



IT-Sicherheit

04 Kryptographie

Gerrit.Kalkbrenner@hwr-berlin.de

Teile:
Norbert Pohlmann



- **Ziele und Ergebnisse der Vorlesung**
- **Einführung**
- **Grundlagen der Verschlüsselung**
- **Elementarverschlüsselung**
- **Symmetrische oder Private-Key Verschlüsselungsverfahren**
- **Asymmetrische oder Public-Key Verschlüsselungsverfahren**
- **One-Way-Hashfunktionen**
- **Zusammenfassung**



- **Ziele und Ergebnisse der Vorlesung**
- Einführung
- Grundlagen der Verschlüsselung
- Elementarverschlüsselungen
- Symmetrische oder Private-Key Verschlüsselungsverfahren
- Asymmetrische oder Public-Key Verschlüsselungsverfahren
- One-Way-Hashfunktionen
- Zusammenfassung



Ziele und Ergebnisse der Vorlesung

- Gutes Verständnis für **kryptographische Verfahren** und ihre Anwendungen.
- Erlangen der Kenntnisse über den **Aufbau**, die **Prinzipien**, die **Architektur** und die **Funktionsweise** von kryptographischen Verfahren.
- Einen guten **Überblick** über aktuelle **kryptographische Verfahren**.



- Ziele und Ergebnisse der Vorlesung
- **Einführung**
- Grundlagen der Verschlüsselung
- Elementarverschlüsselungen
- Symmetrische oder Private-Key Verschlüsselungsverfahren
- Asymmetrische oder Public-Key Verschlüsselungsverfahren
- One-Way-Hashfunktionen
- Zusammenfassung



Einführung

- **Vertraulichkeit**
 - Transformation einer
verständlichen Informationsdarstellung
in eine
nicht verständliche Informationsdarstellung



Einführung

- seit 6000 Jahren gibt es Schrift, seit rund 3000 Jahren Verschlüsselung und seitdem auch den Versuch, die Verschlüsselung zu knacken!
- Romeo und Julia
- Mary Stuart und das Babington-Komplott 1586
- Eintritt der USA in 1. Weltkrieg: Zimmermann-Telegramm
- Enigma-Entschlüsselung, zweiter Weltkrieg
- Nutzung offener Netze
- Motivation: Verschlüsselungstechniken



Zimmerman- Depesche

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

GERMAN LEGATION
MEXICO CITY

via Galveston

JAN 19 1917

862.2012/12A

130	13042	13401	8501	115	3528	416	17214	6491	11310
18147	18222	21560	10247	11518	23677	13605	3494	14936	
98092	5905	11311	10392	10371	0302	21290	5161	39695	
23571	17504	11269	18276	18101	0317	0228	17694	4473	
23284	22200	19452	21589	67893	5569	13918	8958	12137	
1333	4725	4458	5905	17166	13851	4458	17149	14471	6706
13850	12224	6929	14991	7382	15857	67893	14218	36477	
5870	17553	67893	5870	5454	16102	15217	22801	17138	
21001	17388	7446	23638	18222	6719	14331	15021	23845	
3156	23552	22096	21604	4797	9497	22464	20855	4377	
23610	18140	22260	5905	13347	20420	39689	13732	20667	
6929	5275	18507	52262	1340	22049	13339	11265	22295	
10439	14814	4178	6992	8784	7632	7357	6926	52262	11267
21100	21272	9346	9559	22464	15874	18502	18500	15857	
2188	5376	7381	98092	16127	13486	9350	9220	76036	14219
5144	2831	17920	11347	17142	11264	7667	7762	15099	9110
10482	97556	3569	3670						

BEPNSTOPFF.

Charge German Embassy.



Enigma

- Chiffriergerät der Wehrmacht





→ Motivation: Kryptographie im Alltag

- Telefonkarten
- Fernbedienungen
- Mobilfunk (Handys, SIM-Karte) -> Authentikation, Verschlüsselung
- Nummerncodierung der Geldscheine
- Electronic cash (ec), HBCI, SET, ec-Karte, Bankenkarte ... Bitcoin, ...
- Geldautomaten
- Wegfahrsperre im Auto (Autoschlüssel)
- Electronic games (Lotto, virtual casino)
- Online trading and marketplace (secure authentication)
- Multimedia services (video on demand)
- (Wireless) communication (high speed data encryption, SSL, WEP, WPA)
- **Kryptographie und Geheimsprachen sind nicht nur etwas für Agenten.**
- **Kryptographie ist eine moderne, mathematisch geprägte Wissenschaft.**



Kryptographie != Sicherheit



- Ziele und Ergebnisse der Vorlesung
- Einführung
- **Grundlagen der Verschlüsselung**
- Elementarverschlüsselungen
- Symmetrische oder Private-Key Verschlüsselungsverfahren
- Asymmetrische oder Public-Key Verschlüsselungsverfahren
- One-Way-Hashfunktionen
- Zusammenfassung

→ Begrifflichkeiten

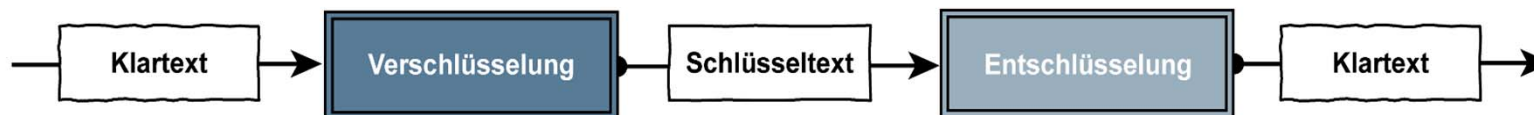
- Ziel der Verschlüsselung ist es, Daten in einer solchen Weise einer **mathematischen Transformation** zu unterwerfen, dass es einem Angreifer nicht möglich ist, die Originaldaten aus den transformierten Daten zu rekonstruieren.
- Damit die verschlüsselten Daten für ihren legalen Benutzer noch verwendbar bleiben, muss es diesem jedoch möglich sein, durch Anwendungen einer inversen Transformation aus ihnen wieder die Originaldaten zu regenerieren.
- Die Originaldaten werden mit „**Klartext**“ (clear text, plain text, message) bezeichnet.
- Die transformierten Daten werden „**Schlüsseltext**“ (Chiffretext, Chiffre, Kryptogramm, cipher text) genannt.
- Die Transformation selbst wird als „**Verschlüsselung**“, ihre Inverse als „**Entschlüsselung**“ bezeichnet.



→ Definition: Kryptographisches System

- **Beschreibbar als 6-Tupel (M; C; KE; KD; E; D):**
 - M = Menge der Klartext-Nachrichten m (messages, plain text)
z.B. $M = \{0, 1\}$, also die Menge der endlichen 0,1-Folgen
 - C = Menge der Kryptogramme c (verschlüsselte Nachrichten, cipher text)
z.B. $C = \{0, 1\}$
 - KE = endliche, nicht-leere Menge der Verschlüsselungs-Schlüssel
z.B. $KE = \{0, 1\}^{256}$ (256 Bit)
 - KD = endliche, nicht-leere Menge der Entschlüsselungs-Schlüssel
mit: $kd = f(ke)$, $kd \in KD$, $ke \in KE$
 - E = Verschlüsselungsverfahren $E: M \times KE \rightarrow C$ (umkehrbar)
 - D = Entschlüsselungsverfahren $D: C \times KD \rightarrow M$ mit
für $m \in M$: $D(E(m, ke), kd) = m$ mit $ke \in KE$, $kd \in KD$ und $f(ke) = kd$

- Das generelle Ziel der Verschlüsselung kann folgendermaßen formuliert werden:
 - Die Entschlüsselung darf nur dem legalen Empfänger/Besitzer der übermittelten/gespeicherten Informationen möglich sein, nicht jedoch anderen Personen - im Extremfall nicht einmal dem Absender, der die Information selbst verschlüsselt hat.
- Dieses Ziel lässt sich offensichtlich genau dann erreichen, wenn nur der legale Empfänger/Besitzer der Information die Entschlüsselung kennt, und wenn es ohne dessen Kenntnis auch nicht möglich ist, diese aus dem Schlüsseltext zu bestimmen.
- Es wäre also auf den ersten Blick ausreichend, wenn Sender und Empfänger eine nur ihnen bekannte Transformation untereinander absprechen und die Kenntnisse darüber geheim halten.





Grundlagen der Verschlüsselung

- Dieser Ansatz ist jedoch aus drei Gründen nicht verwendbar:

1) Der Aufwand zur Definition und Realisierung eines Verschlüsselungs-Algorithmus ist nicht zu vernachlässigen.

Dieses Argument ist um so schwerwiegender, als dass es von Zeit zu Zeit notwendig werden kann, die Verschlüsselung zu wechseln.

In diesem Fall müsste ein neuer Algorithmus eingesetzt werden.



Grundlagen der Verschlüsselung

2.) Es besteht das Risiko, dass es einem Angreifer möglich ist, aus der Struktur der verschlüsselten Daten den Klartext oder die zur Verschlüsselung bzw. Entschlüsselung verwendete Transformation abzuleiten, also die Verschlüsselung zu „brechen“.

Da es sehr aufwendig ist, den Nachweis zu führen, dass ein **bestimmtes Verschlüsselungsverfahren gegen derartige Angriffe durch „Kryptoanalysis“** sicher ist, und da ad hoc bestimmte Algorithmen mit hoher Wahrscheinlichkeit unsicher sind, ist der Einsatz eigener Verfahren für jede einzelne Kommunikation praktisch unmöglich.



Grundlagen der Verschlüsselung

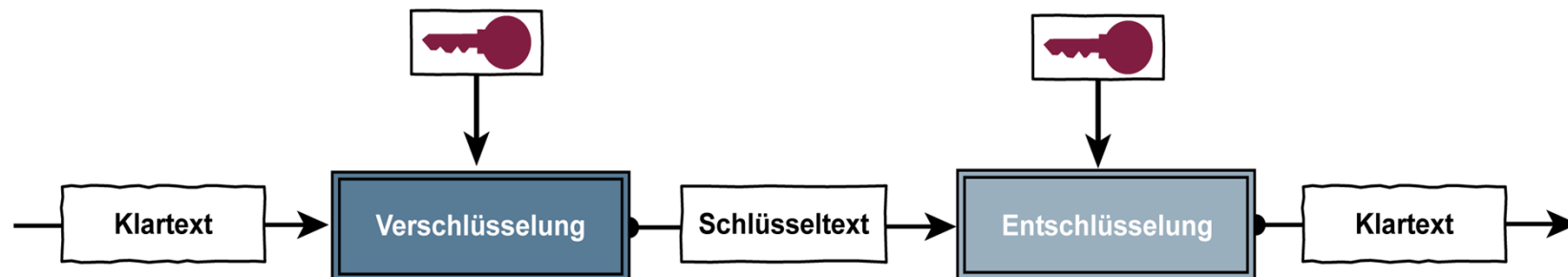
- 3.) Als letztes ist der untragbare Aufwand bei wechselnden Kommunikationspartnern zu nennen, **da für jeweils zwei Partner ein separater Verschlüsselungs-Algorithmus** zur Verfügung stehen muss.



Grundlagen der Verschlüsselung

→ Überblick (3/3)

- Als Lösung dieser Probleme bietet es sich an, zur Verschlüsselung einige wenige Algorithmen einzusetzen, deren Sicherheit erwiesen ist.
- Um die Forderung nach einer Vielzahl von Verschlüsselungsverfahren erfüllen zu können, kann man diese Algorithmen zusätzlich von einem Parameter abhängig machen, dem sogenannten „**Schlüssel**“, der den Ablauf der Transformation so stark beeinflusst, dass ohne seine Kenntnis keine Entschlüsselung möglich ist.



- Wird der Schlüssel geheim gehalten, so kann der **Verschlüsselungs-Algorithmus selbst durchaus öffentlich bekannt sein**; er soll es sogar, da er nur so einer öffentlichen Diskussion preisgegeben wird.



Grundlagen der Verschlüsselung

→ Kerckhoff-Prinzip (formuliert 1883)

- in „Philosophie der modernen Kryptoanalyse“
- niederländischer Philologe Auguste Kerckhoffs von Nieuwenhof
- Die Sicherheit **des Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen!**
- Sie darf sich nur auf die **Geheimhaltung des Schlüssels** gründen!
- „**No security through obscurity**“
 - siehe GSM (Handy) Beispiel (A5/1-Algorithmus)!

Grundlagen der Verschlüsselung

→ Definition einiger Begriffe

- **Kryptographie**
ist die Wissenschaft von den Methoden der Ver- und Entschlüsselung
- **Kryptoanalysis**
ist die Wissenschaft von den Methoden der unbefugten Entschlüsselung von Daten zum Zweck der Rückführung der ursprünglichen Information.
- **Kryptosystem**
dient zur Geheimhaltung von übertragenen oder gespeicherten Informationen gegenüber Dritten.
- **Kryptoanalyse**
ist die Analyse eines Kryptosystems zum Zwecke der Bewertung seiner kryptographischen Stärke.
- **Kryptologie**
ist die Wissenschaft der Verheimlichung von Informationen durch Transformation der Daten. Sie umfaßt Kryptographie und Kryptoanalysis.
- **Steganographie**
ist eine Methode zum Verbergen der Existenz einer Information (auch digitale Wasserzeichen, Copyright-Schutz)



Grundlagen der Verschlüsselung

→ Strategien der Kryptoanalyse (1)

- **Vollständige Suche**

- Diese Methode besteht im Wesentlichen im Ausprobieren aller möglichen Schlüssel.
- Bei einem Know-Plaintext-Angriff verschlüsselt man den bekannten Klartext mit allen möglichen Schlüsseln und vergleicht den entstehenden Schlüsseltext mit dem bekannten Schlüsseltext.
- Speicherung in Rainbow-Tables



Grundlagen der Verschlüsselung

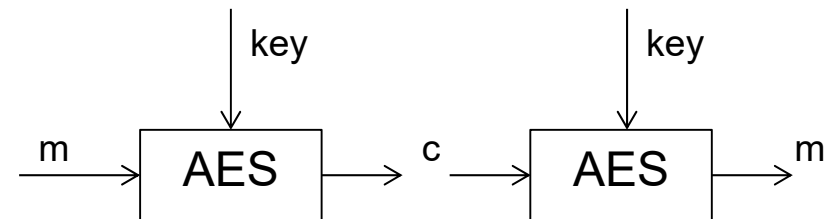
m = Entschlüsselungsfunktion (c , KEY)

→ **Vollständige Suche**

Aufwand für den „guten“ Teilnehmer

Schlüssellänge in Bits	Aufwand in s
128	6,12E-7

m = Brute-Force-Funktion (c) $\rightarrow O(2^n)$



Aufwand für den Angreifer

(Durchprobieren aller möglichen Schlüssel)

Key Länge in Bits	Anzahl der möglichen Schlüssel	Aufwand, den richtigen Schlüssel zu finden in Jahren (Annahme 1.000.000.000 Versuche in der Sekunde)
8	256	0,00000
40	1.099.511.627.776	0,00002
56	72.057.594.037.927.900	1,14
64	1.84E+19	292,47
128	3.40E+38	5.391.448.762.278.160.000.000
192	6,27E+57	9,95E+40
256	1.16E+77	1.83E+60

} bedeutet
praktische
Sicherheit

Grundlagen der Verschlüsselung

→ Begriffe aus der Kryptoanalyse (3)

- Angriffe gegen Kryptosysteme können folgendermaßen unterschieden werden:
- **Ciphertext-only attack**
 - Der Kryptoanalytiker kennt außer dem verwendeten Kryptoverfahren nur den Schlüsseltext.
- **Know-plaintext attack**
 - Hier stehen dem Kryptoanalytiker Klartext/Schlüsseltext Paare zur Verfügung.
 - Diese Paare können z.B. dadurch erlangt werden, dass man bestimmte Zeichenfolgen kennt, die im Klartext vorkommen (z.B. HTTP-Header).



Grundlagen der Verschlüsselung

→ Begriffe aus der Kryptoanalyse (4)

- **Chosen-plaintext attack**

- Der Kryptoanalytiker hat Zugang zum Verschlüsselungsgerät, nicht aber zum Schlüssel. Er kann aber beliebige Klartexte verschlüsseln.
- Durch gezielte Wahl des Klartextes lässt sich unter Umständen der Schlüssel mit wesentlich niedrigerem Aufwand als bei den beiden anderen Verfahren bestimmen, so dass der Angreifer mit ausgewähltem Klartext die höchsten Anforderungen an die Sicherheit des Verschlüsselungsverfahrens stellt!

Grundlagen der Verschlüsselung

→ Strategien der Analyse (5)

- **Trial and Error Methode**

- Bei dieser Methode wird die vollständige Suche dadurch reduziert, dass man nicht mehr den gesamten Schlüsselraum zu untersuchen braucht, sondern nur noch Teilräume, in denen der gesuchte Schlüssel vermutet wird.
- Dieses mag z.B. der Fall sein, wenn es viel äquivalente Schlüssel gibt.
- Schlüssel mit ähnlichen Abschnitten:
 - z.B. Vornamen; Spitznamen, ...
 - Darstellbare ASCII-Zeichen
 - meistens 0...9 (10), A..Z (26) und a...z (26)
 - 62 verschiedene ASCII-Zeichen
 - pro Byte ca. 5-Bit → z.B. von 264 auf 240

**Eine qualitative
Schlüsselgenerierung
ist sehr wichtig !**



Grundlagen der Verschlüsselung

→ Strategien der Analyse (6)

- **Statistische Methoden**

- Hierbei versucht der Kryptoanalytiker die statistischen Strukturen des Klartexts, das sind z.B. Buchstaben oder Worthäufigkeiten, im Schlüsseltext wiederzufinden, um dadurch an den Klartext zu gelangen.

→ Häufigkeitsanalysen von Alphabeten

Ein Verschlüsselungsverfahren
muss mind. 5 Jahre öffentlich
diskutiert werden !

- **Strukturanalyse des Kryptosystems (Short-Cut Methode)**

- Ein solches Verfahren kann immer nur auf ein spezielles Kryptosystem zugeschnitten sein.
- Sind z.B. alle Parameter außer dem Schlüssel bekannt, so wird man mit den gegebenen Parametern versuchen, eine Funktion aufzustellen, mit der sich der Klartext berechnen läßt.



Grundlagen der Verschlüsselung

→ Vollständige Suche (7)

- Prinzipiell läßt sich die vollständige Schlüsselsuche (Brute-Force-Methode) gegen jedes Kryptoverfahren einsetzen.
- Sie führt aber nur dann zum Erfolg, wenn genügend Rechnerzeit und Speicherplatz zur Verfügung stehen.
- Daher lässt sich ein Kryptosystem in zwei Sicherheitskategorien einteilen.
- **Absolute Sicherheit**
 - Absolute Sicherheit liegt vor, wenn es theoretisch unmöglich ist, das System zu brechen
 - (geht nur mit Einmal-Schlüssel mit definierten Eigenschaften).



Grundlagen der Verschlüsselung

→ Vollständige Suche (8)

- **Rechnerische, praktische Sicherheit**
 - Bei der rechnerischen oder praktischen Sicherheit ist es zwar theoretisch möglich, das Kryptosystem zu brechen, praktisch wird dazu jedoch so enorm viel Rechnerzeit bzw. Speicherplatz benötigt, dass dieser Weg einem jeden Kryptoanalytiker aussichtslos erscheinen muss.
 - Die meisten Informationen werden sowieso nach einer längeren Zeit wertlos.
 - Die rechnerische, praktische Sicherheit kann durch eine mathematische Analyse der Komplexität festgestellt werden.



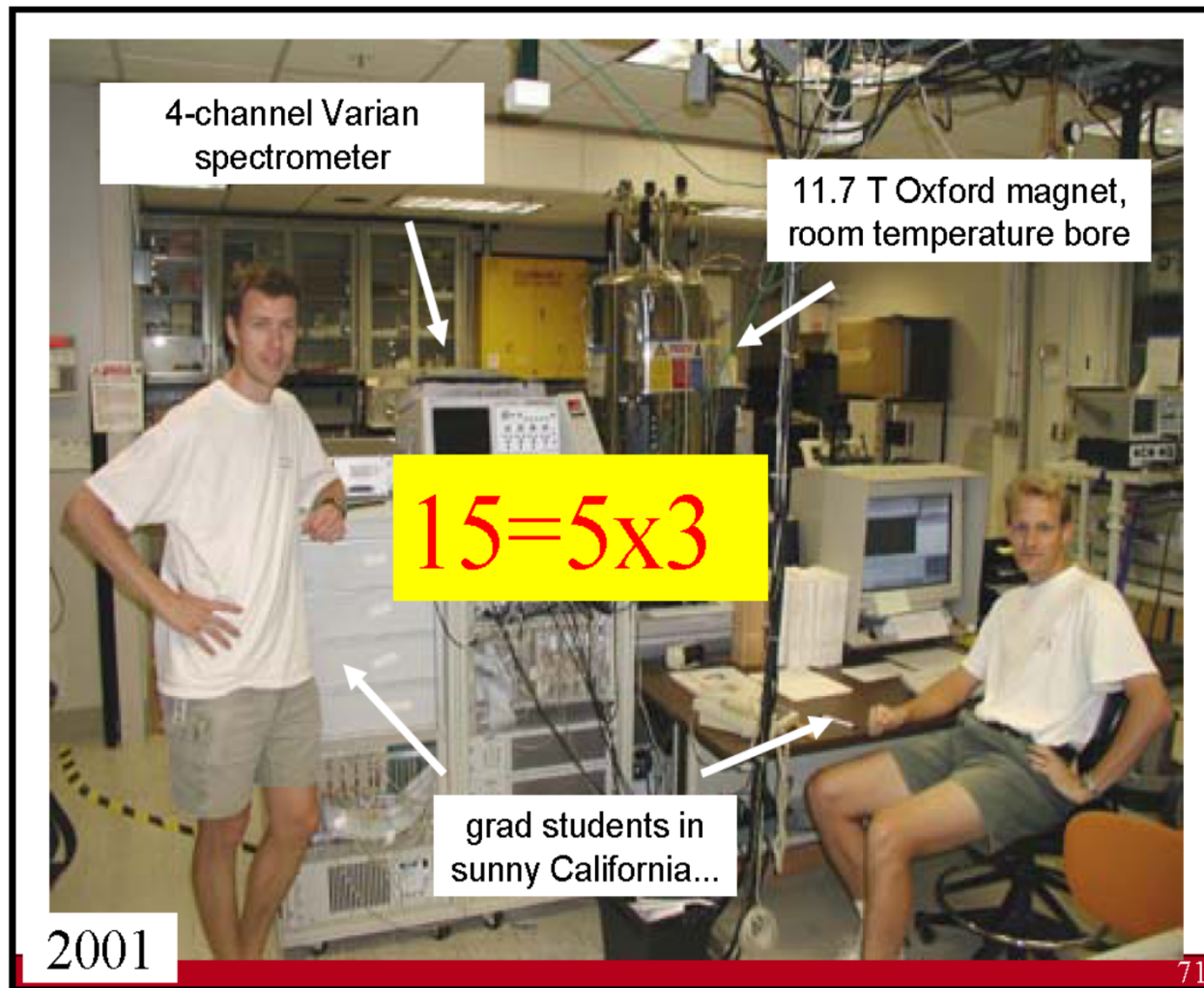
Grundlagen der Verschlüsselung

→ Geschwindigkeit von Computern

- Der Zeitfaktor und die Innovationen (z.B. Quantenrechner) müssen berücksichtigt werden
- **Praktische Sicherheit**
 - vor 20 Jahren: Schlüssellänge von 64 Bit (DES)
 - heute 128 Bit (AES)
 - für die nächsten 20 Jahre 256 Bit (AES)

Alle 10 bis
15 Jahre
ist ein
Wechsel der
Algorithmen
notwendig!





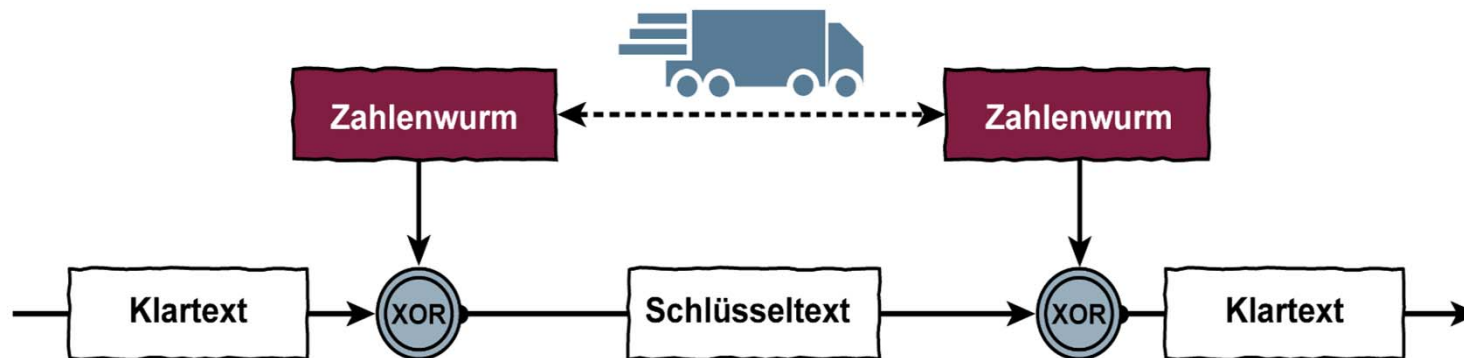
Cryptographic Algorithms and Protocols for Network Security – Bart Preneel 2008



- Ziele und Ergebnisse der Vorlesung
- Einführung
- Grundlagen der Verschlüsselung
- **Elementarverschlüsselungen**
- Symmetrische oder Private-Key Verschlüsselungsverfahren
- Asymmetrische oder Public-Key Verschlüsselungsverfahren
- One-Way-Hashfunktionen
- Zusammenfassung



→ Der Einmal-Schlüssel (1/2)



- Synonyme Einmal-Schlüssel
 - individuelle Wurmverschlüsselung,
 - Zahlenwurm
 - One-Time-Pad genannt.
- Der Einmal-Schlüssel zählt zu den „absolut sicheren“ Verschlüsselungsverfahren.
- Das Verfahren benötigt für jede Nachricht einen Zahlenwurm d.h. einen Schlüssel, der mindestens die Länge des zu übermittelnden Klartextes hat.



Elementarverschlüsselungen

→ Der Einmal-Schlüssel (2/2)

- Der Zahlenwurm/Schlüssel muss für jede Nachricht neu durch Zufallskriterien erzeugt werden und sicher zwischen den Kommunikationspartnern verteilt werden.
- Der Schlüssel und die Nachricht werden bitweise modulo 2 addiert, d.h. XOR verknüpft.
- Da jede Nachricht mit einem gleichlangen Schlüssel verknüpft wird, geht im Schlüsseltext jede Struktur verloren, sodass sich für die Kryptoanalysis keinerlei Ansatzpunkte bieten.
- Wichtig ist die Qualität der Zufallszahlen!
- Obwohl dieses Verfahren für den „heißen Draht“ zwischen Washington und Moskau genutzt wurde (wird?), ist dieses Verfahren für den kommerziellen Einsatz nicht geeignet, da anstelle des absolut geheimen Schlüssels ebenso gut die zu übertragende Nachricht selbst auf dem sicheren Weg übermittelt werden könnte.



- Eine recht einfache Methode, einen Klartext zu verschlüsseln, besteht darin, nach einem bestimmten Schema jedes Zeichen des Klartextes durch ein anderes, dem Klartext fest zugeordnetes Zeichen zu ersetzen d.h. zu substituieren.
- **Verschlüsselungsvorschrift:**
(1) 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
(2) G W X V L O A K U B C N D R M F H Y P Q T Z E I J S
- Beispiel:
 - Schlüssel: Verschlüsselungsvorschrift
 - Klartext: K R Y P T O L O G I E
 - Schlüsseltext: C Y J F Q M N M A U L
- Es können auch verschiedenartige Alphabete verwendet werden
(z.B. lateinische Buchstaben und 26 Buchstaben des chinesischen Alphabetes).



→ Monoalphabetische Substitution: Kryptoanalyse

- Verfahren dieser Art sind durch Häufigkeitsanalysen leicht zu brechen.
- In jeder natürlichen Sprache kommen die Buchstaben nicht gleich häufig vor, vielmehr hat jeder Buchstabe charakteristische Häufigkeiten.

Buchstabe	Häufigkeit (in %)	Buchstabe	Häufigkeit (in %)
A	6,51	N	9,78
B	1,89	O	2,51
C	3,06	P	0,79
D	5,08	Q	0,02
E	17,40	R	7,00
F	1,66	S	7,27
G	3,01	T	6,15
H	4,76	U	4,35
I	7,55	V	0,67
J	0,27	W	1,89
K	1,21	X	0,03
L	3,44	Y	0,04
M	2,53	Z	1,13

Häufigkeit der
Buchstaben der
deutschen Sprache

- Was passiert nun, wenn ein deutscher Klartext mit der monoalphabetischen Substitution verschlüsselt wird?
 - **Die Häufigkeitsverteilung der Buchstaben bleibt erhalten!**



→ Homophone Substitution: Verfahren

- Die homophone Substitution ist eine Verbesserung der monoalphabetischen Substitution.
- Die Verbesserung wird durch einer Verschleierung der Häufigkeit erreicht.
- Bei diesem Verfahren wird die Verschlüsselungsvorschrift so gestaltet, dass alle Schlüsseltextzeichen mit der gleichen Wahrscheinlichkeit auftreten.
- Dazu wird jedem Buchstaben eine Menge von Zeichen zugeordnet, und zwar so, dass die Anzahl der Schlüsseltextzeichen, die zu einem Buchstaben gehören, seiner Häufigkeit entsprechen.
- Bei der Verschlüsselung wird ein Klartextbuchstabe zufällig einem dazugehörigen Schlüsseltextzeichen zugeordnet.
- Da die Zeichen zufällig gewählt werden, kommt jedes Zeichen gleich häufig vor.



→ Homophone Substitution: Verschlüsselungsvorschrift

- Klartext Schlüsseltext

A	(10,21,52,59,71)
B	(20,34)
C	(28,06,80)
D	(19,58,70,81,87)
E	(09,18,29,33,38,40,42,54,55,60,66,75,85,86,92,93,99)
F	(00,41)
G	(08,12,97)
H	(01,07,24)
I	(14,39,50,65,76,88,94)
J	(57)
K	(23)
L	(02,05,82)
M	(27,11,49)
N	(30,35,43,62,67,68,72,77,79)
O	(26,53)
P	(31)
Q	(25)
R	(17,36,51,69,74,78,83)
S	(15,16,45,56,61,73,96)
T	(13,32,90,91,95,98)
U	(03,04,47)
V	(37)
W	(22)
X	(44)
Y	(48)
Z	(64)

- Schlüssel: Verschlüsselungsvorschrift

- Klartext: K R Y P T O L O G I E

- Schlüsseltext: 23 69 48 31 90 26 05 53 08 94 33



→ Homophone Substitution: Kryptoanalyse (1)

- Die Analyse basiert auf der Beobachtung, dass zwar die Häufigkeit der Schlüsseltextzeichen gleich ist, dass aber aus der Betrachtung von Paaren von Schlüsseltextzeichen sehr wohl Informationen gewonnen werden kann.

Buchstabenpaar	Häufigkeit (in %)
en	3,88
er	3,75
ch	2,75
te	2,26
de	2,00
nd	1,99
ei	1,88
ie	1,79
in	1,67
es	1,52

Häufigkeit der
Buchstabenpaare

→ Homophone Substitution: Kryptoanalyse (2)

- Betrachtet man ein Schlüsseltextäquivalent des Buchstaben C, also etwa 28, so wird man feststellen, dass nur bestimmte Schlüsseltextzeichen als unmittelbare Nachfolger von 28 in Frage kommen.
- Das sind für C gleich 01, 07, 24, 23 also die Schlüsseltextäquivalente der Buchstaben H und K.
- Damit weiß man bereits, welche Zeichen dem Buchstaben H und K entsprechen.

■ 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

Schlüsseltext

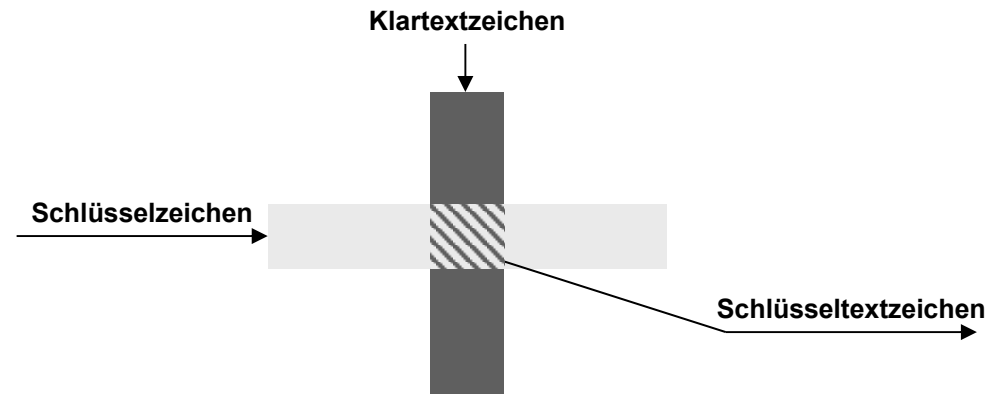
(10,21,52,59,71)
(20,34)
(28,06,80)
(19,58,70,81,87)
(09,18,29,33,38,40,42,54,55,60,66,75,85,86,92,93,99)
(00,41)
(08,12,97)
(01,07,24)
(14,39,50,65,76,88,94)
(57)
(23)
(02,05,82)
(27,11,49)
(30,35,43,62,67,68,72,77,79)
(26,53)
(31)
(25)
(17,36,51,69,74,78,83)
(15,16,45,56,61,73,96)
(13,32,90,91,95,98)
(03,04,47)
(37)
(22)
(44)
(48)
(64)

- Diese Andeutung ist natürlich noch längst keine Kryptoanalyse, sie soll nur zeigen, dass auf den ersten Blick „praktisch unknackbare“ Verfahren doch angreifbar sind.

→ Polyalphabetische Substitution: Verfahren

- Substitutionsverfahren, die die Häufigkeitsanalyse stärker verschleiern, sind z.B. die „polyalphabetischen Substitutionsverfahren“.
- Das bekannteste Verfahren ist die Vigenère-Verschlüsselung

- Diese Verfahren arbeiten mit einem Schlüssel, der aus einer Zeichenfolge besteht, von der jedes Zeichen eine bestimmte Zeile der Tabelle auswählt, und jedes Klartextzeichen wählt eine bestimmte Spalte der Tabelle aus.



- Der Kreuzungspunkt der Zeile und Spalte enthält dann das zugehörige Schlüsseltext-Zeichen.
- Der Schlüssel wird wiederholt, wenn er kürzer als der Klartext ist.
- Die Entschlüsselung erfolgt in der umgekehrten Weise.



→ Polyalphabetische Substitution: Beispiel des Verfahrens

- Verschlüsselungsvorschrift:

	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
1	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
2	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
3	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
4	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
5	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
.																										
.																										
.																										

- Beispiel:

• Klartext: K R Y P T O L O G I E

• Schlüssel: 5 3 2

• Schlüsseltext:

O T Z T V P P Q H M G



Elementarverschlüsselungen

→ Polyalphabetische Substitution: Kryptoanalyse

- Obwohl es aufwendiger statistischer Analyse bedarf, können auch polyalphabetische Verfahren gebrochen werden.
- Ein genügend langer Schlüsseltext weist viele statistisch erfassbare Regelmäßigkeiten auf, die es einem ermöglichen, den Schlüssel zu erhalten.
- Methoden, welche die Länge des benutzten Schlüssels bestimmen.
 - Abstand der beiden Klartextbuchstaben ist ein Vielfaches der Schlüssellänge.
 - Gleicher Klartext = gleicher Schlüsseltext
 - Wenn der Klartext genauso lang wie der Schlüssel ist, arbeitet das Verfahren wie eine monoalphabetische Substitution.



Elementarverschlüsselungen

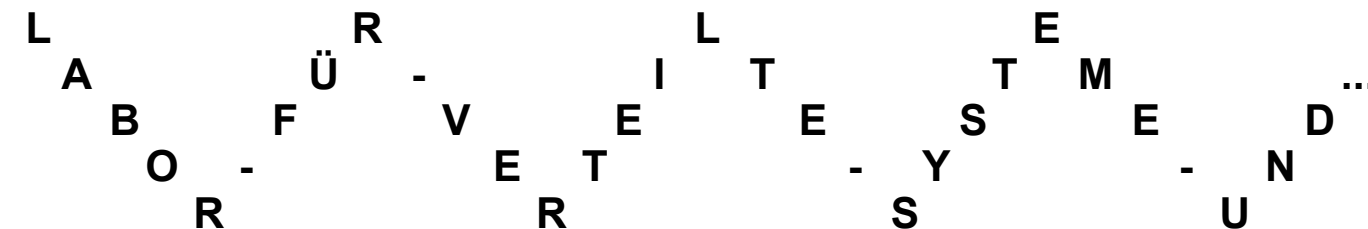
- Monoalphabetische Substitution
- Homophone Substitution
- Polyalphabetische Substitution
- Transpositions-Verfahren

→ Transpositions-Verfahren: Zick-Zack-Verfahren

- Transpositionsverfahren sind Verschlüsselungsverfahren, bei denen die einzelnen Zeichen des Klartextes nach einer bestimmten Regel permutiert d.h. vertauscht werden.

- **Verschlüsselungsvorschrift des Zick-Zack-Verfahrens:**
Der Klartext wird in einer Zick-Zack-Kurve z.B. mit einer Tiefe von fünf (Schlüssel-Wert) aufgeschrieben, und anschließend wird der Schlüsseltext zeilenweise von oben nach unten ausgelesen.

- Schlüssel: Tiefe der Zick-Zack-Kurve (hier 5)
- **Klartext:** **LABOR-FÜR-VERTEILTE-SYSTEME-UND ...**

- 

- Schlüsseltext: **LRLEAÜ-ITTMBFVEESED-ET-Y-NRRSU**

→ Transpositions-Verfahren: Sparta (500 v. Chr.)

- Zwei Zylinder (Holzstäbe) mit genau demselben Radius
 - Sender wickelte ein schmales Band aus Pergament spiralförmig um seinen Zylinder und schrieb dann der Länge nach seine Nachricht auf das Band.
 - Die Nachricht auf dem abgewickelten Band konnte nur von einer Person gelesen werden, die einen Zylinder genau desselben Umfangs hatte.





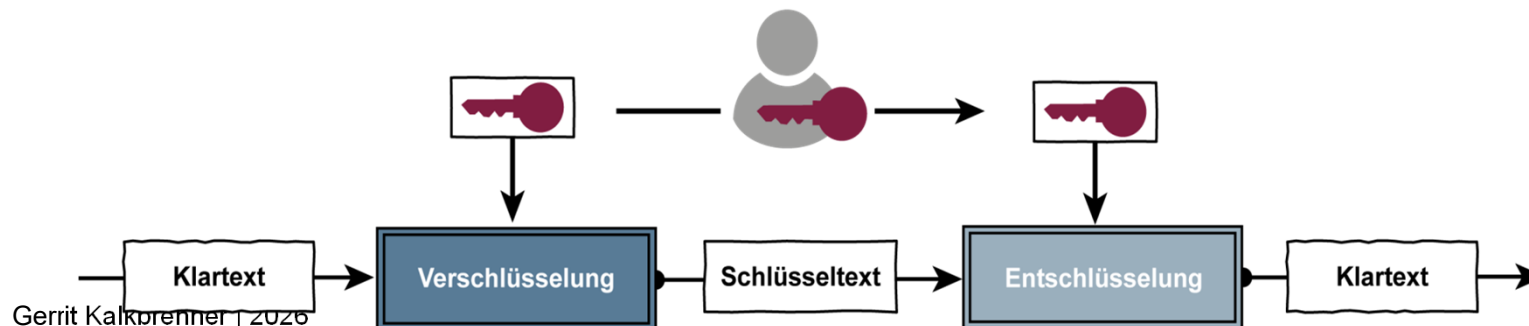
- Ziele und Ergebnisse der Vorlesung
- Einführung
- Grundlagen der Verschlüsselung
- Elementarverschlüsselungen
- **Symmetrische oder Private-Key Verschlüsselungsverfahren**
- Asymmetrische oder Public-Key Verschlüsselungsverfahren
- One-Way-Hashfunktionen
- Zusammenfassung



Symmetrische Verschlüsselungsverfahren

→ Produktverschlüsselung

- Verknüpft man Elementarverschlüsselungen mit verschiedenen kryptographischen Eigenschaften, so spricht man von einer Produktverschlüsselung.
- Ziel der Produktverschlüsselung ist es, kryptographisch stärker d.h. schwerer zu brechen zu sein, als jede ihrer Einzelverschlüsselung.
- Eine der häufigsten Produktverschlüsselungen ist die iterative Verknüpfung von nichtlinearen Substitutionen und Permutationen.



→ Überblick zu den Verfahren

	Schlüssellänge	Als stark betrachtet
• DES	56	
• Triple DES (2-keys)	112	
• Triple DES (3-keys)	168	♦
• IDEA	128	
• RC2, RC4, RC5	variable	
• Blowfish	variable	♦
• CAST	128	
• AES (Rijndael)	variable	♦

Sym-Verschlüsselungsverfahren

→ Data Encryption Standard (DES)

- Weltweiter Standard für 25 Jahren
 - Wurde von IBM entwickelt (undurchsichtiger Vorgang)
 - Lizenz- und rechtefreie Verwendung
- Block Cipher - Blocklänge 64 bit (8 Byte)
- Schlüssellänge 56 Bit - 8 Bit Paritäts Überprüfung (8 Byte)
- Ideal zur Implementierung in Hardware
- Sehr viel Strategie für SW (CPU, RAM, Schlüssel-Vorbereitung, ...)
- Schlüssellänge wird als nicht mehr ausreichend eingestuft
- Eine Abhilfe für ein paar Jahre war die Verwendung des Triple DES



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

**Tele-
kommunikations-
systeme**

AES

Symmetrische Verschlüsselungsverfahren

→ Advanced Encryption Standard (AES)

- Entwickelt von Joan Daemen und Vincent Rijmen
 - Rijndael (Aussprache "Rijndael": "Reign Dahl")
 - Patentfrei
- Block Cipher mit variabler Blocklänge
 - 128, 192 und 256 Bit
- Variabler Schlüssellänge
 - 128, 192 und 256 Bit
- Ersatz für DES
 - FIPS Standard



Symmetrische Verschlüsselungsverfahren

→ AES: Übersicht

- Der AES ist ein Produktverschlüsselungsverfahren, welches aus mehreren Runden besteht.
- Die Länge der zu verschlüsselnden Blöcke und die Länge des Schlüssels kann 128, 192 oder 256 Bit betragen.
- Die Anzahl der Runden hängt von der Blocklänge und der Schlüssellänge ab und beträgt 10, 12 oder 14.

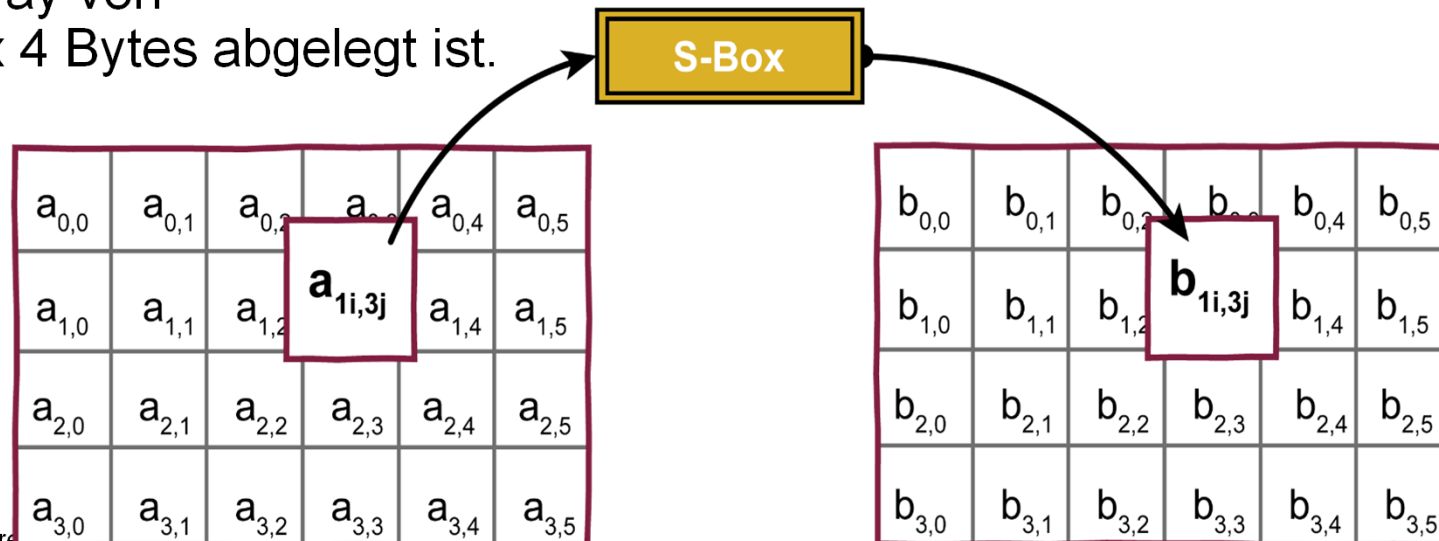
Schlüssellänge (Bit)	Blocklänge (Bit)		
	128	192	256
128	10	12	14
192	12	12	14
256	14	14	14

- Jede der Runden vom AES besteht aus einer Reihe von Byte-orientierten Transformationen, in denen die Stärken vieler anderer Verschlüsselungs-Algorithmen kombiniert wurden.
- Diese eingesetzten Operationen haben sich bei anderen Verschlüsselungsverfahren in der Vergangenheit als widerstandsfähig gegenüber Angriffen erwiesen.

Symmetrische Verschlüsselungsverfahren

→ AES: ByteSub-Transformation

- Die in einem zweidimensionalen Array abgelegten Zeichen des Klartext-Blocks werden zunächst der sogenannten ByteSub-Transformation unterworfen.
- Es handelt sich um eine nichtlineare Substitution der einzelnen Bytes, die über eine Tabelle (S-Box) festgelegt wird.
- Die folgende Abbildung zeigt die Transformation für den Fall einer Blocklänge von 192 Bit, bei denen der Block in einem Array von 6 x 4 Bytes abgelegt ist.






AES S-Box

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

AES S-Box

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6		c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

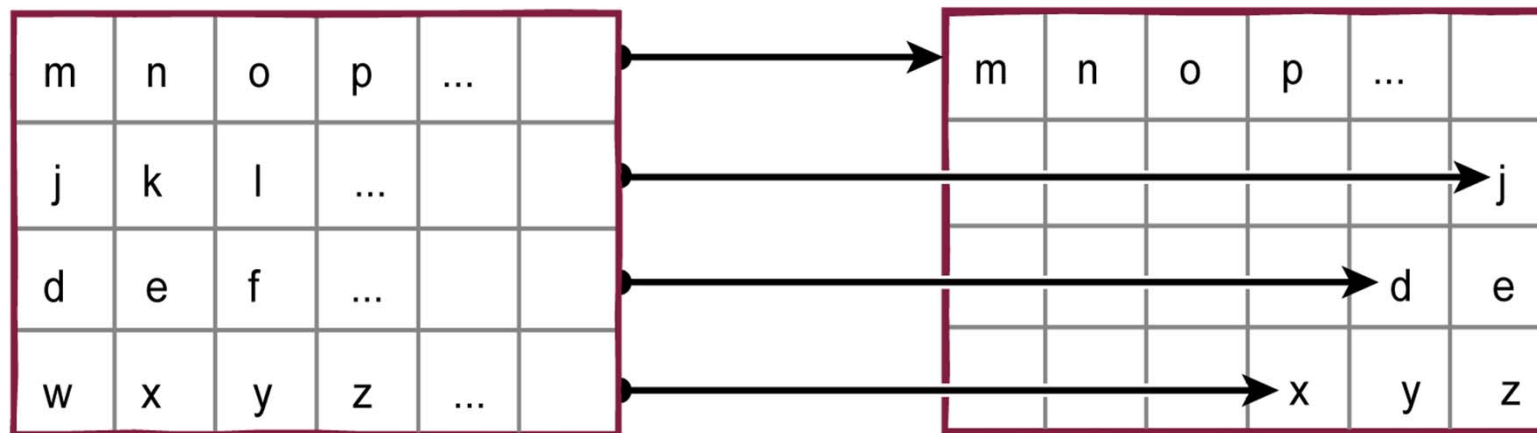
The column is determined by the least significant nibble, and the row by the most significant nibble. For example, the value 9a₁₆ is converted into b8₁₆.



Symmetrische Verschlüsselungsverfahren

→ AES: ShiftRow-Transformation

- Die Bytes werden anschließend der ShiftRow-Transformation unterworfen, bei der die Zeilen des Arrays bis auf die ersten zyklisch geshiftet werden.
- Jede Zeile wird um eine andere Anzahl von Bytes geshiftet.

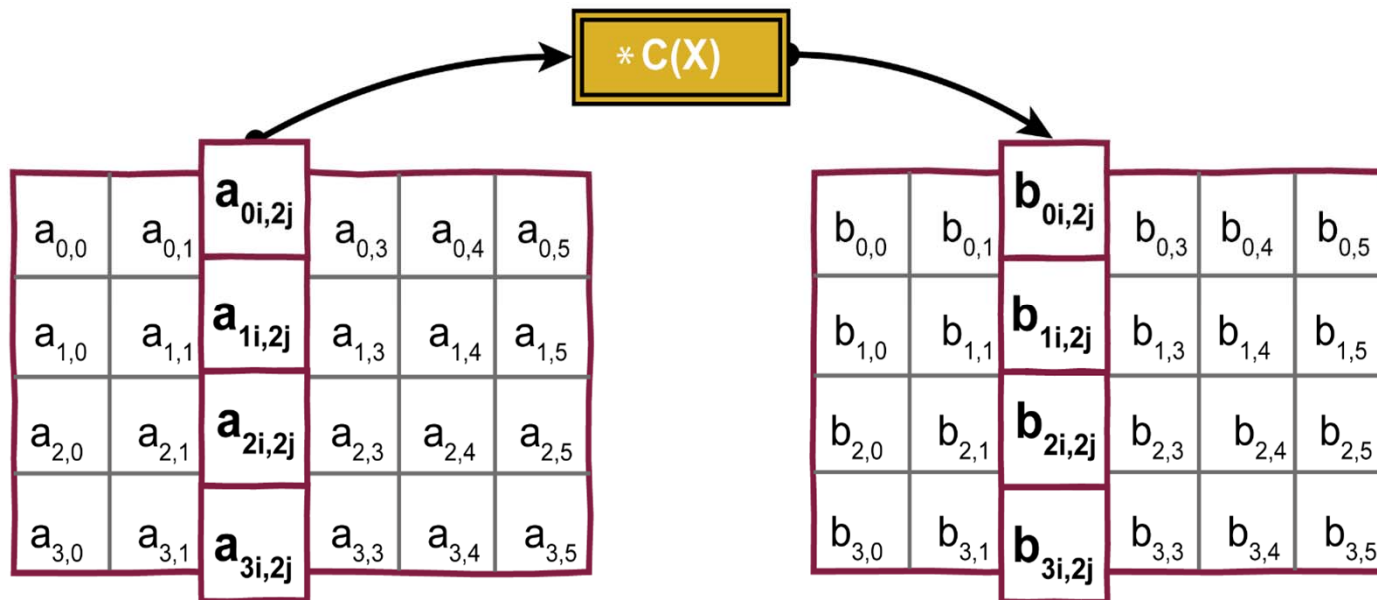




Symmetrische Verschlüsselungsverfahren

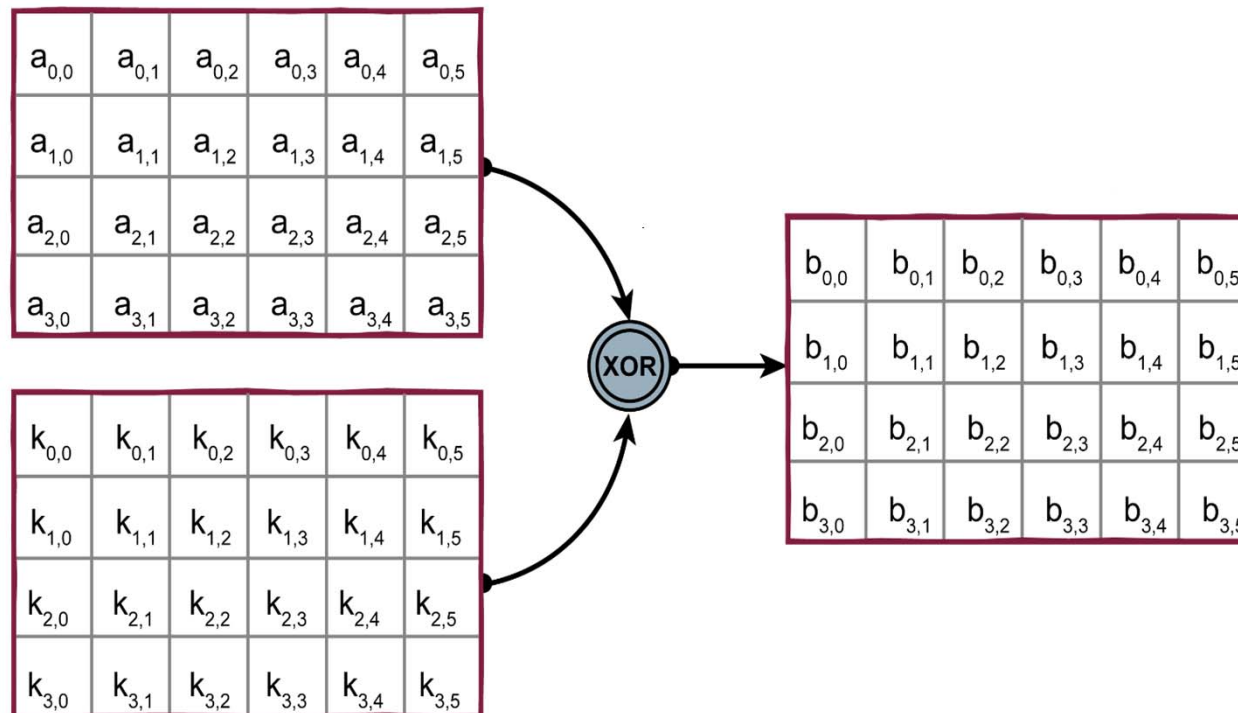
→ AES: MixColumn-Transformation

- Die MixColumn-Transformation unterwirft jeder Spalte des Arrays einer Multiplikation mit einem festen Polynom.



→ AES: AddRoundKey-Transformation

- In der abschließenden AddRoundKey-Transformation wird der aus dem geheimen Schlüssel ermittelte Rundenschlüssel mit dem Array durch ein bitweises XOR verknüpft.



- In der letzten Runde vom AES wird die MixColumn-Transformation überschlagen und direkt in die AddRoundKey-Transformation verzweigt.

Sym-Verschlüsselungsverfahren

→ AES: Rundenschlüssel

- Die in den einzelnen Runden benutzten Rundenschlüssel werden aus dem originalen Schlüssel durch eine Expansions-Funktion berechnet.
- Über XOR, zyklische Shifts und einen Tabellen-Lookup werden vor Beginn der Ver- bzw. Entschlüsselung alle Rundenschlüssel berechnet.
- Dabei wird ein Puffer der Länge (Blocklänge in Bit) * (Anzahl der Runden + 1) gefüllt, aus dem die jeweiligen Rundenschlüssel dann entnommen werden.
- Die ersten N_s Bit (N_s = Schlüssellänge) des Puffers entsprechen dem Schlüssel in unverfälschter Form, alle anderen jeweils N_s Bits entstehen aus dem vorherigen N_s Bits durch eine zyklische Permutation und einer Substitution, die der ByteSub-Transformation ähnelt.
- Vor dem Beginn der ersten Runde wird eine initiale AddRoundKey-Transformation durchgeführt, die den Klartext mit dem ersten Rundenschlüssel verknüpft.
- Die Entschlüsselung erfolgt analog zur Verschlüsselung.



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

**Tele-
kommunikations-
systeme**

Nutzung von AES



Symmetrische Verschlüsselungsverfahren

→ Blockverschlüsselung (1/2)

- Die Algorithmen DES, AES und IDEA gehören zur Familie der Blockverschlüsselungen, bei denen in einem Ver- bzw. Entschlüsselungsvorgang jeweils ein Block von 64/128/192/256 Bits verändert wird.
- Diese Blockverschlüsselungs-Algorithmen können in verschiedenen Betriebsarten oder Modes of Operation ausgeführt werden.
- Die verschiedenen Betriebsarten bieten eine unterschiedliche Sicherheit, die auf der anderen Seite aber auch verschiedenen Aufwand erforderlich macht.



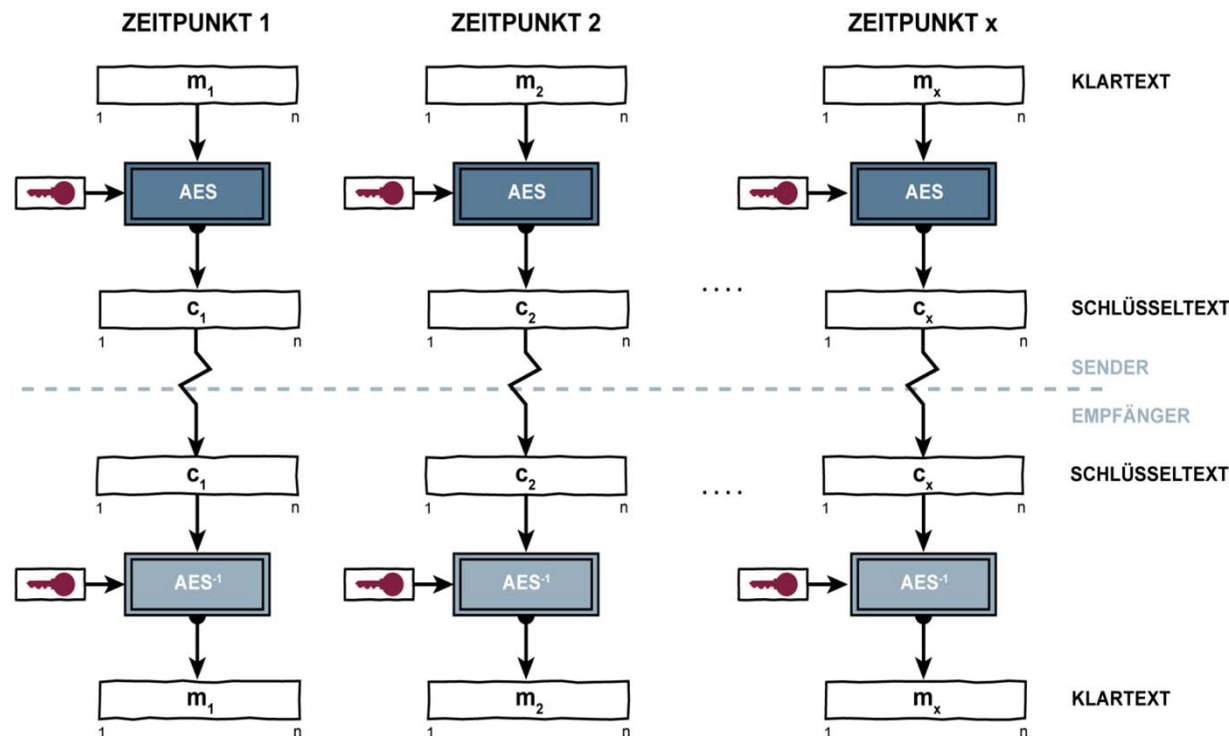
Symmetrische Verschlüsselungsverfahren

→ Blockverschlüsselung (2/2)

- Es gibt die folgenden sechs Betriebsarten:
 - ECB-Mode (Electronic Code Book Mode)
 - CBC-Mode (Cipher Block Chaining Mode)
 - CFB-Mode (Cipher Feedback Mode)
 - OFB-Mode (Output Feedback Mode)
 - CTR-Mode (Counter Mode Mode)
 - GCM-Mode (Galois/Counter Mode)
- Die Betriebsarten werden anhand des AES erläutert.

Sym. Verschlüsselungsverfahren

→ Electronic Code Book Mode (ECB): Verfahren



- Der ECB-Mode stellt die Standardverschlüsselung dar, die jeweils auf einem Block von 256 Bits operiert und diesen unabhängig von anderen Blöcken verschlüsselt.
- Die Nachricht wird in z.B. 256-Bit Blöcke zerlegt, die dann einzeln hintereinander verschlüsselt werden.



Sym. Verschlüsselungsverfahren

→ Electronic Code Book Mode (ECB): Eigenschaften

- Falls innerhalb einer Nachricht ein gleicher 256-Bit Klartext-Block auftritt, ergibt dies auch einen gleichen 256-Bit Schlüsseltext-Block!
- Aufgrund dieser Eigenschaft ist die ECB-Betriebsart nur für spezielle Anwendungen sinnvoll, bei denen Wiederholungen oder häufig auftretende Folgen nicht vorkommen!
- Falls die Blockgrenze zwischen Ver- und Entschlüsselung verloren geht (z.B. durch den Verlust eines Bits), so geht die Synchronisation zwischen Ver- bzw. Entschlüsselung verloren, bis die richtige Blockgrenze wiederhergestellt wird.
- Die Ergebnisse aller Entschlüsselungsoperationen sind dann fehlerhaft.



Sym. Verschlüsselungsverfahren

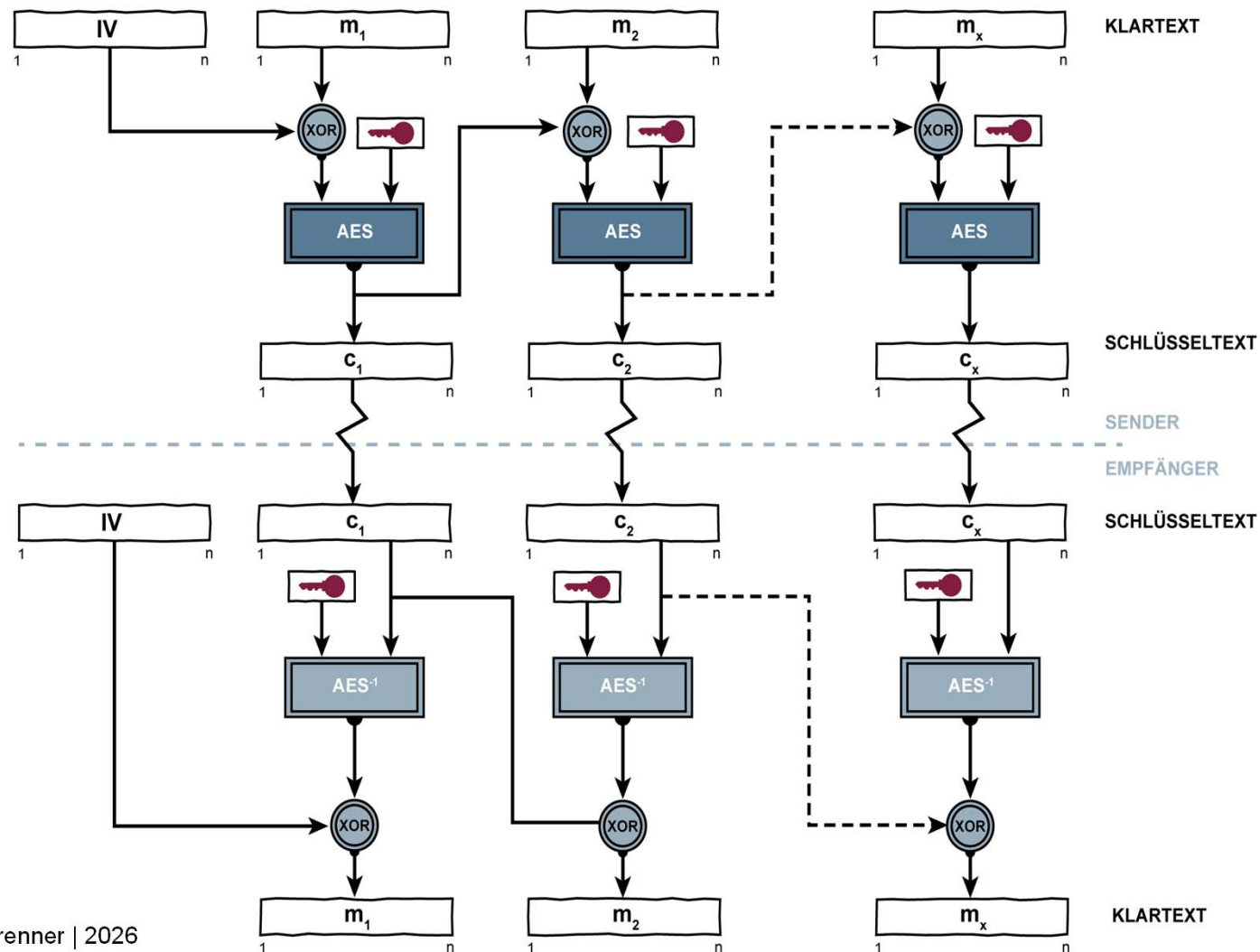
→ Cipher Block Chaining Mode (CBC): Verfahren (1)

- Der Cipher Block Chaining Mode verschlüsselt einen Block, der vor der Verschlüsselung jeweils mit dem verschlüsselten Vorgängerblock verknüpft wird.
- Diese Art der Verschlüsselung heißt Blockverkettung.
- Dies erfordert für den ersten Datenblock einer Nachricht, einen bei Sender und Empfänger verfügbaren Startwert oder Initialisierungsvektor.



Sym. Verschlüsselungsverfahren

→ Cipher Block Chaining Mode (CBC): Verfahren (2)





Sym. Verschlüsselungsverfahren

→ Cipher Block Chaining Mode (CBC): Eigenschaften (1)

- Der CBC-Mode erzeugt denselben Schlüsseltext, wenn derselbe Klartext mit gleichem Schlüssel und Initialisierungswert verschlüsselt wird.
- Mit Hilfe eines variablen Initialisierungsvektors z.B. Zählnummern oder ausgehandelte Zufallszahlen kann dieses verhindert werden.
- Identische Klartext-Blöcke innerhalb einer Nachricht führen zu verschiedenen Schlüsseltext-Blöcken (Blockverkettung).
- Beim CBC-Mode beeinflussen ein oder mehrerer Bitfehler in einem einzigen Schlüsseltext-Block die Entschlüsselung von zwei Blöcken und zwar in dem Block, in dem der Fehler auftritt und in dem folgenden.



Sym. Verschlüsselungsverfahren

→ Cipher Block Chaining Mode (CBC): Eigenschaften (2)

- Wenn die Fehler im i -ten Schlüsseltextblock auftreten, beträgt die durchschnittliche Bitfehlerrate im i -ten Klartextblock 50 %.
- Im $(i+1)$ -ten Klartextblock sind nur die Bit fehlerhaft, die direkt den fehlerhaften Bitpositionen im i -ten Schlüsseltext-Block entsprechen.
- Wie bei ECB-Mode: Falls die Blockgrenze verloren geht, geht auch die Synchronisation verloren, bis die richtige Blockgrenze wiederhergestellt wird. Die Ergebnisse aller Entschlüsselungsoperationen sind dann fehlerhaft.



Sym. Verschlüsselungsverfahren

→ Cipher Feedback Mode (CFB): Verfahren (1)

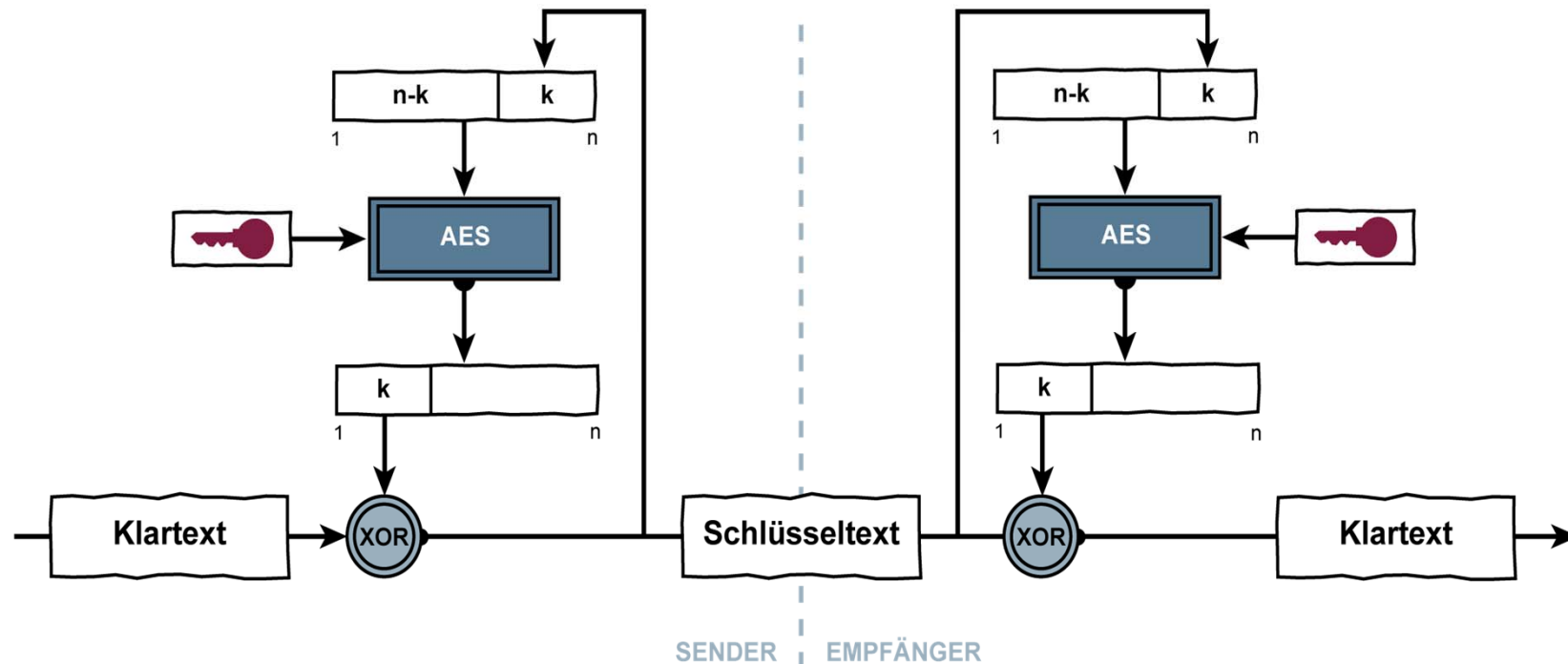
- Eine bevorzugte Methode, eine Folge von Zeichen oder Bits einzeln zu verschlüsseln, ist der Cipher Feedback Mode.
- Durch die Betriebsart wird eine Blockverschlüsselung zu einer kontinuierlichen Verschlüsselung, die auf Klartexteinheiten k-Bit Länge operiert.
- Sowohl sender- als auch empfängerseitig arbeitet die Blockverschlüsselung im Verschlüsselungsmodus und erzeugt eine pseudozufällige Bitfolge, die modulo 2 (XOR) zu dem Klartextzeichen bzw. empfängerseitig zu den Schlüsseltextzeichen addiert wird.
- Zu Beginn einer Verschlüsselung muss der Input der Blockverschlüsselung mit einem Initialisierungsvektor sender- und empfängerseitig geladen werden.



Sym. Verschlüsselungsverfahren

→ Cipher Feedback Mode (CFB): Verfahren (2)

- Für jedes zu verschlüsselnde Zeichen ist eine Blockverschlüsselung erforderlich, so dass diese Betriebsart nicht so effizient ist.





Sym. Verschlüsselungsverfahren

→ Cipher Feedback Mode (CFB): Eigenschaften (1)

- Beim CFB-Mode beeinflussen Fehler in einem k-Bit-Block des Schlüsseltextes die Entschlüsselung des unmittelbaren verstümmelten und des folgenden Schlüsseltextes solange, bis die fehlerbehafteten Bits aus dem CFB-Eingabeblock herausgeschoben sind.
- Der erste betroffene k-Bit-Block des Klartextes ist in genau den Bitpositionen fehlerhaft, in denen der Schlüsseltext fehlerhaft ist.
- Der nachfolgende entschlüsselte Klartext hat eine durchschnittliche Bitfehlerrate von 50% solange, bis alle Fehler aus dem Eingangsblock herausgeschoben sind.
- Sind bis dahin keine zusätzlichen Fehler aufgetreten, so erscheint danach wieder der richtige Klartext.



Sym. Verschlüsselungsverfahren

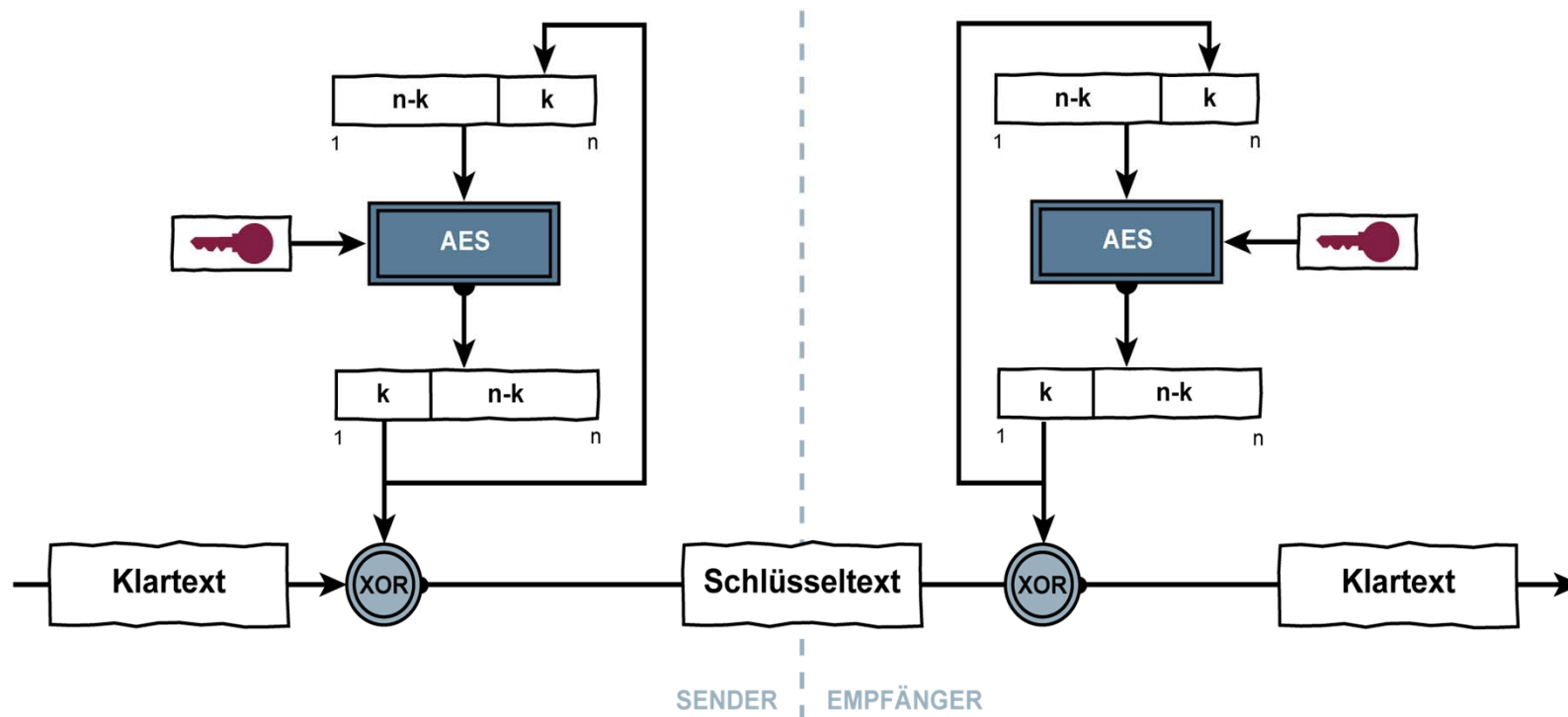
→ Cipher Feedback Mode (CFB): Eigenschaften (2)

- Diese Eigenschaft wird mit „begrenzte Fehlerfortpflanzung“ oder mit „selbst Synchronisation“ bezeichnet.
- Wenn die Grenzen der k-Bit-Blöcke während der Entschlüsselung verloren gehen, so geht auch die kryptographische Synchronisation verloren, bis eine erneute Initialisierung (Reinitialisierung) durchgeführt wird.
- Nach Wiederherstellung der richtigen Grenzen der k-Bit-Blöcke sind höchstens noch die folgenden 64-Bit fehlerhaft.



Sym. Verschlüsselungsverfahren

→ Output Feedback Mode (OFB): Verfahren



- Der Output Feedback Mode arbeitet ähnlich wie der CFB Mode, nur mit dem Unterschied, dass hier nicht das Schlüsseltextzeichen, sondern das Outputzeichen der Blockverschlüsselung in das Inputregister zurückgeführt wird.



Sym. Verschlüsselungsverfahren

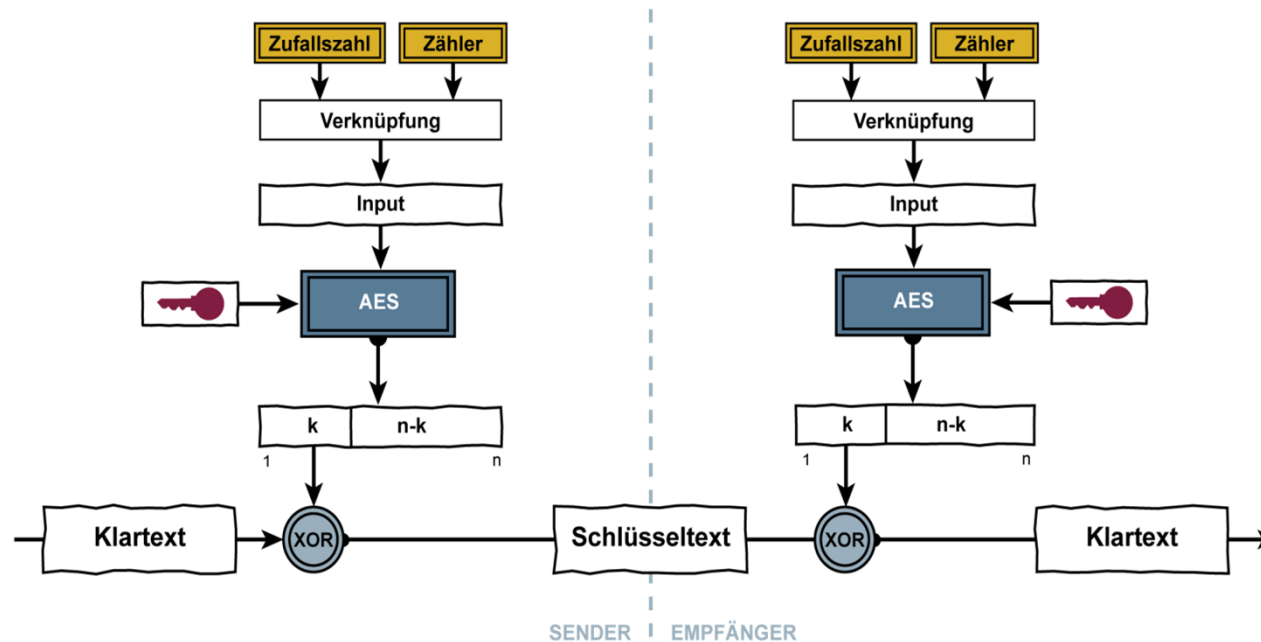
→ Output Feedback Mode (OFB): Eigenschaften

- Der OFB-Mode führt zu keiner Fehlerfortpflanzung in der resultierenden Klartextausgabe.
- Ein fehlerhaftes Bit im Schlüsseltext hat nur ein fehlerhaftes Bit im entschlüsselten Klartext zur Folge.
- Der OFB-Mode ist nicht selbstsynchronisierend.
 - Wenn die beiden Operationen Verschlüsselung und Entschlüsselung aus der Synchronisation geraten, muss das System wieder neu initialisiert werden.
 - Eine Reinitialisierung kann mit einem neuen Startwert bei gleichem Schlüssel durchgeführt werden.
- Dieser Mode ist für störungsanfällige Übertragungswege (z.B. Satellitenverbindung) gedacht, wo eine Fehlerfortpflanzung nicht erwünscht ist.



Sym. Verschlüsselungsverfahren

→ Counter Mode (CTR): Verfahren



- Wie beim CFB und OFM Mode wird eine Blockverschlüsselung zu einer kontinuierlichen Verschlüsselung, die auf Klartexteinheiten k -Bit Länge operiert, umgesetzt
- Der Input für die Verschlüsselung besteht aus der Verknüpfung einer Zufallszahl und einem Zähler



Sym. Verschlüsselungsverfahren

→ Counter Mode (CTR): Eigenschaften

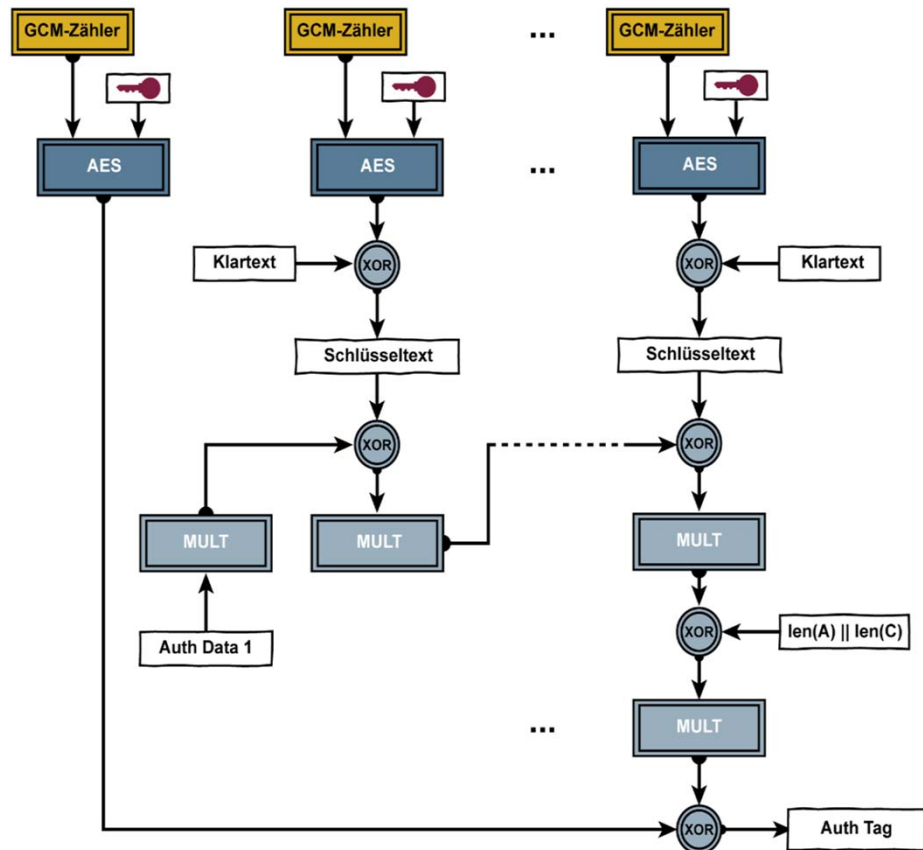
- Ein fehlerhaftes Bit im Schlüsseltext hat nur ein fehlerhaftes Bit im entschlüsselten Klartext zur Folge.
- Wie beim OFB-Mode, wenn die beiden Operationen Verschlüsselung und Entschlüsselung aus der Synchronisation geraten, muss das System wieder neu initialisiert werden.
- Der besondere Vorteil des CTR-Modus ist der wahlfreie Zugriff auf jeden verschlüsselten Block und die Möglichkeit, sämtliche Ver- und Entschlüsselungsoperationen parallel durchzuführen.
- Der CTR-Mode ist besonders geeignet für Massen-Daten, wie Festplatten und ZIP-Archive.



Sym. Verschlüsselungsverfahren

→ Galois/Counter Mode: Verfahren

- Der GCM-Mode gehört zu der Kategorie Authenticated Encryption with Associated Data (AEAD).
- Neben der eigentlichen Verschlüsselung können auch Daten authentisiert werden.
- Beim GCM-Mode wird als Input für die Verschlüsselung ein eindeutiger Zähler verwendet.
- Die Blockgröße ist auf 128 Bit festgelegt.





Sym. Verschlüsselungsverfahren

→ Galois/Counter Mode: Eigenschaften

- Der GCM-Zähler wird in jedem Schritt erhöht.
- „MULT“ bezeichnet die Multiplikation im Galoiskörper $GF(2^{128})$.
- In der NIST Special Publication 800-38D wird die zugehörige Funktion als GHASH bezeichnet.
- $\text{len}(A)$ ist die Bit-Länge der Authentifizierten Daten und $\text{len}(C)$ ist die Bit-Länge der verschlüsselten Daten (in 64-bit Repräsentation).
- Der GCM-Mode hat einen hohen Durchsatz und eignet sich zur parallelen Verarbeitung (z.B. bei Echtzeitverschlüsselung von Kommunikationsdaten und Festplattenverschlüsselung).
- Wird der Schlüsseltext nicht genutzt, reduziert sich der GCM-Mode auf die Authentifizierung der Klartextdaten und wird GMAC (Galois Message Authentication Code) genannt.



Anforderungen

- Gleicher Quelltext, gleicher Schlüssel
→ gleiches Ergebnis
- Probleme mit Bit-Kippen
- Probleme mit dem Verlust von Blockgrenzen
- Selektive Dekodierung von Blöcken

Sym. Verschlüsselungsverfahren

→ Auswahl eines Modes

- Auswahl des Modes of Operations in Abhängigkeit von
 - Performance, die benötigt wird und vorhanden ist (SW/HW)
 - Fehlerfortpflanzung, die gewünscht oder ungewünscht ist
 - Selbstsynchronisation, die evtl. notwendig ist
- Diese Anforderungen können unterschiedlich sein, z.B.:
 - der Kommunikationsebene auf der verschlüsselt werden soll (1 oder 7 OSI)
 - die Qualität des Übertragungskanal
 - ...



Sym. Verschlüsselungsverfahren

→ Festlegung eines Modes

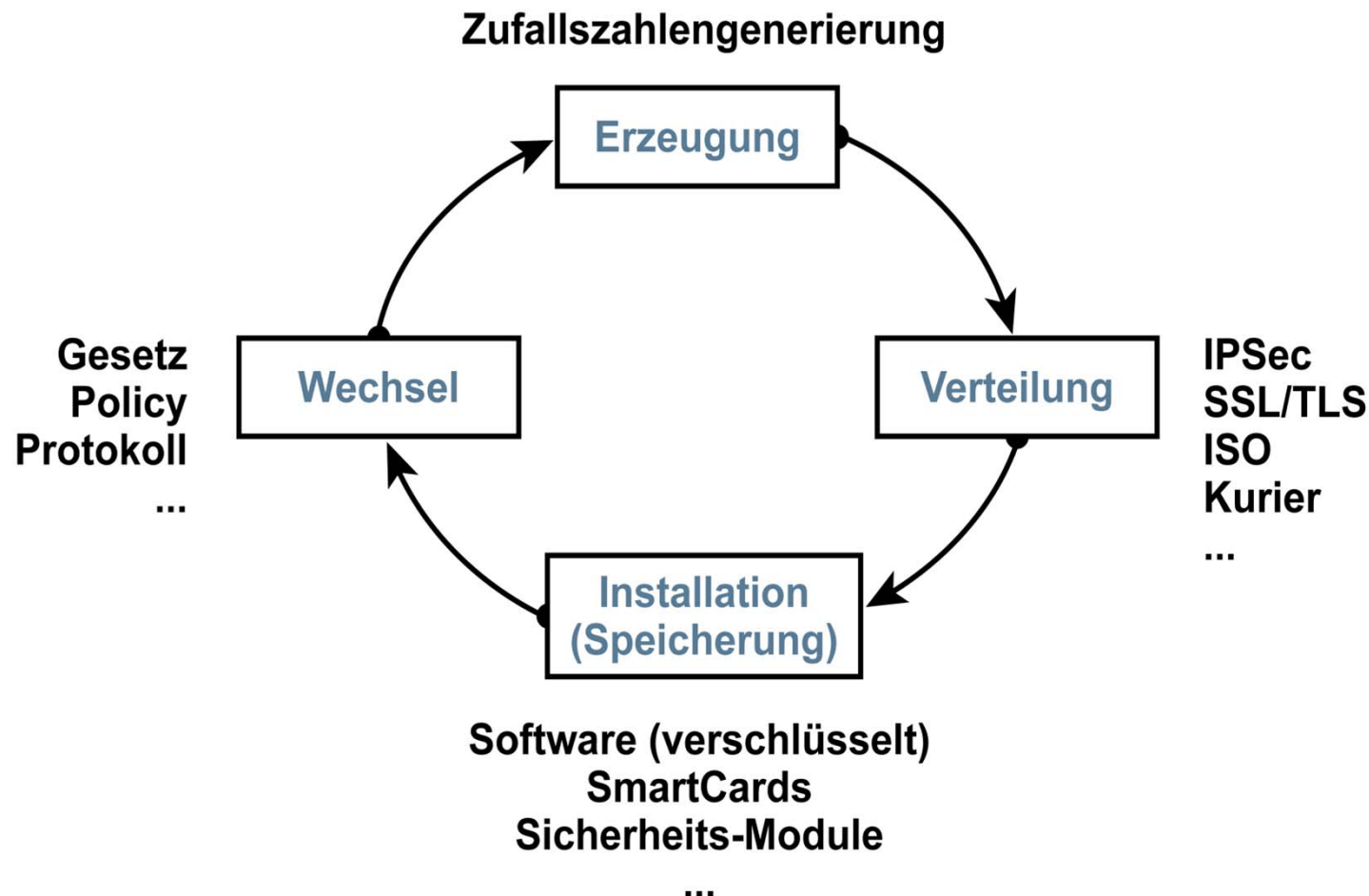
- Die Modes of Operation werden typischerweise in den entsprechenden Standards festgelegt.

Standards	Modes of Operation
WinZip	CTR-Mode
TLS 1.2	CTR-Mode, GCM-Mode
IPSec	GCM-Mode
TLS/SSL	GCM-Mode
IEEE 802.11ad	GCM-Mode
SSH	GCM-Mode



Sym. Verschlüsselungsverfahren

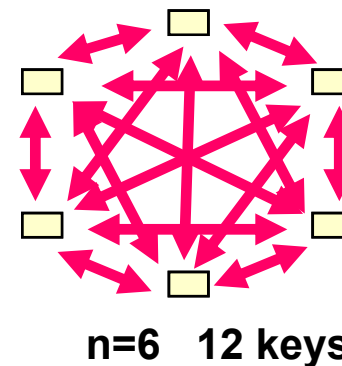
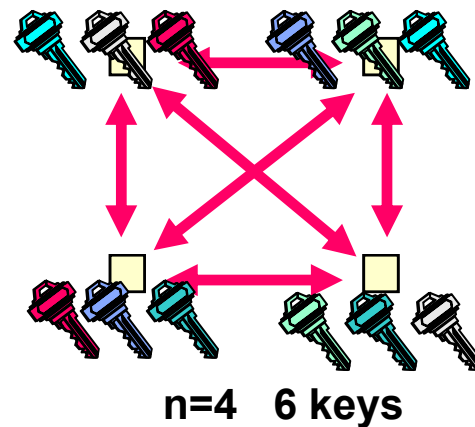
→ Verwaltung von Schlüsseln (1/2)





Sym. Verschlüsselungsverfahren → Verwaltung von Schlüsseln (2/2)

- **Nachteil:**
 - n Partner benötigen: $n*(n-1)/2$ keys
 - n=12: 66 keys
 - n=1000: 499500 keys



Sym. Verschlüsselungsverfahren

→ Abgrenzung zur Steganographie (1)

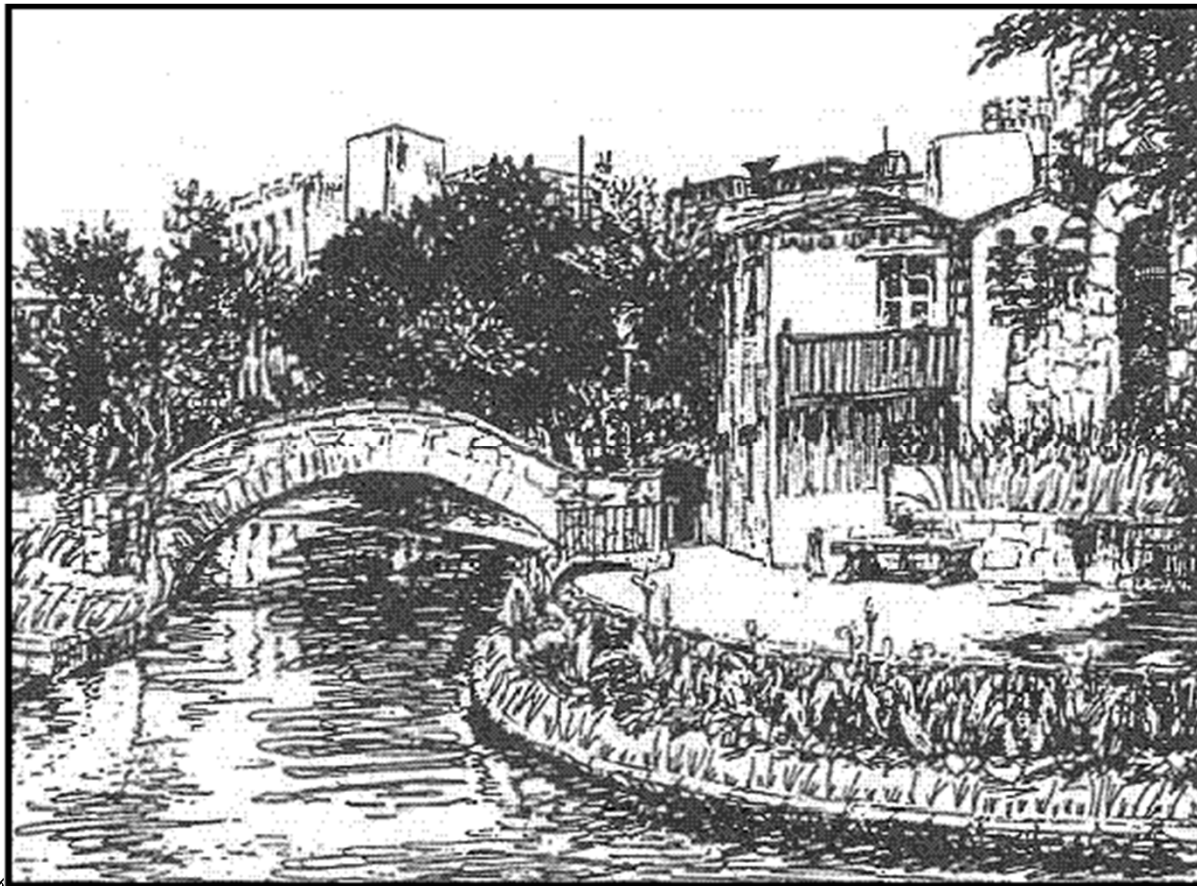
- **Kryptographie:** Nachrichten werden unverständlich gemacht, aber offen übermittelt.
- **Steganographie:** Die Existenz von Nachrichten wird verborgen.
- **Klassische Beispiele:**
 - Unsichtbare Tinte, Mikrofilm, Semagramme: Informationen in Bildern verstecken, verdeckte Kommunikationskanäle, ...
- **Moderne Beispiele:**
 - Verstecken von Bits in Textdateien, Bilddateien, Audiodateien, Videokonferenzen, ...



Sym. Verschlüsselungsverfahren

→ Abgrenzung zur Steganographie (2)

- **Semagramm:** Die Nachricht steht im Morsecode, der aus kurzen und langen Grashalmen von der Brücke entlang des Flusses und auf der kleinen Mauer gebildet wird.



[aus F.L.
Bauer
(Buchtitel
s. Folie 70);
er wiederum
hat es aus
D. Kahn, The

Codebreakers,
S. 523]



→ Stärken des kryptographischen Verfahrens

- Verfahren: anerkanntes, sicheres Verfahren (z.B. AES)
- Schlüssellänge: groß genug (>160, 192, 256)
- richtige Implementierung (Standard)
- Schlüsselgenerierung: Gütekriterien, Streuung, Periodizität, Gleichverteilung
- sichere Schlüsselspeicherung
 - in verschlüsselter Form (siehe Angriffe: ISSE)
 - auf einer SmartCard
 - in einem Security Modul (+ sicheres Verfahren zur Aktivierung)
- sichere Distribution (Key Management)

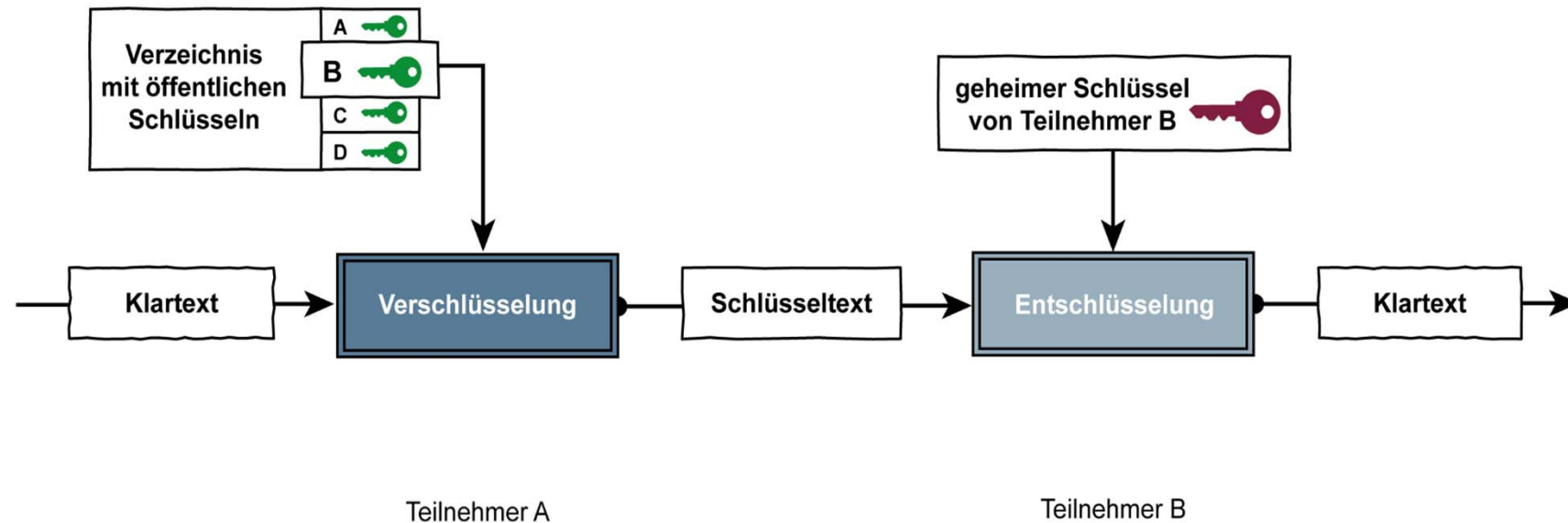


- Ziele und Ergebnisse der Vorlesung
- Einführung
- Grundlagen der Verschlüsselung
- Elementarverschlüsselungen
- Symmetrische oder Private-Key Verschlüsselungsverfahren
- **Asymmetrische oder Public-Key Verschlüsselungsverfahren**
- One-Way-Hashfunktionen
- Zusammenfassung



Asym. Verschlüsselungsverfahren

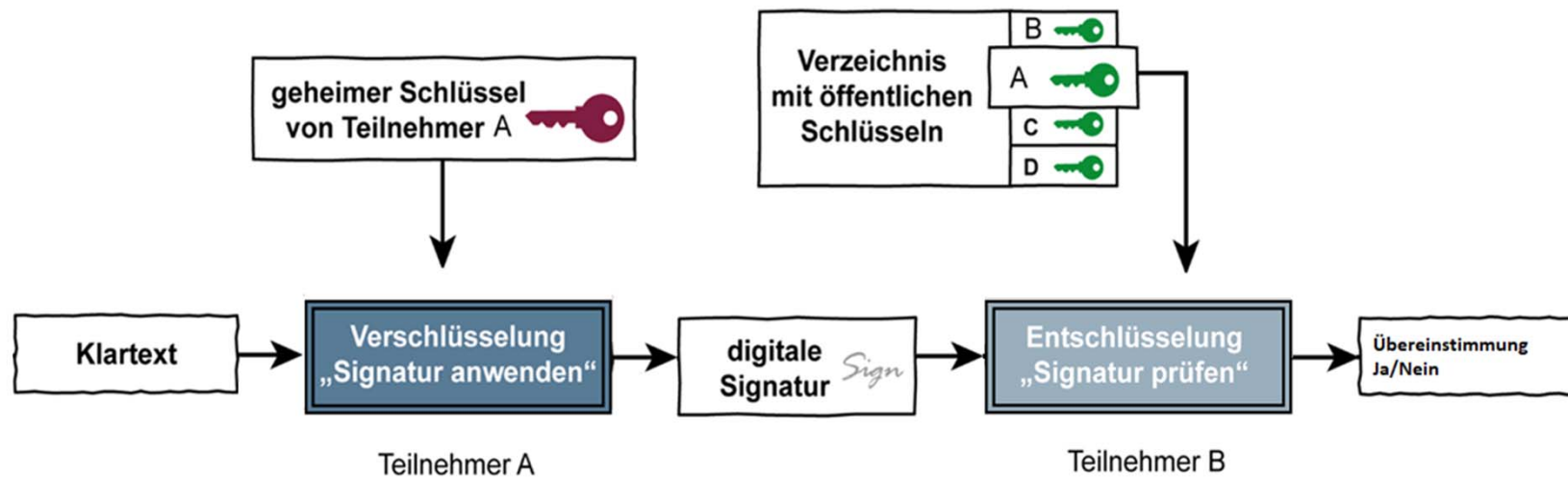
→ Idee



Asym. Verschlüsselungsverfahren

→ Zweite Funktion: Signatur

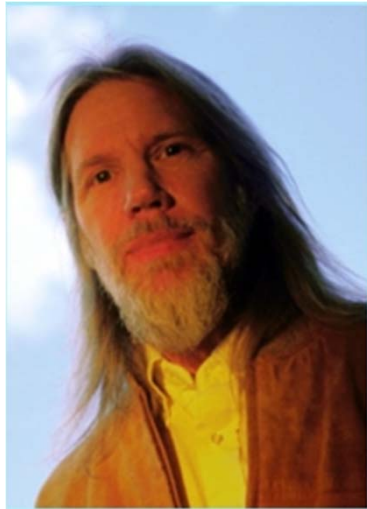
→ Signieren und Signatur Prüfen





DiffieHellman-Verfahren

Whitfield Diffie



Martin Hellman



Famous Paper: New direction in Cryptography, 1976



- Um das klassische Problem der Kryptographie, die Schlüsselverteilung zu erleichtern, wurden Verfahren entwickelt, die mit sogenannten „öffentlichen Schlüsseln“ oder Public-Keys arbeiten.
- Diese Verfahren werden vielfach auch als asymmetrische Verfahren bezeichnet.
- Man geht dabei von Verschlüsselungsverfahren aus, bei denen zur Entschlüsselung ein anderer Schlüssel als zur Verschlüsselung verwendet wird, wobei die folgenden zusätzlichen Forderungen erhoben werden:
 - Der Schlüssel zur Entschlüsselung ist nicht aus dem Schlüssel zur Verschlüsselung ableitbar.
 - Die Verschlüsselung kann nicht durch einen Angriff mit ausgewählten Klartext gebrochen werden.
- Wenn diese beiden Bedingungen erfüllt sind, gibt es keinen Grund mehr, den Schlüssel zur Verschlüsselung geheimzuhalten.



Asym. Verschlüsselungsverfahren

→ Einführung (2/4)

- Man kann sogar den für jeden Teilnehmer gültigen Schlüssel veröffentlichen.
- Daher nennen sich diese Verfahren Public-Key-Verfahren.
- Der Schlüssel zur Verschlüsselung wird als „öffentlicher Schlüssel“ bezeichnet und der Schlüssel zur Entschlüsselung „privater“ oder „geheimer Schlüssel“ genannt.
- Will A eine Nachricht an B senden, so entnimmt er den öffentlichen Schlüssel von B einem öffentlichen Verzeichnis, verschlüsselt die Nachricht damit und sendet sie an B.
- Da nur B den zugehörigen geheimen Schlüssel kennt, und da dieser Schlüssel weder aus dem öffentlichen Schlüssel noch aus der verschlüsselten Nachricht bestimmt werden kann, ist B tatsächlich der Einzige, der die Nachricht wieder entschlüsseln kann.
- Damit ist also eine sichere Kommunikation möglich, ohne dass dazu vorher eine geheime Schlüsselübermittlung zwischen A und B oder von dritter Seite an beide notwendig wäre.



Asym. Verschlüsselungsverfahren

→ Einführung (3/4)

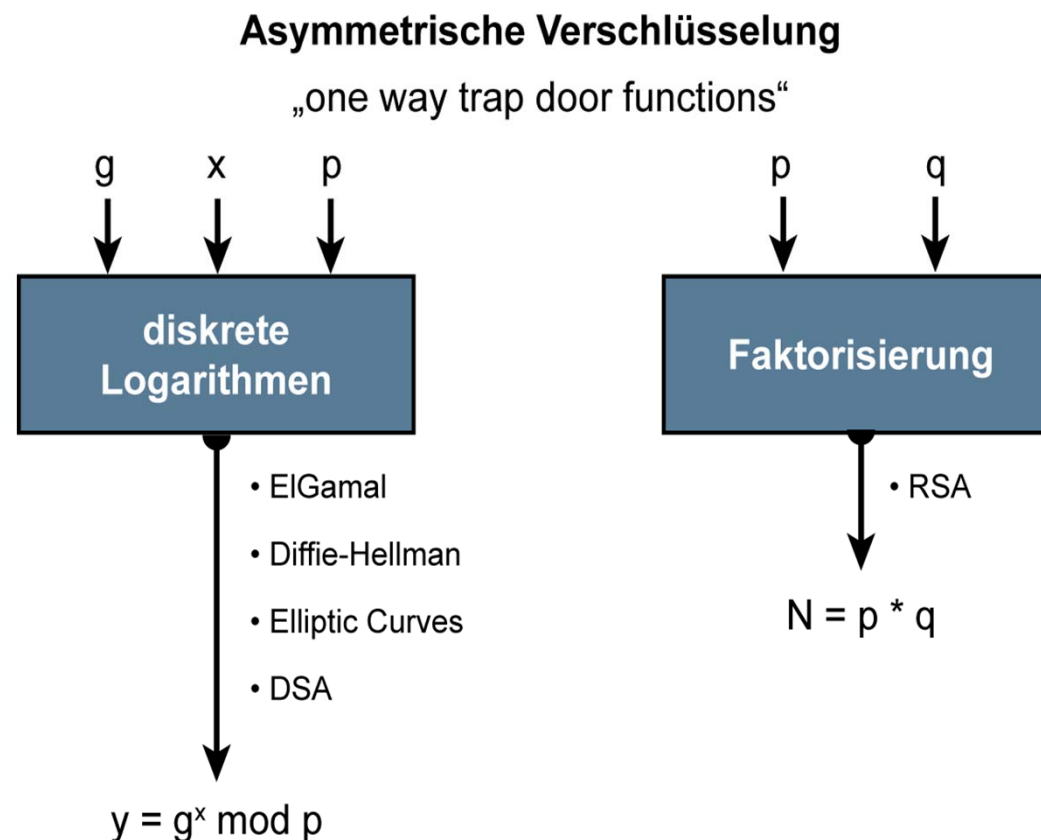
- Da vom Grundsatz her der geheime Schlüssel immer aus dem öffentlichen Schlüssel ableitbar ist, werden für Public-Key-Verfahren Algorithmen gewählt, die auf der Lösung von Problemen der Komplexitätstheorie beruhen.
- Derartige Funktionen werden auch mit „one-way trap door“-Funktionen bezeichnet.
- Bei „one-way“-Funktionen oder Einwegfunktionen handelt es sich um Funktionen, deren Funktionswert „leicht“ zu berechnen ist, während die Berechnung der inversen „schwierig“ oder sogar „unmöglich“ ist.
- Die Begriffe „leicht“, „schwierig“ und „unmöglich“ sollen den rechnerischen Aufwand beschreiben und hängen somit vom Entwicklungsstand der jeweiligen Computergeneration ab.
- Gibt es zu einer „one-way“-Funktion einen Parameter bzw. Schlüssel, mit dem die inverse Transformation „leicht“ zu berechnen ist, so spricht man von einer „one-way trap-door“-Funktion.



Asym. Verschlüsselungsverfahren

→ Einführung (4/4)

- Ausgehend von dieser Überlegung, die Diffie und Hellman im Jahre 1976 veröffentlichten, wurden verschiedene Vorschläge für Public-Key-Verfahren gemacht.





Asym. Verschlüsselungsverfahren

→ Digitale Signatur

- Eine wichtige Anwendung des Public-Key-Verfahrens ist die digitale Signatur
- Daten, die mit einem bestimmten geheimen Schlüssel verschlüsselt wurden, können nur mithilfe des dazugehörigen öffentlichen Schlüssels wieder „entschlüsselt“ werden.
- Hat nun eine Person die Daten mit ihrem geheimen Schlüssel digital signiert, kann mithilfe des öffentlichen Schlüssels überprüft werden, ob es wirklich diese Person war, die die Daten digital signiert hat.
- Die erfolgreich durchgeführte Überprüfung ist der Beweis für die Authentizität der Signatur.
- Mit dem Prinzip der Digitalen Signatur steht somit ein Äquivalent zur handgeschriebenen Unterschrift zur Verfügung.
- Das bekannteste Public-Key-Verfahren ist das RSA-Verfahren, mit dem gleichzeitig signiert und verschlüsselt werden kann.

Asym. Verschlüsselungsverfahren

→ Authentische Schlüssel

- **Problem:**
 - Ein offenes Problem bei Public-Key-Verfahren ist die Frage, wie der öffentliche Schlüssel zum Kommunikationspartner gelangt?
 - Selbst im Fall der Verwendung öffentlicher Schlüssel müssen diese authentisch ausgetauscht werden!
- **Lösung:**
 - Eine elegante Möglichkeit, öffentliche Schlüssel authentisch auszutauschen, ist die Einrichtung eines Zertifizierungs-Systems, eines Trustcenters oder einer Public-Key-Infrastruktur.
 - Der öffentliche Schlüssel jedes Benutzers wird von einer Public-Key-Infrastruktur (Zertifizierungssystem) in Form eines „digitalen Zertifikates“ zur Verfügung gestellt.
 - Siehe digitale Signatur und Public-Key-Infrastruktur!



→ RSA: Fakten

- 1978 entwickelt von Ron Rivest, Adi Shamir und Leonard Adleman
- Nutzbar zur Verschlüsselung, digitaler Signatur und Key Management
- RSA Patent in den USA lief am 20. September 2000 ab.
 - Das Patent war bis dahin ein Problem für die Nutzung (große Firmen)
- Basiert auf dem Problem, dass das Produkt zweier großer Primzahlen nur schwer in seine Faktoren zu zerlegen ist.
 - Welches sind die Faktoren von 377?
 - Mit bekannten Faktoren (29×13) ist die Berechnung des Produkts dagegen einfach: $29 \times 13 = 377$
- Je länger die Faktoren (Primzahlen) desto höher die Sicherheit.



Asym. Verschlüsselungsverfahren

→ RSA: Verschlüsselungsvorschrift

- Message im Klartext: m
- Schlüsseltext: c
- Öffentlicher Schlüssel (ÖS): (e, n)
- Geheimer Schlüssel (GS): d
- Verschlüsselung: $c = m^e \bmod n$
- Entschlüsselung: $m = c^d \bmod n$
- $p * q$ (oder n) ist der Modulus
- e ist der öffentliche Exponent
- d ist der geheime Exponent

$$(X^d)^e = X \pmod{p*q}$$



Asym. Verschlüsselungsverfahren

→ RSA: Beispiel (1/2)

- Erste Primzahl: $p = 61$
- Zweite Primzahl: $q = 53$
- Modulus: $n = p * q = 3233$
- Öffentlicher Exponent: $e = 17$
- Geheimer Exponent: $d = 2753$

- Verschlüsselungsoperation: $c = m^{17} \bmod 3233$
- Entschlüsselungsoperation: $d = c^{2753} \bmod 3233$



Asym. Verschlüsselungsverfahren

→ RSA: Beispiel (2/2)

- **Aufgabe 1**

- Verschlüssele die Zahl: $m = 123$
- Ergebnis 1: $c = 123^{17} \bmod 3233 = 855$

- **Aufgabe 2**

- Entschlüssele die Zahl: $c = 855$
- Ergebnis 2: $d = 855^{2753} \bmod 3233 = 123$

- **Es werden effektive Lösungen zur Berechnung benötigt:**

- Algorithmen in Abhängigkeit von der CPU, Speicherplatz und Zeitanforderung
- Hardware (Sicherheits-Model, SmartCards, TPM, ...)
- Hybride Verschlüsselungsverfahren



Asym. Verschlüsselungsverfahren

→ RSA: Schlüsselgenerierung (1/3)

- Suche zwei große Primzahlen p und q
- Berechne das Produkt $n=p*q$
- Wähle e welches eine relative Primzahl zu $(p-1)(q-1)$ ist und kleiner als $p*q \rightarrow \text{ggT}(e, (p-1)(q-1))=1$ (Teilerfremd)
 - Eine relative Primzahl liegt vor, wenn kein gemeinsamer Teiler vorhanden ist
 - e muss keine Primzahl sein
 - $(p-1)(q-1)$ kann keine Primzahl sein, da es sich um eine gerade Zahl handelt
- Verwende den erweiterten Euklidischen Algorithmus um d zu berechnen
 - $e * d \pmod{(p-1)(q-1)} = 1$



Asym. Verschlüsselungsverfahren

→ RSA: Schlüsselgenerierung (2/3)

- Die Sicherheit des RSA-Verfahrens beruht auf der Schwierigkeit eine große Zahl in ihre Primfaktoren zu zerlegen.
- Es gibt z.B. Faktorisierungsmethoden, die mit Hilfe der Faktoren in $p-1$ und $q-1$ zu viel besseren Ergebnissen kommen.
- Aus diesem Grund sollen die Primzahlen für das RSA-Verfahren noch besondere Eigenschaften aufweisen, die mit starken Primzahlen bezeichnet werden.



Asym. Verschlüsselungsverfahren

→ RSA: Schlüsselgenerierung (3/3)

- **Die Eigenschaften sind für die Primzahlen p und q :**
 - p ist eine große Zahl (z.B. 768 Bit)
 - p ist eine Primzahl (kann sehr unterschiedlich nachgewiesen werden)
 - p wurde zufällig ausgewählt (Zufallszahlengenerator)
 - p hat eine vorher festgelegte Länge (z.B. zwischen 500 und 520 Bit)
 - $p-1$ hat einen großen Primteiler r
 - $p+1$ hat einen großen Primteiler s
 - $r-1$ hat einen großen Primteiler
 - $s-1$ hat einen großen Primteiler.



- 1991 wurde die RSA-Challenge ausgerufen
- Aufforderung an Mathematiker und Informatiker, Primfaktorzerlegungen von konkreten Zahlen variabler Längen zu finden
- Meilensteine:

Stellen	Bits	Preisgeld	Lösung
129	426	100 \$	In 8 Monaten mit 800 Freiwilligen, 1994
174	576	10.000 \$	Uni Bonn, Dezember 2003
193	640	20.000 \$	Uni Bonn, November 2005
212	704
232	768	-	Zusammenarbeit von Instituten unter Leitung von T. Kleinjung“ Dezember 2009
309	1024	100.000 \$	Offen
463	1536	150.000 \$	Offen
617	2048	200.000 \$	Offen

Asym. Verschlüsselungsverfahren

→ RSA: Challenge (2/2)

- Im Mai 2007 hat Uni Bonn eine 312 stellige Zahl (1.039 Bit) faktorisiert.
- Daraufhin hat RSA die Challenge zurückgezogen, da laut dem Unternehmen das Ziel, die Darlegung der Sicherheit des Algorithmus, nun ausreichend geklärt worden sei.
- Mittels neuer Faktorisierungsalgorithmen wie dem Quadratischen Sieb stellen Zahlen mit 1.024 Bit kein Problem mehr für einen großen Rechnerverbund dar.
- Viele RSA-Schlüssel benutzen noch standardmäßig 1024 Bit!





Asym. Verschlüsselungsverfahren

→ Diffie-Hellman: Fakten

- Erster Public Key Algorithmus in 1976
- Kein Verschlüsselungsalgorithmus
 - Gesicherter Austausch eines geheimen Schlüssels
 - keine Authentifizierung der Partner
- Das Schlüsselpaar von A besteht aus dem geheimen Schlüssel **prv_A** und dem öffentlichen Schlüssel **pub_A**

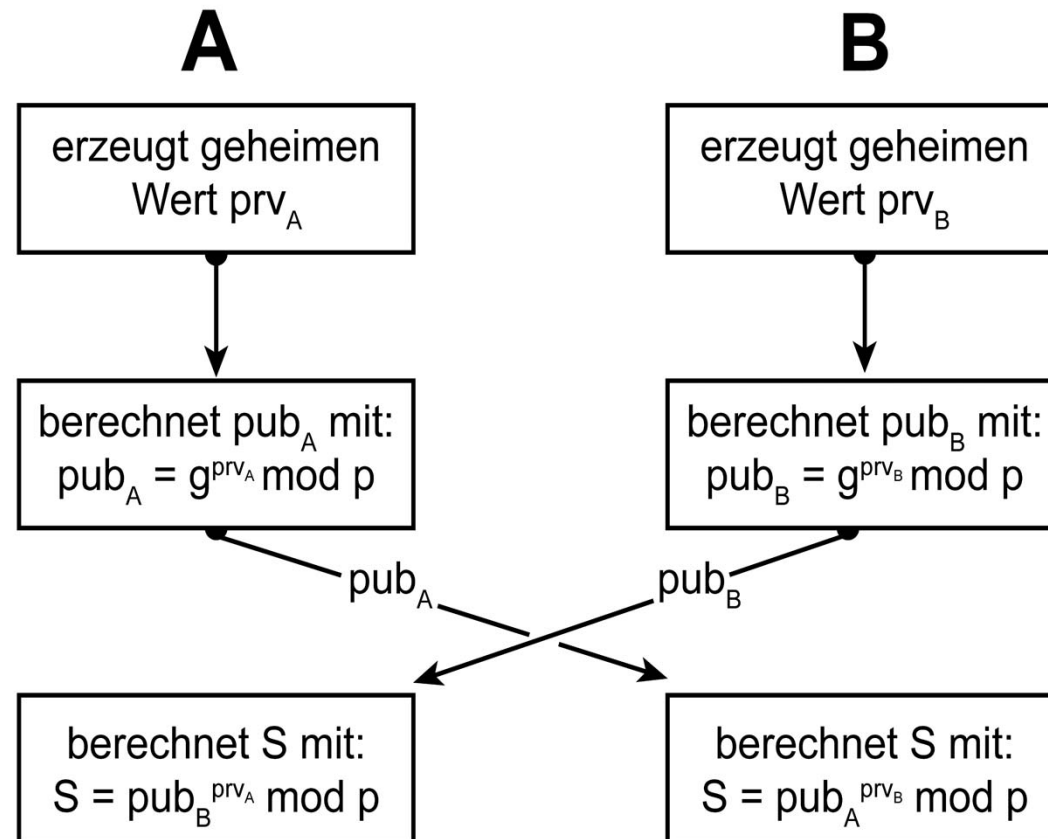
$$\text{pub}_A = g^{\text{prv}_A} \bmod n$$

- **g** und **n** sind öffentlich bekannt. **n** ist eine lange Primzahl und **g** eine zu **n** teilerfremde Zahl.



Asym. Verschlüsselungsverfahren

→ Diffie-Hellman: Verfahren



öffentlich bekannt ist
die Primzahl p und die Zahl g



Asym. Verschlüsselungsverfahren

→ Elliptische Kurven

- Elliptische Kurven basierende Kryptographie (auch bekannt als EC bzw. ECC) wird als Ersatz für RSA, DSA und Diffie-Hellman Schlüsselaustausch angepriesen.
- Vorteile:
 - Kürzere Schlüssel (256 Bit statt 2.024 Bit)
 - Schnellere Verarbeitung
 - Geringere Speicherbedarf
 - Schnellere Kommunikation
 - besonders Interessant für SmartCards (findet Verwendung im nPA)



Asym. Verschlüsselungsverfahren

→ Einsatzgebiet

- Wahrung der Integrität (Signatur)
 Verbindlichkeit
- Absenderüberprüfung (Zertifikat mit Signatur)
- Key-Management (Diffie Hellman und weitere
 Schlüsselaustausch Protokolle)
- Vertraulichkeit (Ver-/Entschlüsselung (z.B. RSA))



Asym. Verschlüsselungsverfahren

→ Quantencomputer

- Die Einführung von leistungsfähigen Quantencomputern hätte zur Folge, dass alle zurzeit gebräuchlichen asymmetrischen Verschlüsselungsverfahren (z.B. RSA) unsicher wären.
- Ein Quantencomputer mit genügend Qubits und dem Shor-Algorithmus kann das Faktorisierungsproblem theoretisch in Polynomialzeit lösen.
- Dies hätte zur Folge, dass sämtliche Geschäftsprozesse im E-Commerce nicht mehr vertraulich wären und somit jegliche Formen von Onlinehandel effektiv nicht mehr möglich wären.
- Die Sicherheit von symmetrischen Verschlüsselungsverfahren (z.B. AES) kann wahrscheinlich durch die Erhöhung der Schlüssellängen realisiert werden.
- Mit dem Grover-Algorithmus kann die Sicherheit von symmetrischen Verschlüsselungsverfahren halbiert werden.



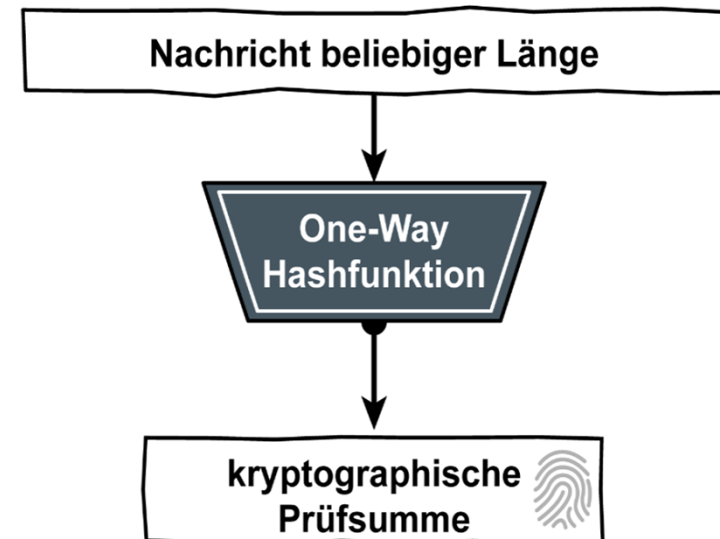
- Ziele und Ergebnisse der Vorlesung
- Einführung
- Grundlagen der Verschlüsselung
- Elementarverschlüsselungen
- Symmetrische oder Private-Key Verschlüsselungsverfahren
- Asymmetrische oder Public-Key Verschlüsselungsverfahren
- **One-Way-Hashfunktionen**
- Zusammenfassung



One-Way-Hashfunktionen

→ Grundlagen

- Die Digitale Signatur entspricht einer Operation mit einem Public-Key-Verfahren und ist daher sehr rechenintensiv.
 - Um den Aufwand zu reduzieren, signiert man nicht die gesamte Datei mit dem Public-Key-Verfahren, sondern erstellt eine Prüfsumme als “Konzentrat” der Nachricht, welche dann digital signiert wird.
- Auf eine Nachricht, deren Länge variabel ist, wird eine sogenannte One-Way-Hashfunktion angewendet, die eine kryptographische Prüfsumme (Hashwert) fester kurzer Länge als Ergebnis erzeugt.
 - Zu den besonderen Eigenschaften von One-Way-Hashfunktion gehört, dass die Berechnung des Funktionswertes einfach ist, während es aber praktisch unmöglich ist, systematisch einen Wert zu finden, der dieselbe kryptographische Prüfsumme ergibt.





One-Way-Hashfunktionen

→ Eigenschaften (1/2)

- H ist eine öffentliche bekannte Einwegfunktion
- $h = H(M)$, h ist ein eindeutiger “Fingerabdruck” von M (Hashwert)
 - Eingabe M kann beliebig lang sein
 - Hashwert h hat eine feste Länge, z.B. 256 Bit
- $H(M)$ ist eine One-Way Funktion (Einwegfunktion)
 - $H(M)$ ist einfach zu berechnen, bei gegebenem M
 - Mit gegebenem h , ist es schwer (praktische unmöglich) M zu berechnen, sodass $M = f(h)$ ist !



One-Way-Hashfunktionen

→ Eigenschaften (2/2)

- $H(M)$ ist kollisionsresistent
 - Mit gegebenem M , ist es schwer (praktisch unmöglich) eine weitere Nachricht M' zu finden, sodass $H(M) = H(M')$!
 - Zwei verschiedene digitale Dokumente (Nachrichten), die denselben Hashwert abbilden werden, bilden eine Kollision!
 - Die Existenz von Kollisionen ist unvermeidbar.
 - Dieses ist aber nur eine theoretische Aussage.
 - Bei praktischen Anwendungen kommt es nur darauf an, dass es, wie oben verlangt, praktisch unmöglich ist, Kollisionen zu finden.



One-Way-Hashfunktionen

→ Arbeitsweise

Das Original:

In Xanadu did Kubla Khan
A stately pleasure-dome decree:
Where Alph, the sacred river, ran
Through caverns measureless to man
Down to a sunless sea

Hashfunktion

Hashwert

a89d e23f ede8

Die veränderte Kopie:

In Xanadu did Napoleon
A stately pleasure-dome decree:
Where Alph, the sacred river, ran
Through caverns measureless to man
Down to a sunless sea

Hashfunktion

Hashwert

38fe 38aa 9c2d

Minimaler Unterschied

Großer Unterschied



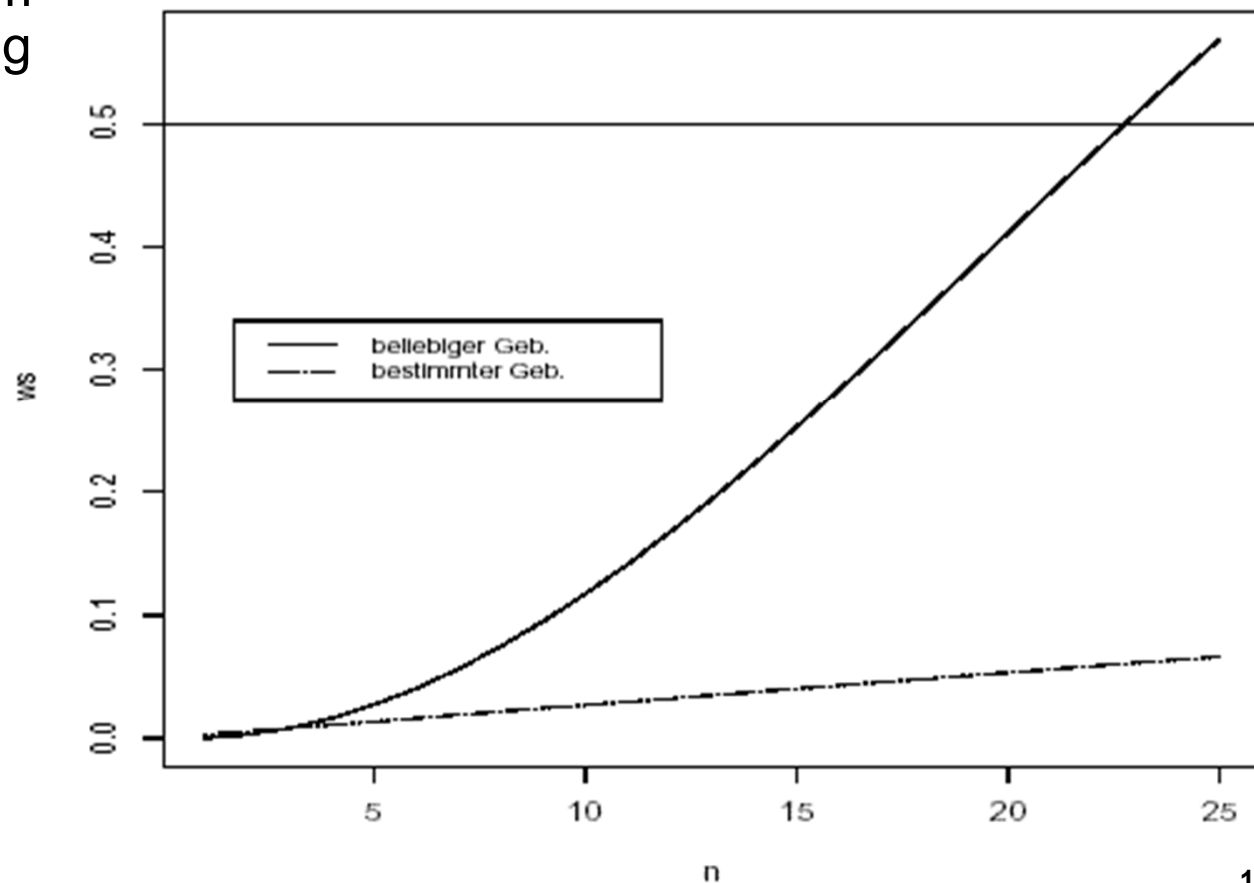
One-Way-Hashfunktionen

→ Das Geburtstags-Paradox (1/2)

Wieviele zufällig
ausgewählte Menschen
braucht man, damit mit
 $p > 0,5$ mindestens 2 am
gleichen Tag Geburtstag
haben?

- Ergebnis: nur 26 Menschen!

Die Entwicklung der Wahrscheinlichkeiten





One-Way-Hashfunktionen

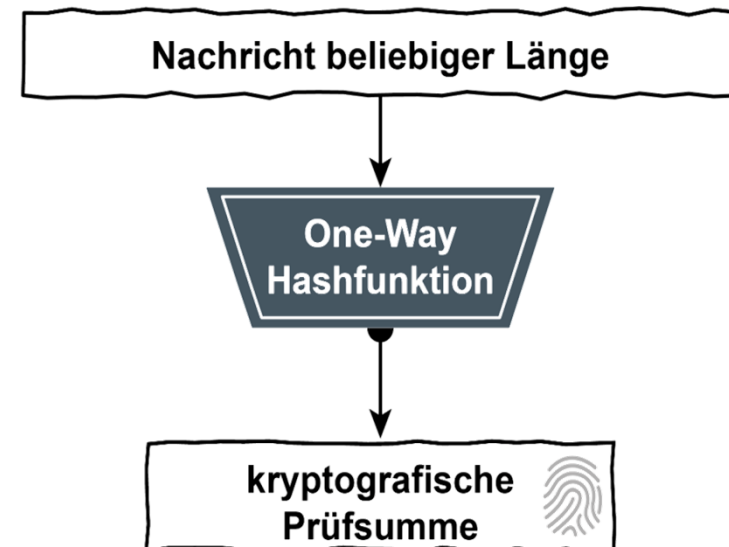
→ Das Geburtstags-Paradox (2/2)

- **Aufgabe:** Ein Angreifer will ein geändertes Dokument erzeugen, das denselben Hashwert liefert, da nur der Hashwert bei einer digitalen Signatur von einem elektronischen Dokument signiert wird.
- **Problem:** Wenn eine Hashfunktion H Nachrichten auf Komprimierte einer Länge von 60 Bit abbildet, dann braucht ein Angreifer rein statistisch „nur“ 230 verschiedene Eingabenachrichten, um eine Kollision zu finden (in Texten z.B. lange Artikelnummern).
- **Anforderung an Hashfunktionen**
 - Hashfunktionen H sollten einen längeren Hashwert h haben als Schlüssellängen bei symmetrischen Verschlüsselungsverfahren, z.T. mindestens 160 Bit!

One-Way-Hashfunktionen

→ Übersicht

- Hashfunktionen
 - Sind praktisch unumkehrbare Komprimierungsfunktionen
- Typische Vertreter:
 - MD5, SHA, ...
 - RIPEMD = RIPE Message Digest 1992 innerhalb des EU-Projekts RIPE entwickelt;
 - SHA-3 neuer NIST-Standard



One-Way-Hashfunktionen

→ MD5

- Message Digest #5, von Ron Rivest
- Eingabe in 512 Bit Blöcken (kürzere Nachrichten werden aufgefüllt)
-
- Hashwert: 128 Bit (zu klein für die meisten Anwendungen!)
- 4 Runden
- Theoretische Angriffe waren erfolgreich
 - Dies hat keine Auswirkungen auf praktische Anwendungen
- Dieses Verfahren soll nicht mehr eingesetzt werden!
(ist aber noch in vielen Standards vorhanden, z.B. IPSec)



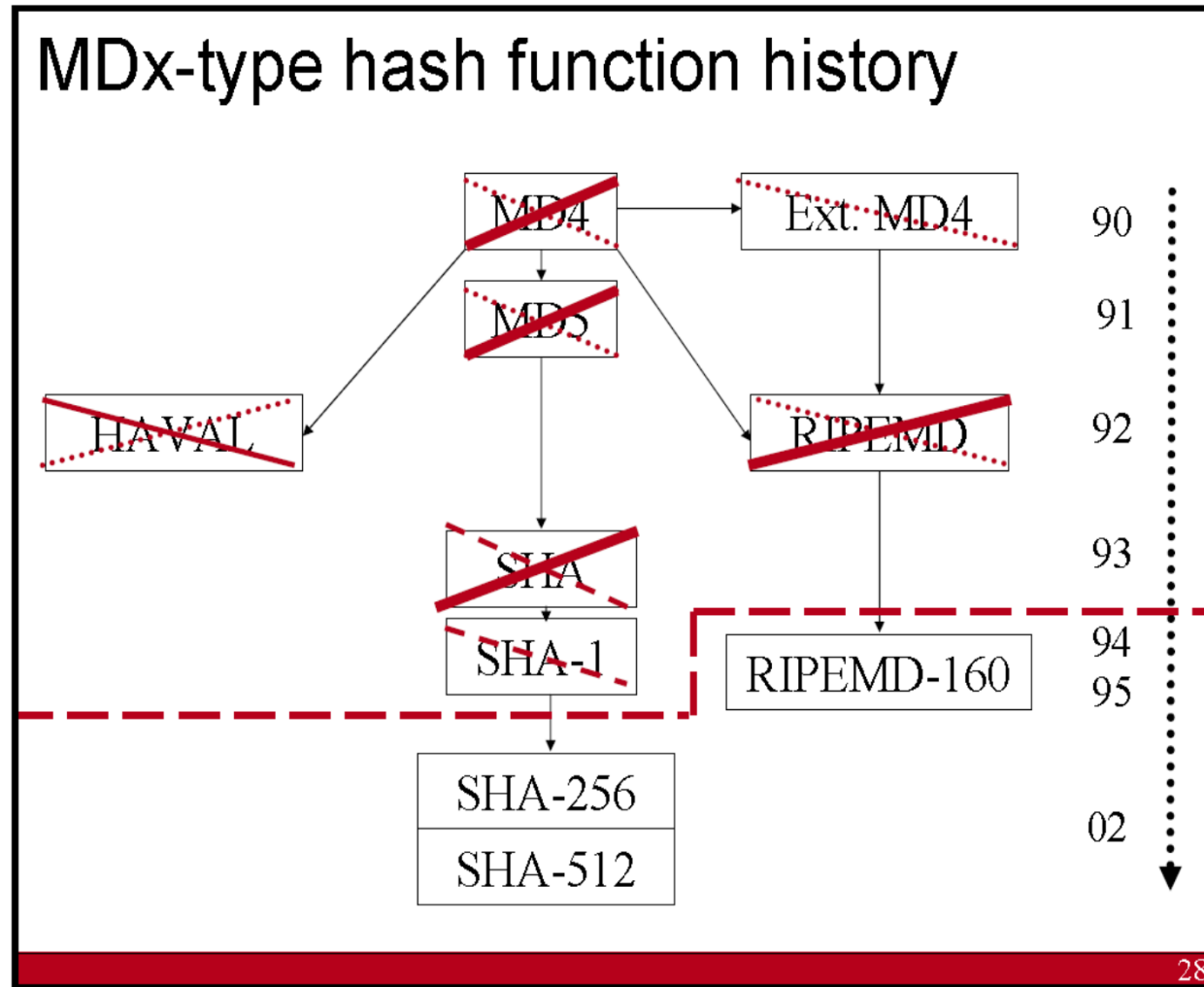
One-Way-Hashfunktionen

→ SHA-3 (Secure Hash Algorithm)

- 2012 wurde Keccak vom NIST zum Standard ausgewählt.
- Hashwert: 224 Bit, 256 Bit, 384 Bit, 512 Bit
- Einstellbare Rundenzahl
- Einstellbare Wortlänge

One-Way-Hashfunktionen

→ Geschichte der Hashfunktionen



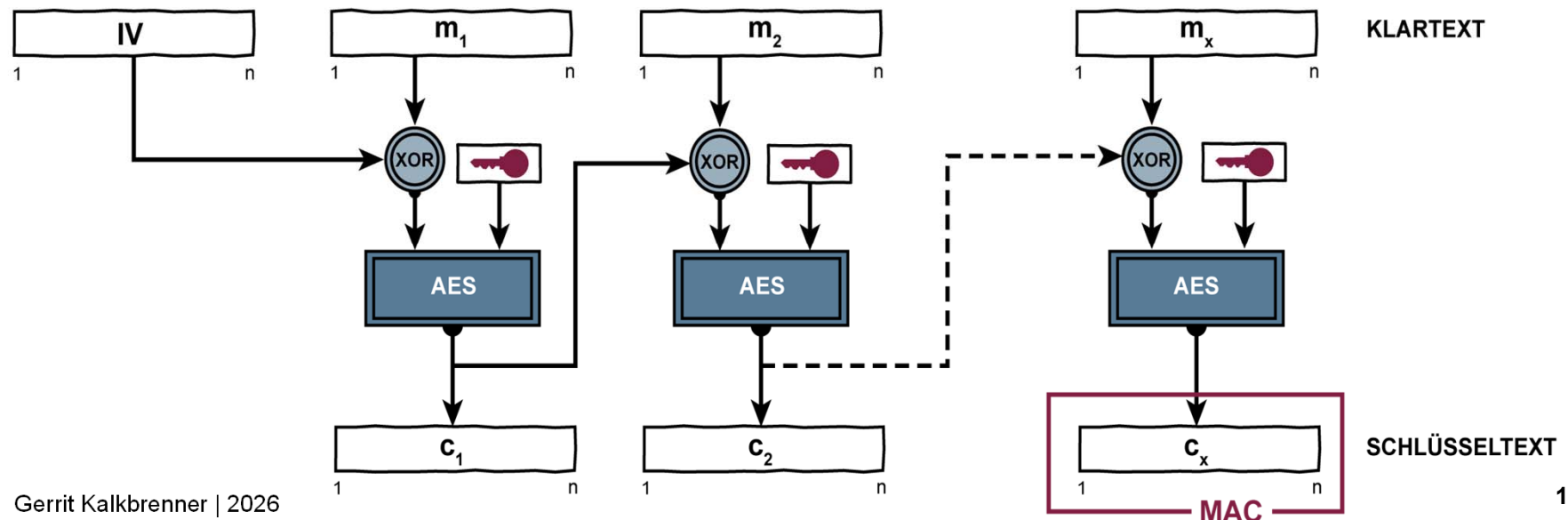
Cryptographic Algorithms and Protocols for Network Security - Bart Preneel
2008



- Ein Message Authentication Code oder MAC ist eine Einweg-Hashfunktion, die einen Schlüssel enthält, mit nur diesem man den Hashwert verifizieren kann.
- Damit kann man Authentizität ohne Geheimhaltung erreichen.
- Mit Hilfe von MACs können mehrere Benutzer ihre Dateien authentifizieren und einzelne Benutzer können mit MACs überprüfen, ob ihre Dateien verändert wurden, z.B. von Viren.
- Im Gegensatz zu Einweg-Hashfunktionen ist der Schlüssel des MACs zur Berechnung des Hashwertes nur dem Benutzer bekannt und der Hashwert kann nicht unbemerkt verändert werden.
- Eine einfache Möglichkeit zur Umwandlung einer Einweg-Hashfunktion in einen MAC besteht darin, den Hashwert mit einem symmetrischen Algorithmus zu verschlüsseln.
- Jeder MAC kann in eine Einweg-Hashfunktion umgewandelt werden, indem man den Schlüssel veröffentlicht.

One-Way-Hashfunktionen → CBC MAC

- CBC MAC, weit verbreiteter Standard [NIS85].
- Die Idee ist die Verwendung von DES (oder auch andere wie AES) im CBC Modus und die anschließende Verwendung des letzten Blocks des Ciphertextes als Prüfsumme.
- Diese Verfahren wird oft in der Bankenwelt verwendet.





One-Way-Hashfunktionen

→ HMAC (1/5)

- HMAC (Keyed-Hashing for Message Authentication)
Randbedingungen: (Internet-Standard (RFC 2104), z.B. IPSec)
- Die Geschwindigkeit der Hashfunktion soll nur wesentlich verlangsamt werden!
- Das Verfahren soll mit möglichst vielen Hashfunktionen zusammenarbeiten, ohne dass diese modifiziert werden müssen.
- Die Sicherheit der Hashfunktion darf durch die Manipulation mit geheimen Schlüsseln nicht verringert werden.



One-Way-Hashfunktionen

→ HMAC (2/5)

- **HMAC = KH(K XOR opad, H(K XOR ipad, M))**
 - $\text{ipad} = 0x36, 0x36, 0x36, \dots$ (gleiche Länge wie die Blocklänge der Hashfunktion)
 - $\text{opad} = 0x5c, 0x5c, 0x5c, \dots$ (gleiche Länge wie die Blocklänge der Hashfunktion)
 - K = geheimer Schlüssel
 - M = Input (Nachricht)
 - XOR = bitweise modulo 2 addieren
 - H = „Keyed-Hashing for Message Authentication“-Verfahren -HMAC-Verfahren



One-Way-Hashfunktionen

→ HMAC (3/5)

- Die Felder ipad und opad haben eine Länge, die der Blockgröße B der eingesetzten Hashfunktion entspricht (64 Bytes bei SHA-1 und RIPEMD).
- Der Schlüssel K wird durch das Anhängen von Nullen ebenfalls auf die Länge B gebracht.
- Verknüpfe den auf die Länge B gebrachten geheimen Schlüssel K mittels XOR mit dem Feld ipad.
- Stelle das Ergebnis dieser Operation vor die Nachricht und berechne mit der Hashfunktion den Hashwert aus diesem Input.
- Der Hashwert hat die Länge L (16 Byte bei SHA-1 und RIPEMD).



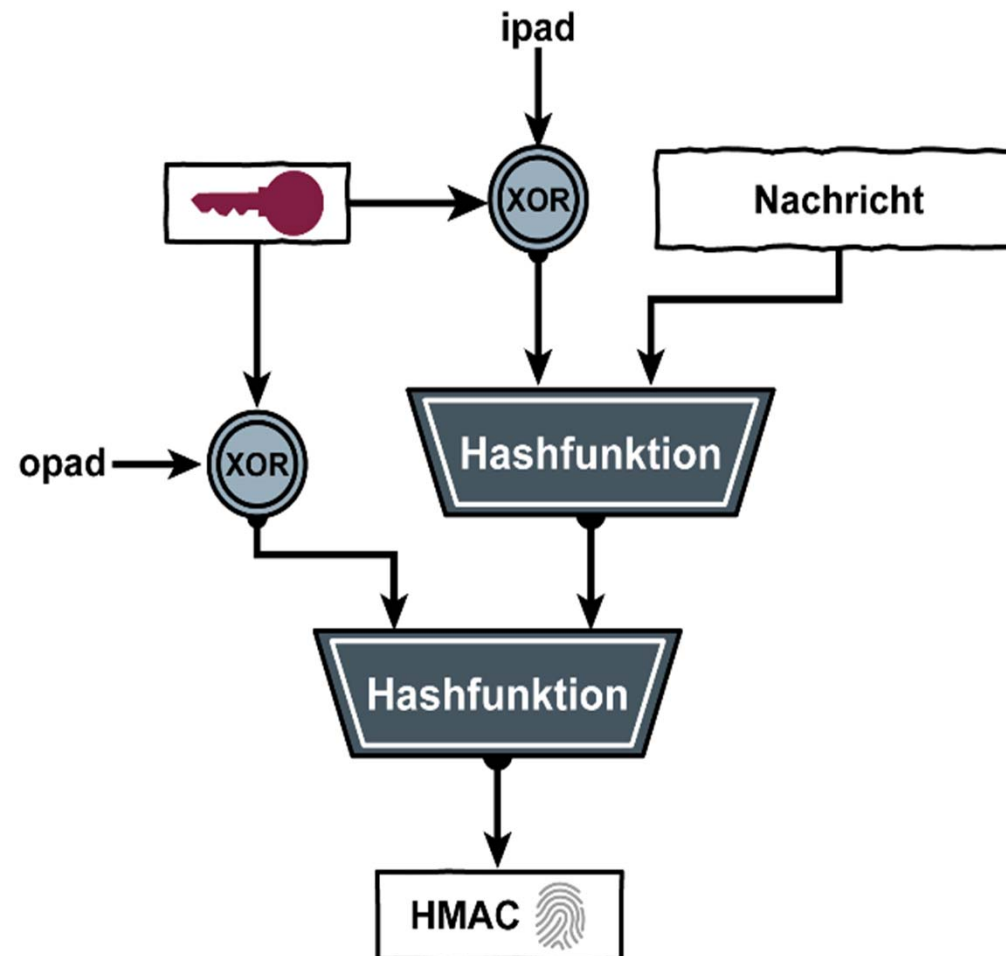
One-Way-Hashfunktionen

→ HMAC (4/5)

- Verknüpfe den auf die Länge B gebrachten geheimen Schlüssel K mittels XOR mit dem Feld opad.
- Stelle das Ergebnis dieser Operation (Länge B) vor den Hashwert (Länge L) und berechne mit der Hashfunktion den HMAC-Hashwert.
- Der HMAC-Hashwert hat die Länge L (16 Byte bei SHA-1 und RIPEMD).

One-Way-Hashfunktionen

→ HMAC (5/5)





- Ziele und Ergebnisse der Vorlesung
- Einführung
- Grundlagen der Verschlüsselung
- Elementarverschlüsselungen
- Symmetrische oder Private-Key Verschlüsselungsverfahren
- Asymmetrische oder Public-Key Verschlüsselungsverfahren
- One-Way-Hashfunktionen
- **Zusammenfassung**



Kryptographie

→ Zusammenfassung (1/2)

- Kryptographische Verfahren sind die Basis der meisten Sicherheitssysteme.
- Die Sicherheit eines kryptographischen Systems
 - hängt niemals von der Geheimhaltung der Algorithmen ab
 - basiert ausschließlich auf der Geheimhaltung des privaten Schlüssels
- Der jeweilige Algorithmus sollte anhand der folgenden Kriterien ausgewählt werden:
 - Die Kosten, um den Algorithmus zu brechen, sollten höher als die damit geschützten Informationen sein.
 - Der zeitliche Aufwand, um den Algorithmus zu knacken, sollte länger als das Interesse an den Informationen sein.



Kryptographie

→ Zusammenfassung (2/2)

- Es sollten die Empfehlungen der Experten beachtet werden (in D z.B. BSI u. Bundesnetzagentur bezüglich des Signaturgesetzes).
- Web-Seiten:
 - www.bsi.de
 - www.bundesnetzagentur.de
 - www.cryptool.de