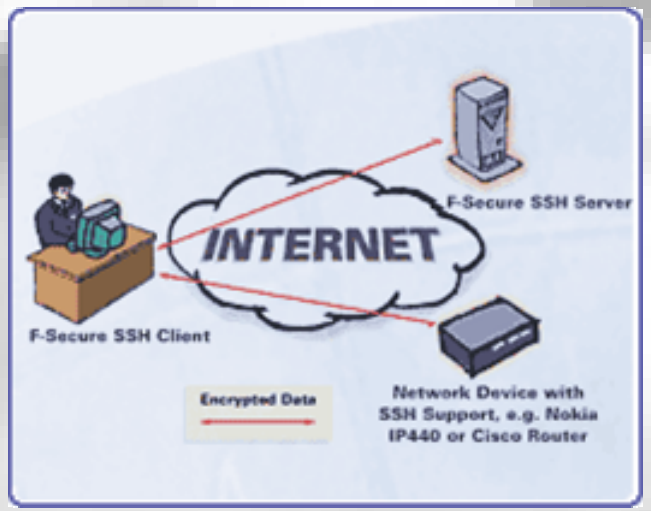
Aktuelle Anwendungen

- PGP (Pretty Good Privacy)
  - Arbeitet mit Hybrid Verfahren
  - Aufgaben
    - Email-Verschlüsselung
    - Digitale Unterschrift
  - Infrastruktur
    - Trust-Centren
      - Schlüsselauthentifizierung

Aktuelle Anwendungen

- SSH (Secure Shell)
  - Benutzt Public-Key-Verfahren zur Authentifizierung
  - Kommunikation zwischen Server und Client wird verschlüsselt





http://www.f-secure.com/estore/ssh.shtml

Politische Randbedingungen

- Einleitung
- Historisches
- Blockchiffren
  - Symmetrische Verfahren
  - Asymmetrische Verfahren
  - Hybrid Verfahren
- Aktuelle Anwendung
- **Politische Randbedingungen**
- Ausblick

Politische Randbedingungen

- Deutschland
  - Kryptographie ist generell erlaubt
  - 1. Signaturgesetz 1997
    - Signaturen sind rechtlich gültig
    - Strenge Vorgaben für Benutzer
    - praktisch kaum durchführbar

  ➡ EU Vorgaben 1999 / Gesetz 2001

Politische Randbedingungen

- USA
  - 1993 bis 1996 Standard EES
    - Clipper Chip codieren und beim NIST hinterlegen
    - richterliche Anordnung zum Abhören
  - Ab 1996 ähnliche Regelungen
  - Mittlerweile liberalere Gesetzesvorschläge

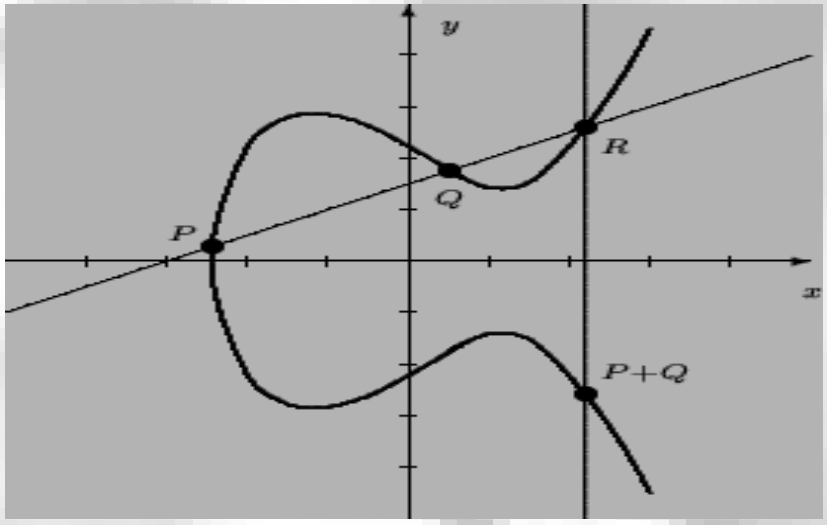
  - Exportgesetz
    - Unterzeichnung des Wassenaar-Abkommens 1996
    - dennoch Exportverbot für Verschlüsselungssoftware
    - Seit kurzem aufgehoben

Ausblick

- Einleitung
- Historisches
- Blockchiffren
  - Symmetrische Verfahren
  - Asymmetrische Verfahren
  - Hybrid Verfahren
- Aktuelle Anwendung
- Politische Randbedingungen
- **Ausblick**

Ausblick

- Elliptische Kurven
  - $y^2 = ax^3 + bx^2 + cx + d$
  - neuen Arithmetik durch elliptische Kurve
  - Verkürzte Schlüssellänge



http://www.roehri.ch/~sr/studium/ecc-semaev/node4.html

Ausblick

- Allgemein
  - Kryptographie wird noch wichtiger
  - bessere Ausnutzung der Vernetzung
  - Bekanntheitsgrad steigt
  - Software wird benutzerfreundlicher

FRAGEN???