IT-Sicherheit

Symmetrische Kryptographie

Prof. Dr. Dominik Merli, Prof. Dr. Lothar Braun

Sommersemester 2020

Hochschule Augsburg - Fakultät für Informatik

Begriffserklärung

- Kryptographie
  - *griechisch* kryptós = versteckt, verborgen, geheim
  - *griechisch* gráphein = schreiben
  - Früher: Wissenschaft der Geheimschriften
  - Heute: Wissenschaft der Informations- und Datensicherheit
  - Oft synonym: Kryptologie

- Kryptoanalyse/Kryptanalyse
  - Früher: Wissenschaft der Untersuchung verschlüsselter Nachrichten
  - Heute: Wissenschaft der Analyse von diversen kryptographischen Verfahren

Symmetrische Kryptographie

- Wichtigste Eigenschaft
  - Gleicher, geheimer Schlüssel auf beiden Seiten (Sender und Empfänger)
- Weitere Eigenschaften
  - Hohe Performance möglich
  - Relativ kleine/leichtgewichtige Implementierungen möglich

Geschichte der Kryptographie

Caesar-Chiffre - 1. Jh. v. Chr.

- Angeblich von Julius Caesar eingesetzt
- Substitution mit einem verschobenen Alphabet, z.B. ROT13
- Kann einfach gebrochen werden (nur 26 Möglichkeiten)
- Beispiel (um drei Buchstaben nach rechts verschoben):

Klartext	a	b	c	d	e	f	g	h	i	j	k	l	m
Geheimtext	x	y	z	a	b	c	d	e	f	g	h	i	j

Klartext	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimtext	k	l	m	n	o	p	q	r	s	t	u	v	w

Vigenère-Chiffre - 16. Jh.

- Entwickelt von Blaise de Vigenère
- Nutzt ein Schlüsselwort und mehrere Alphabete
- Kryptoanalyse: Buchstabenhäufigkeit, Schüsselwortperiode (erstmals gebrochen durch Charles Babbage Mitte 19. Jh.)
- Beispiel (mit reduzierten Alphabeten):

	Klartext			
Schlüssel	a	b	c	d
	b	c	d	a
	c	d	a	b
	d	a	b	c

Kerckhoffs Prinzip - 19. Jh.

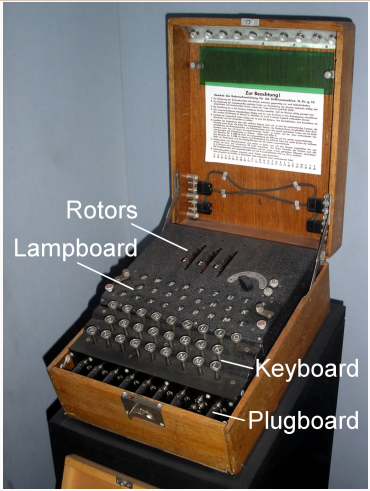
- Sechs Prinzipien für den Entwurf kryptographischer Systeme
- Beschrieben durch Auguste Kerckhoff
- Kontext: Militärische Kryptographie
- Wichtigste Forderung:
  - **Geheimhaltung des Verfahrens darf nicht von Nöten sein**
  - d.h. Gegner/Angreifer können nichts daraus lernen
  - d.h. der Schlüssel ist das einzige Geheimnis

One-Time Pad - Ende 19. Jh.

- Kombination einer Nachricht mit einem gleich langen Schlüssel
- Kann nicht gebrochen werden, wenn gilt:
  - Schlüssel ist zufällig gewählt
  - Schlüssel wurde noch nie zuvor genutzt
  - Schlüssel wird komplett geheim gehalten
- Beispiel XOR
  - Nachricht $\oplus$ Schlüssel
  - `0110101011010111` $\oplus$ `1010101110110011`

Enigma - 1918

- Entwickelt von Arthur Scherbius am Ende des 1. Weltkriegs
- Polyalphabetische Substitution durch elektrische Pfade und Rotorscheiben
- Meist mit täglich wechselnden Schlüsseln genutzt
- Im großen Stil gebrochen mit Maschinen von Alan Turing (1939/1940)



Karsten Sperling, Public Domain

Caesar nutze bereits im 1. Jh. v. Chr. eine Substitution zum Verschlüsseln von Nachrichten. Richtig oder falsch?

A) Definitiv Richtig!

B) Falsch, Substitution wurde erst später genutzt!

Seit Ende des 19. Jh. ist das One-Time Pad bekannt und wird auch heute noch in diversen Anwendungen eingesetzt. Richtig oder falsch?

A) Richtig, es kommt selbst auf jedem Smartphone zum Einsatz!

B) Falsch, ein One-Time Pad ist total unpraktisch!

Moderne symmetrische Chiffren

- Klartext-Nachricht M
- Geheimtext-Nachricht C
- Symmetrischer Schlüssel K
- Verschlüsselungsfunktion $Enc_K()$
- Entschlüsselungsfunktion $Dec_K()$

$$C = Enc_K(M)$$

$$M = Dec_K(C)$$

Sicherheitsniveau

- Schlüssellänge als Indikator für Sicherheitslevel
  - z.B. 56-bit, 64-bit, 80-bit, 128-bit, 192-bit, 256-bit, 512-bit
- Sicherheitslevel gibt möglichen Schlüsselraum an
  - z.B. 64-bit für 2^{64} mögliche Schlüssel
  - Ist ein Schlüsselbit bekannt, reduziert sich der Suchraum um den Faktor 2

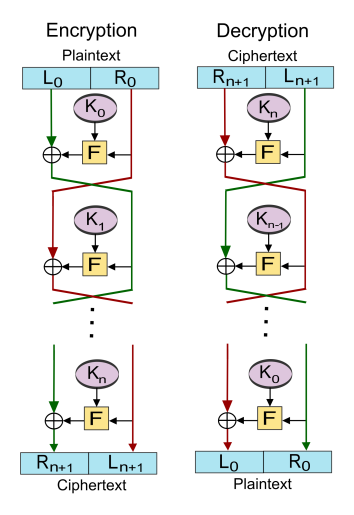
Block- und Strom-Chiffren

- Block-Chiffren
  - Verarbeiten Klar-/Geheimtexte Block für Block
  - Feste Anzahl von Bits in einem Block
- Strom-Chiffren
  - Verknüpfen einen Klartext-Strom mit einem Schlüssel-Strom
  - Verknüpfung erfolgt Bit für Bit

Data Encryption Standard (DES) - 1977

- Entstanden aus Arbeiten von Horst Feistel (IBM)
- Standardisiert im Jahr 1977
- Schlüssellänge: 56-bit (+ 8 Paritätsbits)
  - Gilt heutzutage als unsicher
  - 1999 innerhalb von 22 Stunden und 15 Minuten gebrochen
- Blockgröße: 64-bit
- Basiert auf einem Feistel-Netzwerk mit 16 Runden

Feistel-Netzwerk / Feistel-Chiffre



Amirki (Wikipedia), CC BY-SA 3.0

Triple DES (3DES) - 1998

- DES wird auf jeden Block dreifach angewendet ($K1, K2, K3$)
- Gesamte Schlüssellänge: $3 \cdot 56 = 168$ Bits
- Mehrere Attacken gegen 3DES bekannt
- Einschätzung durch NIST: 80-bit Sicherheit

$$C = Enc_{K3}(Dec_{K2}(Enc_{K1}(M)))$$

$$M = Dec_{K1}(Enc_{K2}(Dec_{K3}(C)))$$

Advanced Encryption Standard (AES) - 2001

- Gewinner des NIST AES Wettbewerbs (1997 - 2000)
- Entwickelt von Vincent Rijmen und Joan Daemen
- Ursprünglicher Name: Rijndael (niederländisch)
- Standardisiert in FIPS PUB 197 und ISO/IEC 18033-3
- Basiert auf einem Substitutions-Permutations-Netzwerk
- Blockgröße: 128-bit
- Schlüssel: 128-bit (10 Runden), 192-bit (12 R.), 256-bit (14 R.)

AES Zustand (engl. state)

- Besteht aus 16 Bytes in einer 4x4 Matrix

$$state = \begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

AES Ablauf

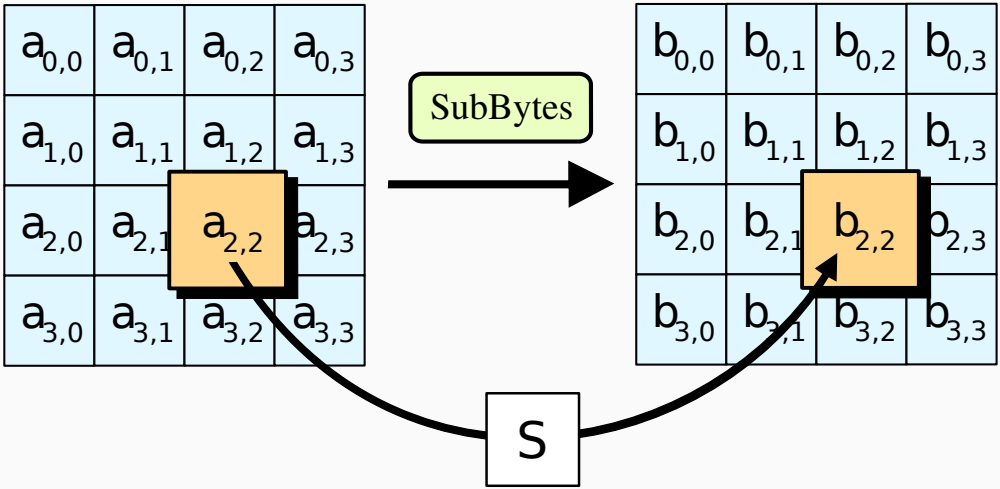
1) Schlüssel-Expansion für R Runden (10, 12 oder 14)

2) Initiale Runde ($r = 0$)
   a) `AddRoundKey( key[0] )`

3) Weitere Runden ($r = 1 \ldots R - 1$)
   a) `SubBytes()`
   b) `ShiftRows()`
   c) `MixColumns()`
   d) `AddRoundKey( key[r] )`

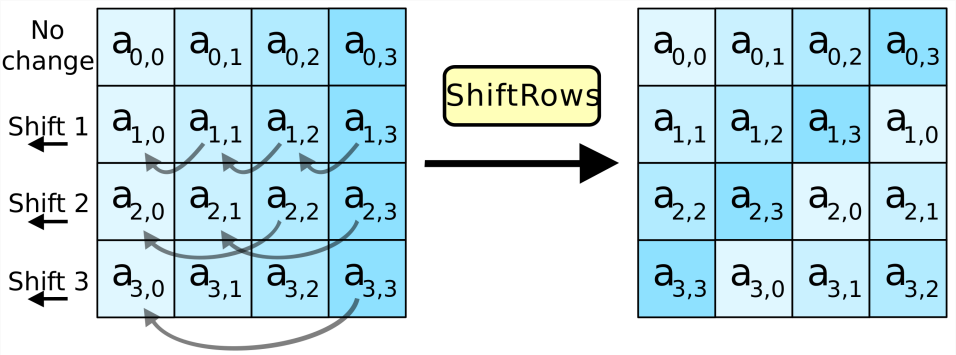
4) Letzte Runde ($r = R$)
   a) `SubBytes()`
   b) `ShiftRows()`
   c) `AddRoundKey( key[R] )`

AES SubBytes()



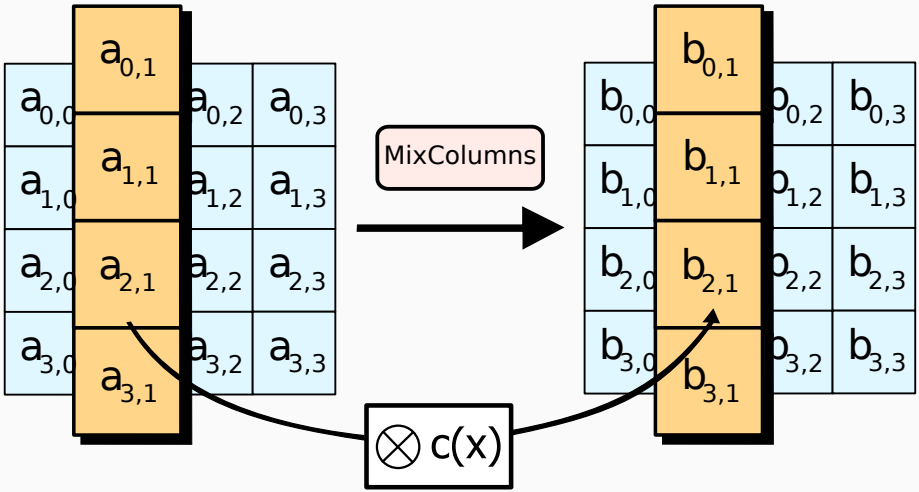
Matt_Crypto (Wikipedia), Public Domain

AES ShiftRows()



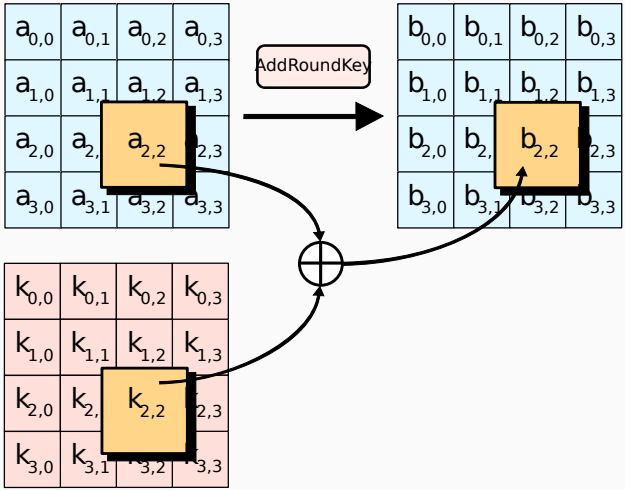
Matt_Crypto (Wikipedia), Public Domain

AES MixColumns()



Matt_Crypto (Wikipedia), Public Domain

AES AddRoundKey( )



Matt_Crypto (Wikipedia), Public Domain

AES Implementierung und Nutzung

- Implementierung
  - Effiziente Implementierung möglich (Hardware/Software)
  - Vielzahl von freien Bibliotheken verfügbar
  - Von manchen Prozessoren unterstützt, z.B. Intel AES-NI

- Nutzung
  - Festplatten- und Dateiverschlüsselung
  - Nutzdatenverschlüsselung in Transport Layer Security (TLS)
  - Viele weitere Einsatzmöglichkeiten ...

QUIZ: Advanced Encryption Standard (twbk.de)

Die Blockgröße von AES beträgt 128-bit für 128-bit Schlüssel und 256-bit für 256-bit Schlüssel. Richtig oder falsch?

A) Richtig!

B) Falsch!

QUIZ: Advanced Encryption Standard (twbk.de)

AES ist der Nachholger von DES, aber DES kann auch heut noch guten Gewissens eingesetzt werden. Richtig oder falsch?

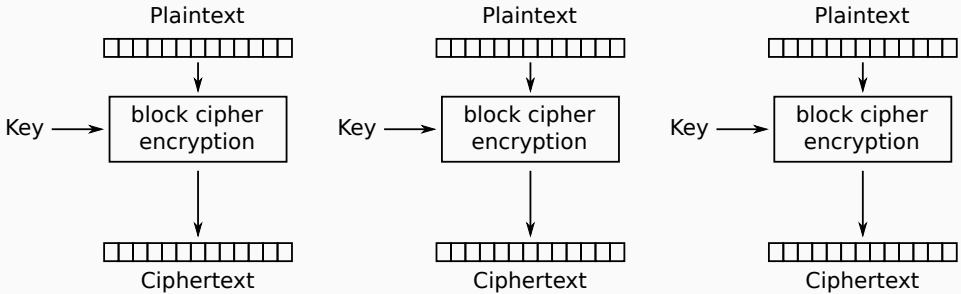
A) Richtig!

B) Falsch!

Betriebsmodi für Block-Chiffren

- Electronic Code Book Mode (ECB)
- Cipher Block Chaining Mode (CBC)
- Cipher Feedback Mode (CFB)
- Output Feedback Mode (OFB)
- Counter Mode (CTR)
- XOR-Encrypt-XOR Mode (XEX)
- XEX-based Tweaked-Codebook Mode with Ciphertext Stealing (XTS)
- Und viele weitere ...

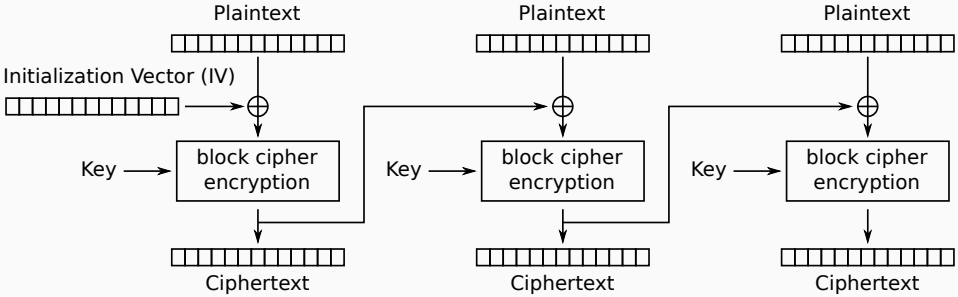
Verschlüsselung im ECB Modus



Electronic Codebook (ECB) mode encryption

WhiteTimberwolf (Wikipedia), Public Domain

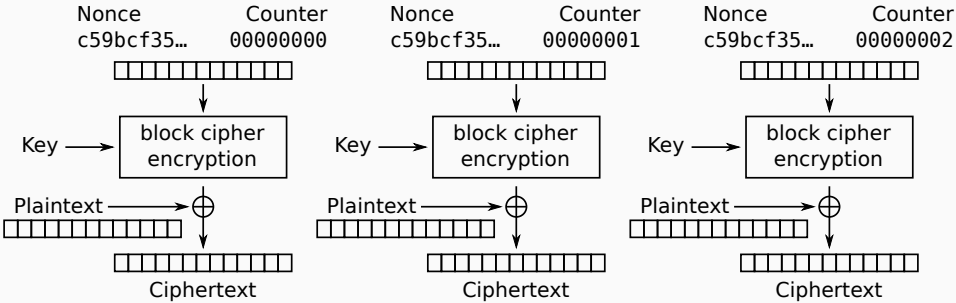
Verschlüsselung im CBC Modus



Cipher Block Chaining (CBC) mode encryption

WhiteTimberwolf (Wikipedia), Public Domain

Verschlüsselung im CTR Modus



Counter (CTR) mode encryption

WhiteTimberwolf (Wikipedia), Public Domain

Initialisierungs-Vektor (IV)

- Manchmal auch ”Nonce” (number used once) genannt
- Muss unbedingt passend zum Modus gewählt werden
  - Darf meist nur einmal benutzt werden
  - Muss manchmal zufällig/pseudo-zufällig gewählt sein

Weitere symmetrische Chiffren

- Block-Chiffren
  - PRESENT → Lightweight Cryptography
  - Threefish → Keine S-Box, Blockgrößen bis 1024-bit
  - Simon/Speck → Sehr effizient, entwickelt von NSA
  - Serpent → Zweiter Platz bei AES Wettbewerb
  - Camellia → Moderne Feistel Cipher
  - ...

- Strom-Chiffren
  - RC4 → Eine der ersten Stromchiffren, heute unsicher
  - Salsa/ChaCha → Moderne Add-Rotate-XOR Chiffren
  - ...

Gibt es noch Fragen?