Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Einführung IT Security

Kapitel 2

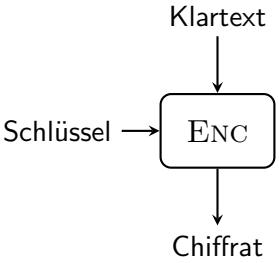
Verschlüsselungsverfahren

Moderne Kryptologie

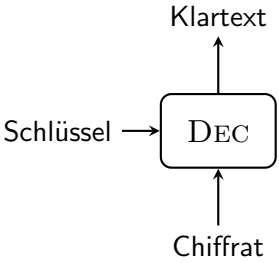
Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

	symmetrische Kryptologie	**asymmetrische Kryptologie**
Vertraulichkeit	symmetrische Verschlüsselung	asymmetrische Verschlüsselung
Integrität	MAC	Signaturen
Authentizität		PKI
Schlüsselaustausch	symmetrischer Schlüsselaustausch	asymmetrischer Schlüsselaustausch
Kryptoanalyse	symmetrische Kryptoanalyse	Mathematik
	Implementierungsangriffe	
	Seitenkanalanalyse	
Bausteine	Hashfunktionen	
	⋮	⋮

Verschlüsselung

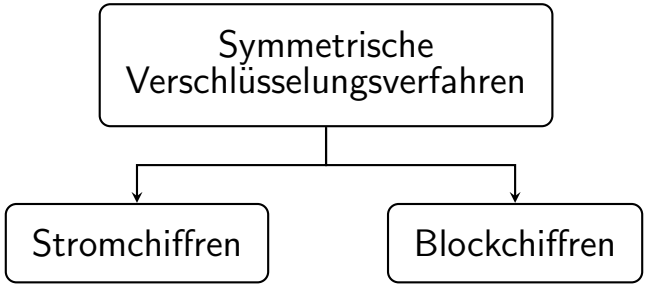


Entschlüsselung

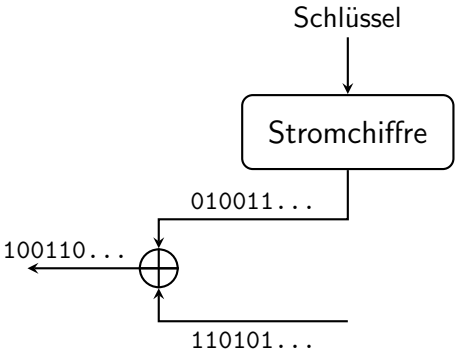


Korrektheit: $\mathrm{DEC}(\mathrm{ENC}(m)) = m$

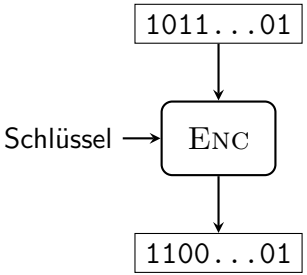
Symmetrische Verschlüsselungsverfahren



Symmetrische Verschlüsselungsverfahren

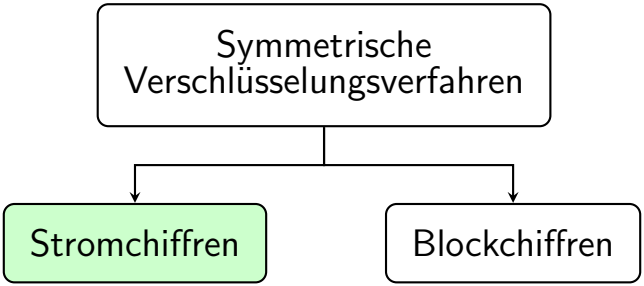


- Pseudozufallszahlengenerator
- erzeugt Schlüsselstrom
- Verknüpfung mit Klartextstrom mit XOR
- Ergebnis ist Chiffratstrom



Blockchiffre

- zufällige Permutation
  (*random permutation*)
- Eingabe ist Klartextblock fester Länge
- Ausgabe ist Chiffratblock gleicher Länge


Symmetrische
Verschlüsselungsverfahren
Stromchiffren
Blockchiffren

XOR

XOR - exklusives Oder

$\oplus$	0	1
0	0	1
1	1	0

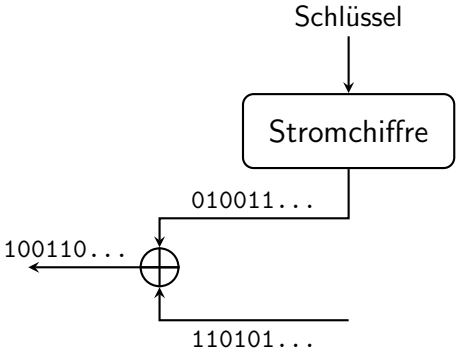
reversible Verknüpfung:

$b \oplus k = c$

$c \oplus k = b$

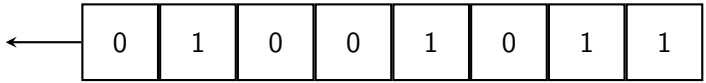
Korrektheit: $(b \oplus k) \oplus k = b$

Stromchiffren

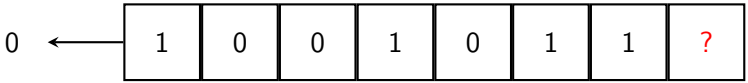


- Pseudozufallszahlengenerator
- erzeugt Schlüsselstrom
- Verknüpfung mit Klartextstrom mit XOR
- Ergebnis ist Chiffratstrom

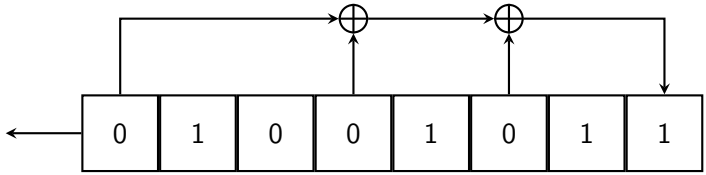
Linear Rückgekoppelte Schieberegister



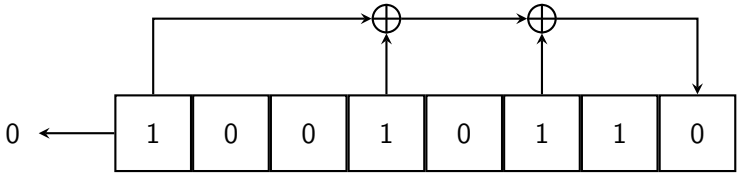
Linear Rückgekoppelte Schieberegister



Linear Rückgekoppelte Schieberegister

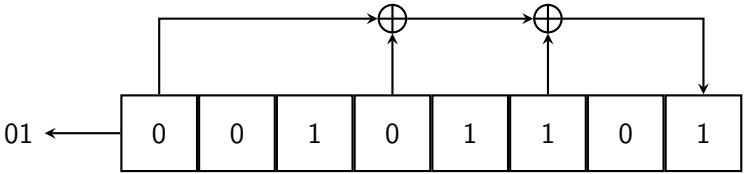


Linear Rückgekoppelte Schieberegister



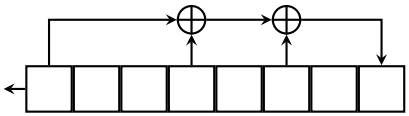
LFSR: *linear-feedback shift register*

Linear Rückgekoppelte Schieberegister



LFSR: *linear-feedback shift register*

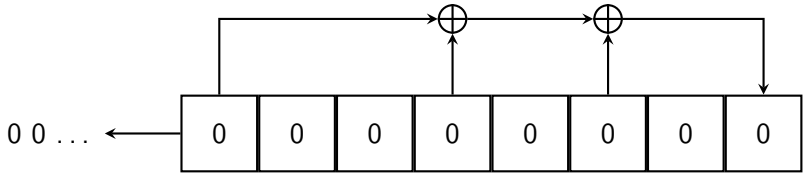
Periode von LFSR



Wie viele verschiedene Zustände kann ein LFSR der Länge n haben?

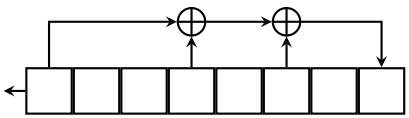
2^n interne Zustände sind möglich, aber...

Linear Rückgekoppelte Schieberegister



nur Nullen $\rightarrow$ LFSR bleibt im Null-Zustand

Periode von LFSR



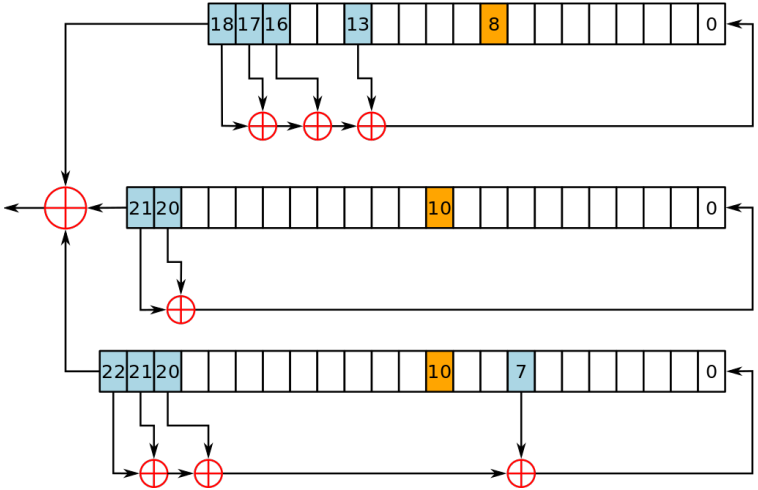
Bei „guter“ Wahl der Rückkopplung hat ein LFSR der Länge n eine Persiode der Länge $2^n - 1$.


Schlüsselstrom
0100101101...
Chiffratstrom
1111100011...
Schlüsselstrom
0100101101...
1011001110...
Klartextstrom
1011001110...
Klartextstrom

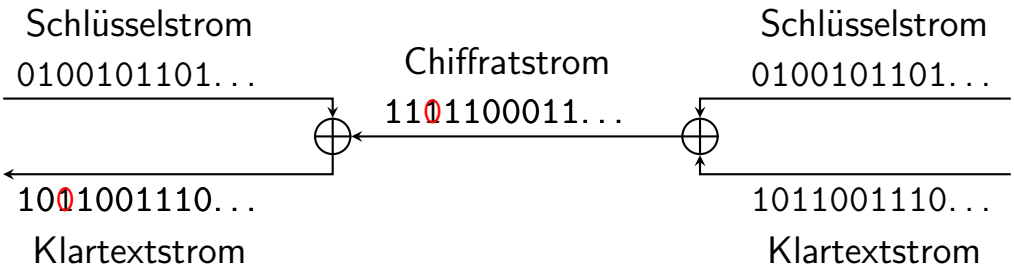
bekannter Klartext $\rightarrow$ Schlüsselstrom

LFSR-Stromchiffren kombinieren mehrere LSFR

LFSR-Stromchiffre A5/1



User:Matt Cryptoderivative work: Tsaitgaist (talk) - A5-1.png, Gemeinfrei



bitflip im Chiffratstrom → *bitflip* im entschlüsselten Klartextstrom an der gleichen Position

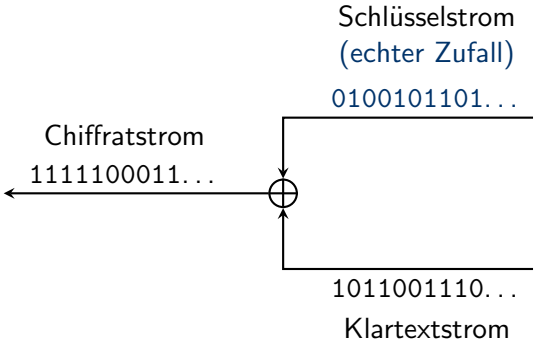
Vorteile

- beliebige Klartextlänge
- Auswirkungen von Übertragungsfehlern gering
- (schnell & günstig)

Nachteile

- bekannter Klartext $\rightarrow$ Schlüsselstrom $\rightarrow$ Kryptoanalyse
  einfache LFSR sind unsicher
- Manipulation des Chiffrats möglich
- ältere Stromchiffren oft unsicher

One-Time-Pad



- Verschlüsselung mit echtem Zufall
- informationstheoretisch sicher

One-Time-Pad

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

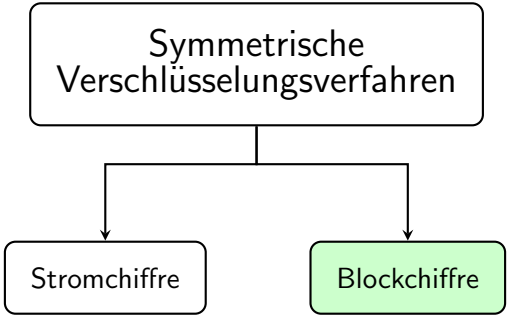
Perfekte Sicherheit...

Zu jedem Chiffrat gibt es für jeden möglichen Klartext einen Schlüssel, der das Chiffrat zu diesem Klartext entschlüsselt.

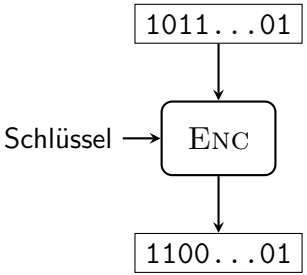
...aber

- Verschlüsselung mit *echtem* Zufall
- Schlüssel so lang wie die Nachricht
- Schlüssel nur einmal nutzbar
- kein Schutz gegen Manipulation (nur Vertraulichkeit, keine Integrität)
- Schlüssel muss sicher ausgetauscht werden Quantenschlüsselaustausch (QKD) will dies lösen

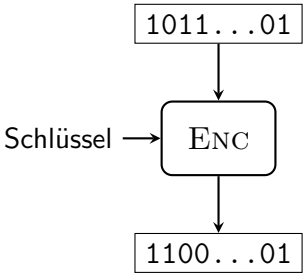
Die Verwendung eines One-Time-Pad ist keine Garantie für perfekte Sicherheit in der Praxis, sondern bestenfalls eine Voraussetzung.


Symmetrische Verschlüsselungsverfahren
Stromchiffre
Blockchiffre

Blockchiffren



- zufällige Permutation (*random permutation*)
- Eingabe ist Klartextblock fester Länge
- Ausgabe ist Chiffratblock gleicher Länge



Blockchiffre

- zufällige Permutation
  (*random permutation*)
- Eingabe ist Klartextblock fester Länge
- Ausgabe ist Chiffratblock gleicher Länge

Blockchiffren

26 Buchstaben
→ 26! Permutationen

A	↔	a
B	↔	b
⋮		⋮
F	↔	f
G	↔	h
H	↔	g
⋮		⋮
Z	↔	z

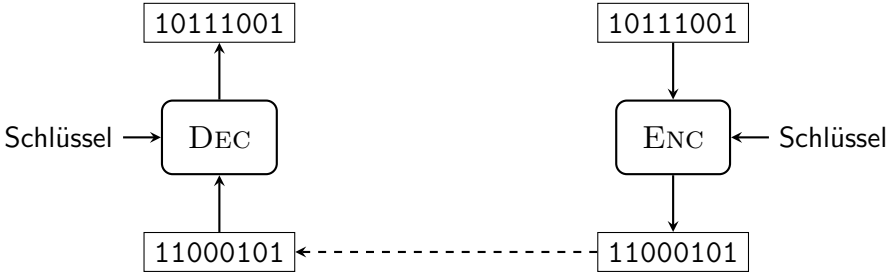
Blocklänge n
→ 2^n! verschiedene Permutationen

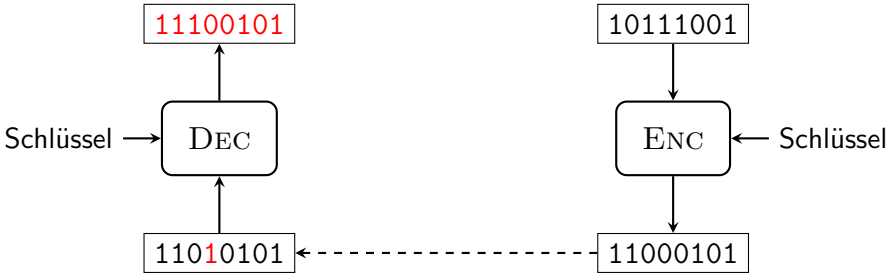
0000	↔	0000
0001	↔	0001
⋮		⋮
1001	↔	1010
1010	↔	1001
⋮		⋮
1111	↔	1111

Blockchiffren

gewünschte Eigenschaften

- schnell & effizient
- kurze Schlüssel
- nur „gute“ Permutationen


10111001
10111001
Schlüssel
DEC
ENC
Schlüssel
11000101
11000101


11100101
10111001
Schlüssel
DEC
ENC
Schlüssel
11010101
11000101
Übertragungsfehler

Eigenschaften Blockchiffren

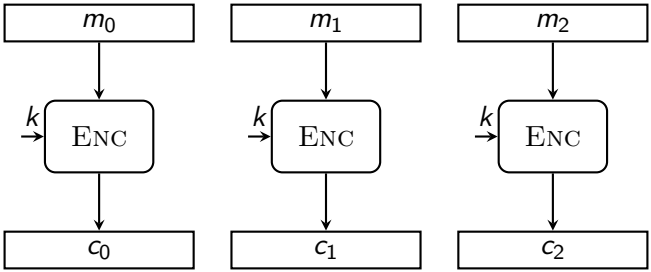
Vorteile

- Rückschlüsse auf Schlüssel schwer

Nachteile

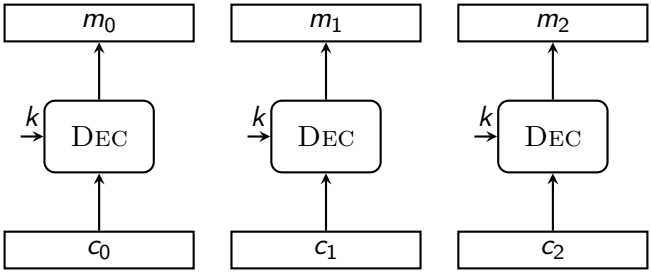
- Ver- und Entschlüsselung:
  nur ganze Blöcke
- Übertragungsfehler „zerstören“ Block

Electronic Codebook Mode – ECB



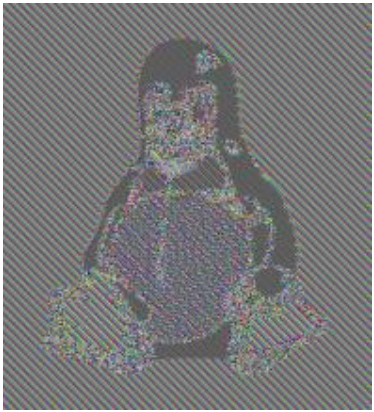
Verschlüsselung

Electronic Codebook Mode – ECB



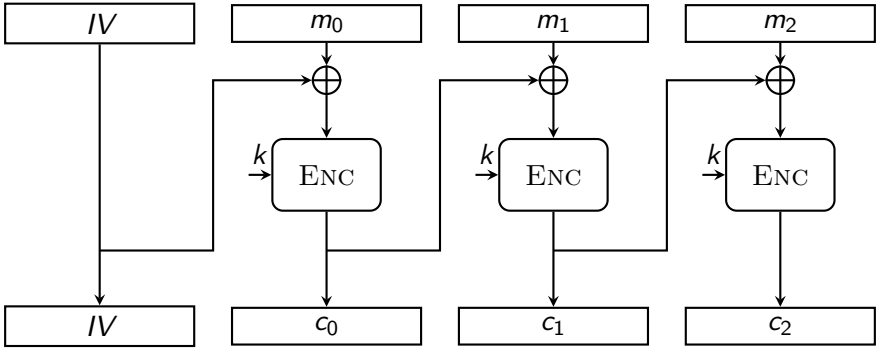
Entschlüsselung

Attribution



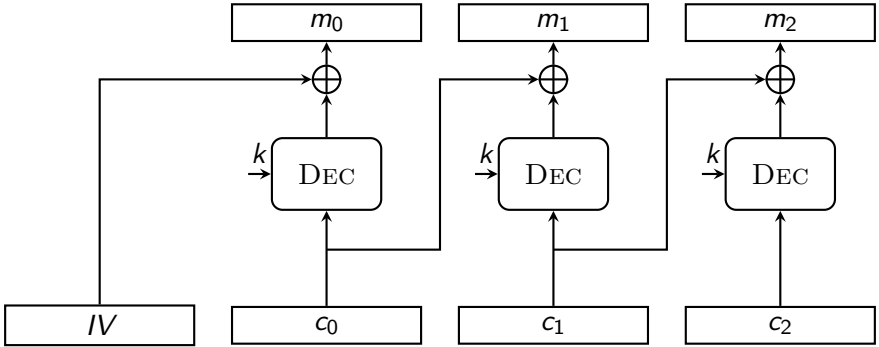
By en:User:Lunkwill

Cipherblock Chaining Mode – CBC



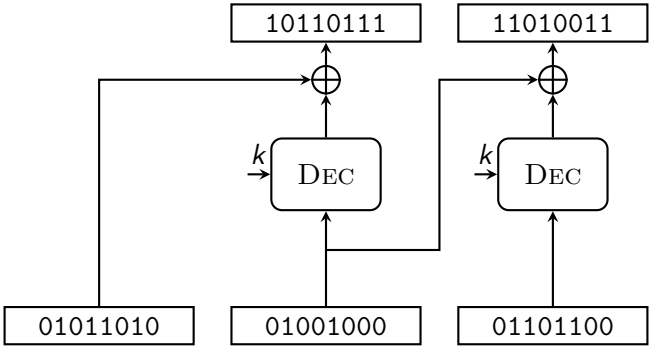
Verschlüsselung

Cipherblock Chaining Mode – CBC



Entschlüsselung

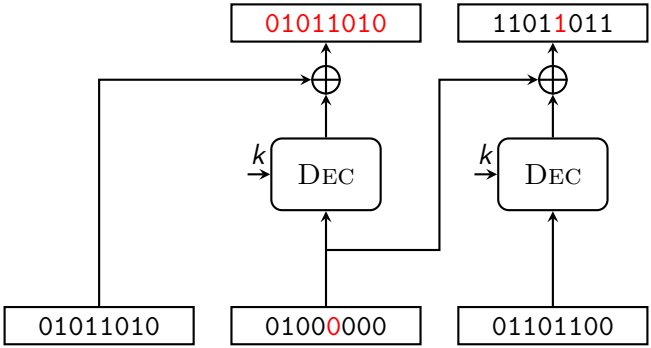
Fehlerfortpflanzung CBC



bitflip im Chiffratblock → zugehöriger Klartextblock „zerstört“

→ *bitflip* im nachfolgenden Klartextblock an der gleichen Position

Fehlerfortpflanzung CBC



bitflip im Chiffratblock → zugehöriger Klartextblock „zerstört“

→ *bitflip* im nachfolgenden Klartextblock an der gleichen Position

Eigenschaften CBC

Vorteile

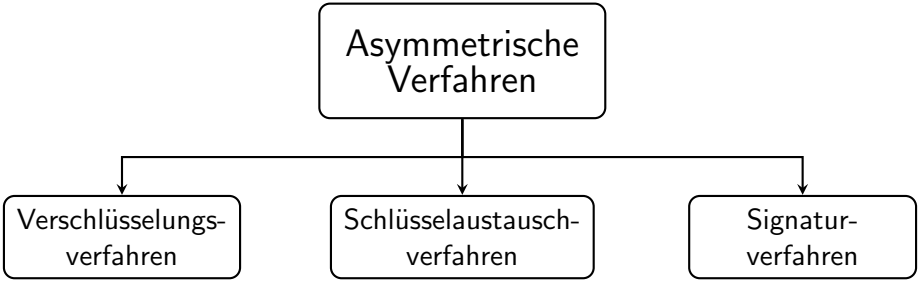
- wahlfreier Zugriff möglich
- durch IV: probabilistisch

Nachteile

- IV nur einmal nutzbar (NONCE)
- Fehlerfortpflanzung

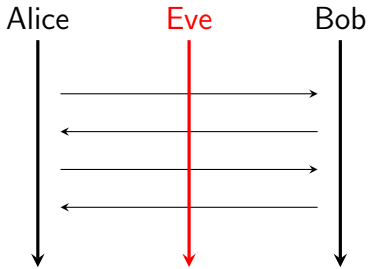
	symmetrische Kryptologie	**asymmetrische Kryptologie**
Vertraulichkeit	symmetrische Verschlüsselung	asymmetrische Verschlüsselung
Integrität	MAC	Signaturen
Authentizität		PKI
Schlüsselaustausch	symmetrischer Schlüsselaustausch	asymmetrischer Schlüsselaustausch
Kryptoanalyse	symmetrische Kryptoanalyse	Mathematik
	Implementierungsangriffe	
	Seitenkanalanalyse	
Bausteine	Hashfunktionen	
	⋮	⋮

Asymmetrische Verschlüsselungsverfahren



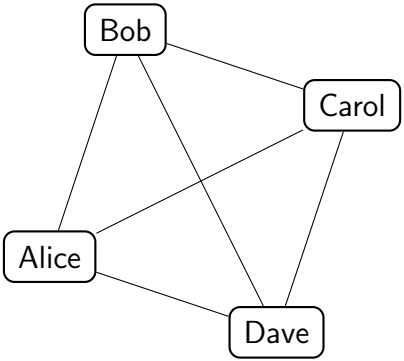
Alice und Bob möchten verschlüsselt kommunizieren.

Alice und Bob haben keinen sicheren Kanal und kein gemeinsames Geheimnis.

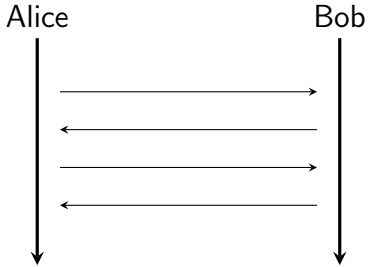


n Parteien möchten verschlüsselt kommunizieren.

Dazu benötigen sie $\frac{n \cdot (n-1)}{2}$ symmetrische Schlüssel.



Schlüsselaustauschproblem
galt lange als unlösbar.



Merkle's Puzzle

Alice möchte

- eine Nachricht an Bob schicken,
- die nur Bob lesen kann,
- ohne gemeinsames Geheimnis.

Alice soll nur verschlüsseln!

Einwegfunktion mit Falltür

Jeder kann die Einwegfunktion benutzen (verschlüsseln).

Nur der Empfänger kennt die Falltür (trapdoor) und kann die Funktion invertieren (entschlüsseln).

Merkle's Puzzle

Ralph Merkle: 1974 (veröffentlicht 1978)

Vorschlag für Projekt im Studium

Beginn der Public-Key-Kryptography

Idee

Bob veröffentlicht Puzzle (Rätsel) mit ID und symmetrischen Schlüssel.

Alice bricht Puzzle (Brute-Force), verschlüsselt mit dem Schlüssel und sendet Chiffrat mit ID an Bob.

Bob entschlüsselt mit dem zur ID zugehörigen Schlüssel.

KeyGen

Öffentlicher Schlüssel

- Menge von Chiffraten mit kurzen Schlüsseln κ_i
- Klartext ist eine ID und ein langer Schlüssel k_i

$$\begin{gathered}\textsc{Enc}_{\kappa_1}(\mathsf{ID}_1, k_1) \\ \vdots \\ \textsc{Enc}_{\kappa_i}(\mathsf{ID}_i, k_i) \\ \vdots \\ \textsc{Enc}_{\kappa_n}(\mathsf{ID}_n, k_n)\end{gathered}$$

Geheimer Schlüssel

- Tabelle mit ID_i und k_i

$$\begin{gathered}(\mathsf{ID}_1, k_1) \\ \vdots \\ (\mathsf{ID}_i, k_i) \\ \vdots \\ (\mathsf{ID}_n, k_n)\end{gathered}$$

Enc

1. wähle zufälliges Chiffrat i des öffentlichen Schlüssels
2. rate κ_i (brute force) und entschlüssele gewähltes Chiffrat
3. verschlüssel Nachricht m mit k_i
4. sende $(\mathrm{ID}_i, \mathrm{Enc}_{k_i}(m))$

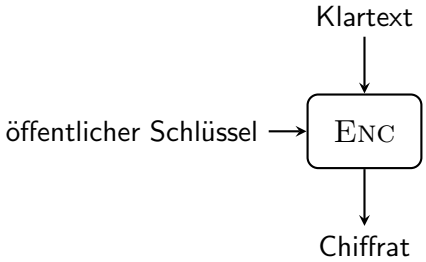
Dec

1. lese ID_i
2. wähle zugehörigen k_i aus Tabelle
3. entschlüssele $\mathrm{Enc}_{k_i}(m)$

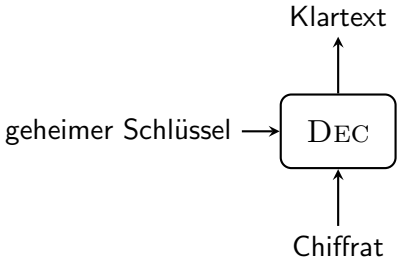
Nachteile

- hoher Aufwand für Verschlüsselung
- großer öffentlicher Schlüssel
- Schlüssel wird „verbraucht“
- geringer Vorteil gegenüber Angreifer ($O(2^n)$ vs. $O(2^{2n})$)

Verschlüsselung



Entschlüsselung



Asymmetrische Verschlüsselungsverfahren

definiert durch drei Algorithmen

- KeyGen
- Enc
- Dec

öffentlicher Schlüssel (*public key*) pk

geheimer Schlüssel (*secret key*) sk

oft auch: Public-Key Kryptografie (PKK)

$\text{KeyGen}() = (sk, pk)$

$\text{Enc}(pk, m) = c$

$\text{Dec}(sk, c) = m$

Korrektheit

$\text{Dec}(sk, \text{Enc}(pk, m)) = m$

Rivest, Shamir, Adleman 1977

- erstes publiziertes PKK-Verfahren
- weit verbreitet
- Grundlage für Verschlüsselungs- und Signaturverfahren

Sicherheit basiert auf Faktorisierung

Rechnen modulo n

$5 + 4 = 2 \bmod 7$

$5 \cdot 4 = 6 \bmod 7$

Potenzieren modulo n

$5^4 = 1 \bmod 7$

KeyGen

1. wähle zwei Primzahlen $p, q \in \mathbb{P}$
2. berechne $n = p \cdot q$
3. wähle e, d mit
   $e \cdot d = 1 \mod (p-1)(q-1)$
4. öffentlicher Schlüssel (e, n)
5. geheimer Schlüssel (d, n)

Verschlüsselung $\text{Enc}(e, m)$

$c = m^e \mod n$

Entschlüsselung $\text{Dec}(d, m)$

$m = c^d \mod n$

Korrektheit

$c^d = (m^e)^d = m \bmod n$

Sicherheit

Sicherheit beruht auf der Schwierigkeit, n in die Faktoren p und q zu zerlegen.

Taher ElGamal 1985

- weit verbreitet
- Verschlüsselungsverfahren
- verwandt mit Signaturverfahren

Sicherheit basiert auf dlog-Problem.

diskreter Logarithmmus

gegeben	Modulus n, Basis g und Zahl y
gesucht	x so dass $y = g^x \bmod n$

Der Logarithmus in $\mathbb{R}$ ist leicht zu berechnen.

Der diskrete Logarithmus (dlog) modulo n ist schwer zu berechnen.

KeyGen

1. gegeben $p \in \mathbb{P}$ und $g < p$
2. wähle x, berechne $y = g^x \bmod p$
3. öffentlicher Schlüssel (y, p)
4. geheimer Schlüssel (x, p)

Verschlüsselung $\mathrm{Enc}(y, m)$

1. $r \leftarrow \{1, \ldots, p-1\}$
2. $c_1 = g^r \bmod p$
3. $c_2 = y^r \cdot m \bmod p$
4. $c = (c_1, c_2)$

Entschlüsselung $\mathrm{Dec}(c, x)$

$m = (c_1^x)^{-1} \cdot c_2 \bmod p$

Korrektheit

$(c_1^x)^{-1} \cdot c_2 = ((g^r)^x)^{-1} \cdot y^r \cdot m =$
$g^{-rx} \cdot g^{rx} \cdot m = m \bmod p$

Sicherheit

Sicherheit beruht auf der Schwierigkeit, den diskreten Logarithmus x modulo p aus $y = g^x \bmod p$ zu berechnen.

Asymmetrische Verschlüsselungsverfahren

Vorteile

- löst Schlüsselaustauschproblem
- vereinfacht Schlüsselmanagement
- beweisbare Sicherheitsaussagen

Nachteile

- langsam & teuer
- „große“ Schlüssel
- Sicherheit beruht auf mathematischen Problemen
- begrenzte Klartextlänge

Hybride Verschlüsselung

Praxis: Kombination aus symmetrischer und asymmetrischer Verschlüsselung

Schlüsseltransport

symmetrischer Schlüssel k, verschlüsselt mit Public-Key Verschlüsselung

key encapsulation

key transport

Datenverschlüsselung

Nutzdaten verschlüsselt mit symmetrischer Verschlüsselung und k

Verschlüsselung schützt die Vertraulichkeit, nicht die Integrität.

Moderne Kryptologie

	symmetrische Kryptologie	**asymmetrische Kryptologie**
Vertraulichkeit	symmetrische Verschlüsselung	asymmetrische Verschlüsselung
Integrität	MAC	Signaturen
Authentizität		PKI
Schlüsselaustausch	symmetrischer Schlüsselaustausch	asymmetrischer Schlüsselaustausch
Kryptoanalyse	symmetrische Kryptoanalyse	Mathematik
	Implementierungsangriffe	
	Seitenkanalanalyse	
Bausteine	Hashfunktionen	
	⋮	⋮

DH-Schlüsselaustausch

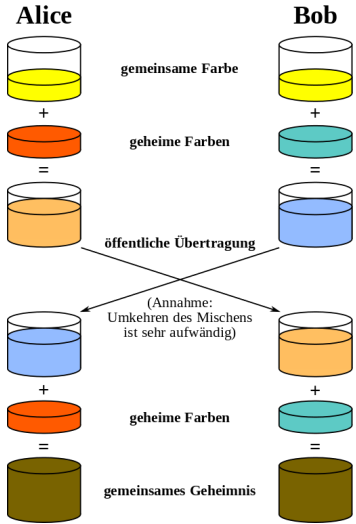
Diffie, Hellman 1976

- erstes asymmetrisches Verfahren
- oft DHKE (Diffie-Hellman Key-Exchange)
- auch Diffie-Hellman-Merkle-Schlüsselaustausch
- eigentlich Schlüsselvereinbarung
- essentieller Bestandteil vieler moderner Protokolle

Sicherheit basiert auf dlog-Problem.

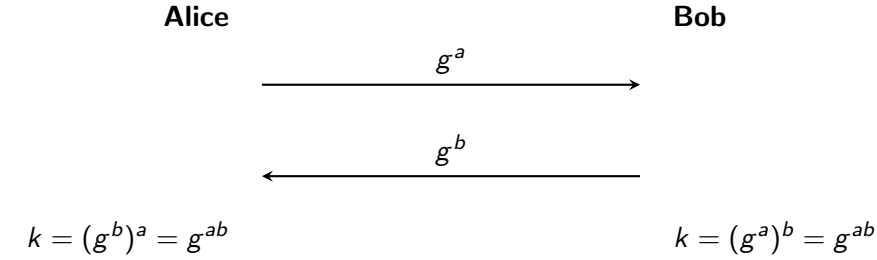
Farben

1. Alice wählt geheime Farbe und mischt diese mit der öffentlichen Farbe.
2. Bob wählt geheime Farbe und mischt diese mit der öffentlichen Farbe.
3. Alice sende gemischte Farbe an Bob.
4. Bob sendet gemischte Farbe an Alice.
5. Alice mischt ihre geheime Farbe zur Farbe von Bob.
6. Bob mischt seine geheime Farbe zur Farbe von Alice.
7. Alice und Bob erhalten die gleiche Farbe.



A.J. Han Vinck, University of Duisburg-Essen, Gemeinfrei

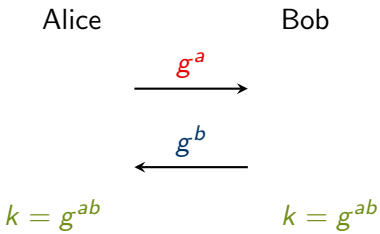
Key Agreement: Diffie-Hellman Key Exchange (DHKE)



Der Diffie-Hellman-Schlüsselaustausch ist eigentlich eine Schlüsselvereinbarung (*key agreement*): Beide Protokollteilnehmer beeinflussen den Schlüssel.

DH-Schlüsselaustausch & ElGamal

Diffie-Hellman Key Exchange (DHKE)



ElGamal

$$
\begin{aligned}
pk &= g^a \\
\text{ENC}(\text{pk},\text{m}) &= (c_1, c_2) \\
c_1 &= g^r \\
c_2 &= (g^a)^r \cdot m = k \cdot m
\end{aligned}
$$

DH-Schlüsselaustausch und ElGamal sind eng verwandt:

- pk von ElGamal entspricht erster Nachricht von DHKE
- c_1 von ElGamal entspricht zweiter Nachricht von DHKE
- c_2 von ElGamal entspricht $k \cdot m$, wobei k das gemeinsame Geheimnis von DHKE ist

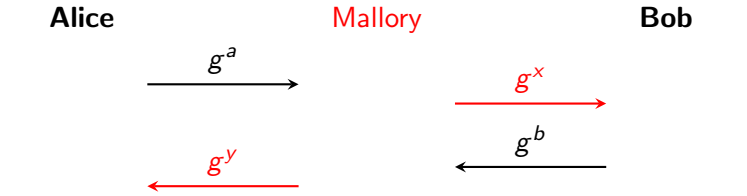
Einsatz von DHKE

- TLS
- SSH
- IPSec
- ...

Problem

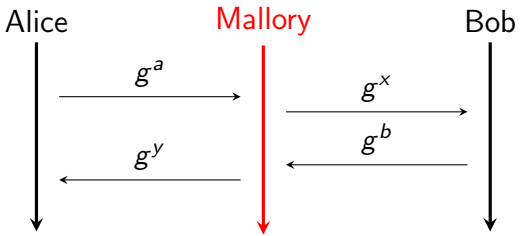
DHKE ist anfällig für
Man-in-the-Middle-Angriff

DH-Schlüsselaustausch



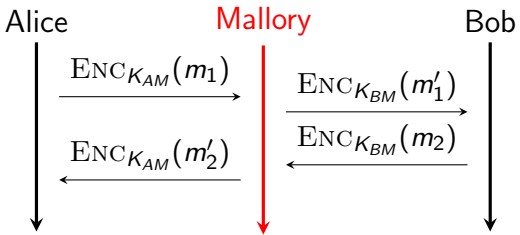
Man-in-the-Middle

- Alice und Mallory teilen sich $K_{AM} = g^{ay}$
- Mallory und Bob teilen sich $K_{BM} = g^{bx}$



Man-in-the-Middle

- Alice und Mallory teilen sich $K_{AM} = g^{ay}$
- Mallory und Bob teilen sich $K_{BM} = g^{bx}$
- Kommunikation zwischen Alice und Bob läuft über Mallory



Snake Oil

Snake Oil (Schlangenöl) wird häufig als Bezeichnung für Produkte verwendet, die mit großen Versprechungen beworben werden, aber teuer und unwirksam sind.

Warnsignale

- pseudomathematischer Blödsinn

Meganet:
„VME beruht auf einer virtuellen Matrix, eine Matrix mit binären Werten, die theoretisch unendlich groß ist und daher keine sich wiederholenden Werte hat. Die zu verschlüsselten Daten werden mit dem Inhalt der virtuellen Matrix verglichen. Wenn eine Übereinstimmung gefunden wurde, werden Zeiger generiert, die angeben, wie man sich in der virtuellen Matrix bewegt. Diese Zeigermenge (die ohne die korrekte virtuelle Matrix nutzlos sind) werden dann mit einer Reihe von Algorithmen in verschiedenen Stadien verschlüsselt, um einen Lawineneffekt zu erreichen.“

Warnsignale

- pseudomathematischer Blödsinn

Cennoid:
„Da Schlüssellänge und -struktur variieren und da die Verschlüsselung keinen mathematischen Algorithmus benutzt ist Rückentwicklung unmöglich und Raten keine Option.“

Warnsignale

- pseudomathematischer Blödsinn

US Data Security:
„Von einem mathematischen Standpunkt aus ist der TTM Algorithmus intuitiv natürlich und weniger schwerfällig als Methoden, die auf Zahlentheorie beruhen.“

Warnsignale

- pseudomathematischer Blödsinn

Singularics:
„Unsere Weiterentwicklungen im Bereich der Zahlentheorie haben zu einem neuen Bereich der Mathematik geführt, der Neutronics genannt wird. Neutronische Funktionen machen es erstmals möglich, Regionen der Mathematik zu analysieren, die bisher als undefiniert galten, so wie der Punkt, an dem 1 durch 0 geteilt wird. Kurzgesagt, wir haben einen völlig neuen Weg gefunden, undefinierte Punkte zu analysieren, wie in der höheren Mathematik immer wieder anzutreffen sind.“

Warnsignale

- pseudomathematischer Blödsinn
- neue Mathematik

- Chaostheorie
- Neural Networks
- Kodierungstheorie
  Achtung! Hier gibt es durchaus ernste Vorschläge.
- Zetafunktion
- Genetik

Warnsignale

- pseudomathematischer Blödsinn
- neue Mathematik
- revolutionäre Durchbrüche

Warnsignale

- pseudomathematischer Blödsinn
- neue Mathematik
- revolutionäre Durchbrüche
- proprietäre Kryptographie

Denken Sie an Kerckhoffs' Prinzip!

Warnsignale

- pseudomathematischer Blödsinn
- neue Mathematik
- revolutionäre Durchbrüche
- proprietäre Kryptographie
- Ahnungslosigkeit

Kryptochef Detlef Granzow:
„Warum ist 256 Bit die technisch höchste Verschlüsselungstiefe die überhaupt auf Computern möglich ist?
[...]
Sie können selbstverständlich natürlich auch noch nacheinander mehrfach verschlüsseln, sogar bis zur Unendlichkeit, wobei dabei die Verschlüsselungstiefe dadurch nicht größer werden kann. Mehr als 256 bit (Vollbit) geht nun mal nicht.“

Warnsignale

- pseudomathematischer Blödsinn
- neue Mathematik
- revolutionäre Durchbrüche
- proprietäre Kryptographie
- Ahnungslosigkeit
- lächerliche Schlüssellängen

Crypteto:
„Die wichtigste Eigenschaft eines Verschlüsselungsverfahrens in die Schlüssellänge. Der bis heute stärkste bekannte Algorithmus benutzt einen 448-Bit Schlüssel. Crypteto bietet jetzt einen 49.152-Bit Schlüssel. Das bedeutet für jedes einzelne zusätzliche Bit bietet Crypteto 100% mehr Sicherheit gegenüber der Konkurrenz. Die Sicherheit und Geheimhaltung, die dadurch erreicht wird, ist überwältigend.“

Warnsignale

- pseudomathematischer Blödsinn
- neue Mathematik
- revolutionäre Durchbrüche
- proprietäre Kryptographie
- Ahnungslosigkeit
- lächerliche Schlüssellängen

Meganet:
„1 Millionen Bit symmetrische Schlüssellänge – Der Markt bietet nur 40 bis 160 Bit.“

Warnsignale

- pseudomathematischer Blödsinn
- neue Mathematik
- revolutionäre Durchbrüche
- proprietäre Kryptographie
- Ahnungslosigkeit
- lächerliche Schlüssellängen
- One-Time-Pad

IT–5D Sicherheit in Raum Zeit und Zufall:
„Das Akronym HROTP bezeichnet die Hyper-Raum-One-Time-Pad-Verschlüsselung. [...] Schaut man sich das HROTP-Verfahren an, so ist sofort erkennbar, dass HROTP nichts mit dem Vernam-OTP gemeinsames hat. HROTP-Verfahren wurde deshalb als eine One-Time-Pad-Verschlüsselung klassifiziert, weil es die Shannon-Bedingungen für eine hohe Hackerresistenz erfüllt.“

Warnsignale

- pseudomathematischer Blödsinn
- neue Mathematik
- revolutionäre Durchbrüche
- proprietäre Kryptographie
- Ahnungslosigkeit
- lächerliche Schlüssellängen
- One-Time-Pad
- unbelegte Behauptungen

Meganet:
„VME98 (Virtual Matrix Encryption) ist das stärkste erhältliche Verschlüsselungsprodukt auf dem Markt und enthält den unbrechbaren Virtual Matrix Algorithmus und einen 1 MILLION BIT symmetrischen Schlüssel.“

Warnsignale

- pseudomathematischer Blödsinn
- neue Mathematik
- revolutionäre Durchbrüche
- proprietäre Kryptographie
- Ahnungslosigkeit
- lächerliche Schlüssellängen
- One-Time-Pad
- unbelegte Behauptungen
- Schlagworte

Beispiele:

- military grade
- patentiert
- zertifiziert
- schneller als AES
- cracking contests
- Schlüsselwiedergewinnung (key recovery)