Kryptografie verständlich

Ein Fachbuch für
Studierende und Anwender

von
Christof Paar und Jan Pelzl

www.crypto-textbook.com

Kapitel 5

Mehr über Blockchiffren

(Version: 1. Dezember 2016)

Übersicht

- Einsatzgebiete für Blockchiffren
- Verschlüsselung mit Blockchiffren: Operationsmodi
  - Electronic Code Book Modus (ECB)
  - Cipher Block Chaining Modus (CBC)
  - Output Feedback Modus (OFB)
  - Cipher Feedback Modus (CFB)
  - Counter Modus (CTR)
  - Galois Counter Modus (GCM)
- Genauere Betrachtung der ausführlichen Schlüsselsuche
- Erhöhen der Sicherheit von Blockchiffren

Blockchiffren
Verwendungsarten

- Eine Blockchiffre ist mehr als ein Verschlüsselungsalgorithmus:
  - Aufbau von Block-basieren Verschlüsselungsverfahren
  - Realisierung von Stromchiffren
  - Konstruktion von Hashfunktionen
  - Erzeugung von Message Authentication Codes
  - Aufbau von Schlüsselaustauschprotokollen
  - Konstruktion von Pseudozufallszahlengeneratoren
  - ...

- Die Sicherheit von Blockchiffren kann erhöht werden durch
  - Key Whitening
  - Mehrfachverschlüsselung

Übersicht

- Einsatzgebiete für Blockchiffren
- **Verschlüsselung mit Blockchiffren: Operationsmodi**
  - **Electronic Code Book Modus (ECB)**
  - Cipher Block Chaining Modus (CBC)
  - Output Feedback Modus (OFB)
  - Cipher Feedback Modus (CFB)
  - Counter Modus (CTR)
  - Galois Counter Modus (GCM)
- Genauere Betrachtung der ausführlichen Schlüsselsuche
- Erhöhen der Sicherheit von Blockchiffren

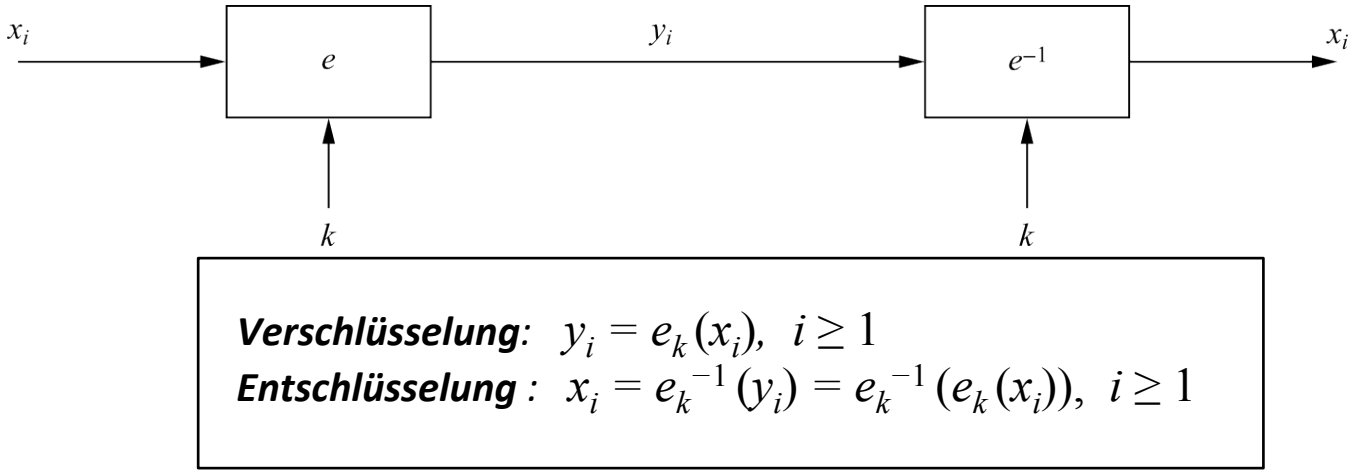
Blockchiffren
Verschlüsselung

- Zahlreiche Möglichkeiten der Verschlüsselung langer Klartexte (z.B. E-Mails, Dateien) mit einer Blockchiffre: Operationsmodi
  - Electronic Code Book Modus (ECB)
  - Cipher Block Chaining Modus (CBC)
  - Output Feedback Modus (OFB)
  - Cipher Feedback Modus (CFB)
  - Counter Modus (CTR)
  - Galois Counter Modus (GCM)

Blockchiffren

Electronic Code Book Modus

- $e_k(x_i)$ bezeichnet die Verschlüsselung eines b-Bit Klartextblocks x_i mit Schlüssel k
- $e_k^{-1}(y_i)$ bezeichnet die Verschlüsselung eines b-Bit Chiffratblocks y_i mit Schlüssel k
- Nachrichten größer als b Bit werden in b-Bit Blöcke aufgeteilt
- **Separate Verschlüsselung jedes einzelnen Blocks**



Blockchiffren

ECB Modus: Vor- und Nachteile

- Vorteile
  - Keine blockweise Synchronisierung zwischen Sender und Empfänger notwendig
  - Übertragungsfehler wirken nur auf dem betreffenden Block
  - Parallelisierbar
    - Vorteil für Anwendungen mit hohen Datendurchsätzen

- Nachteile
  - Verschlüsselung ist deterministisch
    - Identische Klartexte resultieren in identischen Chiffraten
    - Angreifer können mehrfach gesendete Texte erkennen
    - Klartextblöcke werden unabhängig voneinander verschlüsselt
      - Angreifer kann Blöcke vertauschen

Blockchiffren

ECB Modus: Beispiel eines Substitutions-Angriffs

- Annahme: Eine Abbildung von Klartext auf Chiffrat $x_i \rightarrow y_i$ ist bekannt
- Beispiel: Eine (sehr einfache) *elektronische Überweisung*

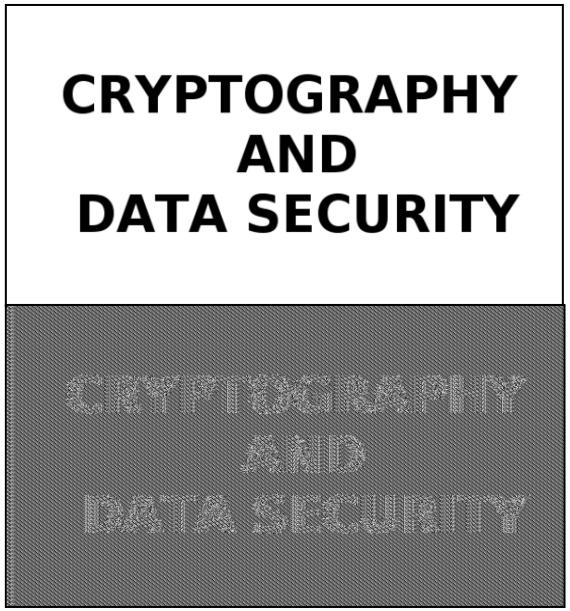
Block	1	2	3	4	5
	Sender Bank A	Sender Kontonr.	Empfänger Bank B	Empfänger Kontonr.	Betrag €

  - Weiter Annahme: Der Sitzungsschlüssel für die Kommunikation zwischen den Banken wechselt nicht zu häufig
  - Ein Angreifer sendet €1,00 wiederholt von seinem Konto bei Bank A zu seinem Konto bei Bank B
    - Er kann hierbei die sich wiederholenden Chiffratblöcke erkennen und speichert die Blöcke 1,3 und 4
  - Nun kann er einfach Block 4 einer anderen Überweisung durch den gespeicherten Block 4 ersetzen
    - *Alle Überweisungen von einem beliebigen Konto* bei Bank A auf ein beliebiges Konto bei Bank B werden auf das Konto des Angreifers bei Bank B umgeleitet!

Blockchiffren

ECB Modus: Beispiel einer verschlüsselten Bilddatei

- Identische Klartexte werden auf identische Chiffrate abgebildet



- Statistische Eigenschaften des Klartextes bleiben im Chiffrat erhalten

Übersicht

- Einsatzgebiete für Blockchiffren
- **Verschlüsselung mit Blockchiffren: Operationsmodi**
  - Electronic Code Book Modus (ECB)
  - **Cipher Block Chaining Modus (CBC)**
  - Output Feedback Modus (OFB)
  - Cipher Feedback Modus (CFB)
  - Counter Modus (CTR)
  - Galois Counter Modus (GCM)
- Genauere Betrachtung der ausführlichen Schlüsselsuche
- Erhöhen der Sicherheit von Blockchiffren

Blockchiffren

Cipher Block Chaining Modus (CBC)

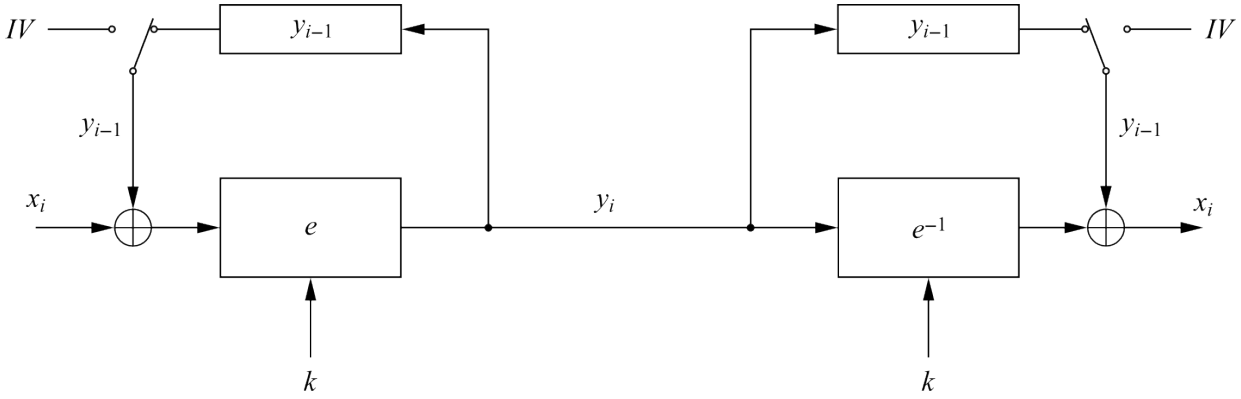
- Zwei Grundideen hinter des CBC:
  - „Verkettung“ aller Chiffrat-Blöcke
    - Chiffrat y_i hängt nicht mehr alleine von x_i aber auch von allen vorherigen Klartext-Blöcken ab
  - Randomisierung der Verschlüsselung durch Verwendung eines Initialisierungsvektors (IV)

***Verschlüsselung* (*erster Block*)**:	$y_1 = e_k(x_1 \oplus \mathrm{IV})$
***Verschlüsselung* (*weitere Blöcke*)**:	$y_i = e_k(x_i \oplus y_{i-1}), \quad i \geq 2$
***Entschlüsselung* (*erster Block*)**:	$x_1 = e_k^{-1}(y_1) \oplus \mathrm{IV}$
***Entschlüsselung* (*weitere Blöcke*)** :	$x_i = e_k^{-1}(y_i) \oplus y_{i-1}, \quad i \geq 2$

Blockchiffren

Cipher Block Chaining Modus (CBC)

- Für ersten Klartextblock x_1 gibt es keinen vorhergehenden Chiffratblock
  - Addition eines IV auf den ersten Klartext, im CBC Verschlüsselung nicht-deterministisch zu machen
  - Erstes Chiffrat y_1 hängt vom Klartext x_1 und dem IV ab
- Der zweite Chiffrat-Block y_2 hängt vom IV, x_1 *und* x_2 ab
- Der zweite Chiffrat-Block y_3 hängt vom IV und x_1, x_2 *und* x_3 ab, etc.



Blockchiffren

CBC: Substitutionsangriff

- Siehe letztes Beispiel (*electronische Überweisung*)
  - Ist der IV vernünftig gewählt, ist der Angriff nicht praktikabel
  - Ändert der IV sich nicht, kann ein Angreifer Überweisungen von seinem Konto bei Bank A zu Bank B erkennen
  - Wählen wir bei jeder Verschlüsselung einen neuen IV, wird der CBC Modus zu einem probabilistischen Verschlüsselungsverfahren, d.h. die Chiffrate zweier Klartexte sind vollkommen unterschiedlich
- Der IV muss *nicht* geheim gehalten werden!
- Üblicherweise ist der IV eine *nonce* (value used only once), welche nicht geheim sein muss

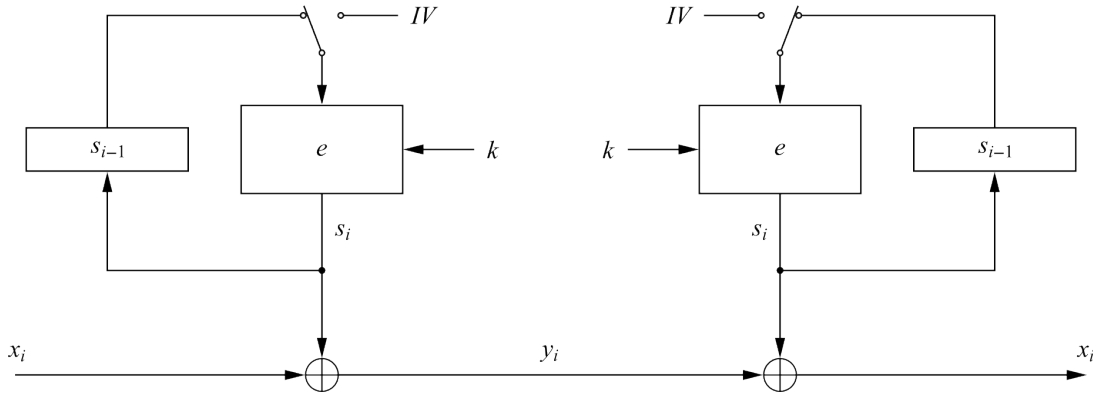
Übersicht

- Einsatzgebiete für Blockchiffren
- **Verschlüsselung mit Blockchiffren: Operationsmodi**
  - Electronic Code Book Modus (ECB)
  - Cipher Block Chaining Modus (CBC)
  - **Output Feedback Modus (OFB)**
  - Cipher Feedback Modus (CFB)
  - Counter Modus (CTR)
  - Galois Counter Modus (GCM)
- Genauere Betrachtung der ausführlichen Schlüsselsuche
- Erhöhen der Sicherheit von Blockchiffren

Blockchiffren

Output Feedback Modus (OFB)

- Aufbau einer *synchronen* **Stromchiffre** aus einer Blockchiffre
- Erzeugung eines Schlüsselstroms in Blöcken (nicht bitweise)
- Ausgabe der Chiffre sind die Bit des Schlüsselstroms S_i mit welcher der Klartext per XOR verschlüsselt wird



***Verschlüsselung* (*erster Block*)**: $s_1 = e_k(\mathrm{IV})$ *und* $y_1 = s_1 \oplus x_1$

***Verschlüsselung* (*weitere Blöcke*)**: $s_i = e_k(s_{i-1})$ *und* $y_i = s_i \oplus x_i$, $i \geq 2$

***Entschlüsselung* (*erster Block*)**: $s_1 = e_k(\mathrm{IV})$ *und* $x_1 = s_1 \oplus y_1$

***Entschlüsselung* (*weitere Blöcke*)** : $s_i = e_k(s_{i-1})$ *und* $x_i = s_i \oplus y_i$, $i \geq 2$

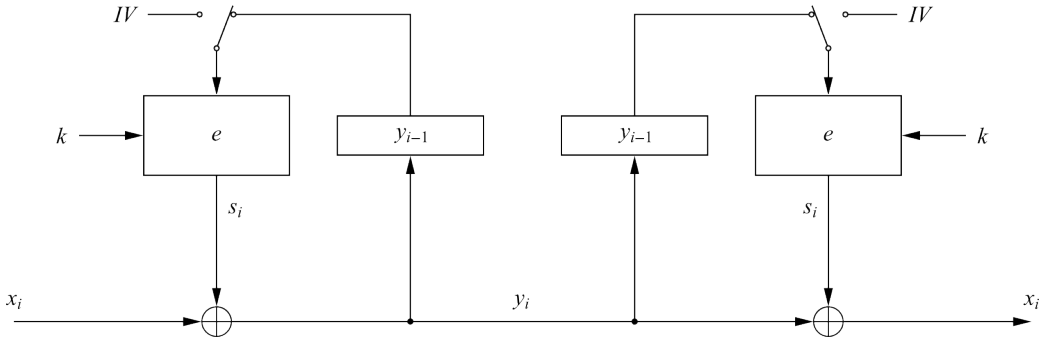
Übersicht

- Einsatzgebiete für Blockchiffren
- **Verschlüsselung mit Blockchiffren: Operationsmodi**
  - Electronic Code Book Modus (ECB)
  - Cipher Block Chaining Modus (CBC)
  - Output Feedback Modus (OFB)
  - **Cipher Feedback Modus (CFB)**
  - Counter Modus (CTR)
  - Galois Counter Modus (GCM)
- Genauere Betrachtung der ausführlichen Schlüsselsuche
- Erhöhen der Sicherheit von Blockchiffren

Blockchiffren

Cipher Feedback Modus (CFB)

- Aufbau einer *asynchronen* **Stromchiffre** aus einer Blockchiffre (wie beim OFB Modus)
- Blockweise generierung der S_i als Funktion des Chiffrats
- Durch Verwendung eines IV ist die CFB Verschlüsselung nicht-deterministisch



***Verschlüsselung* (*erster Block*)**:	$y_1 = e_k(\mathrm{IV}) \oplus x_1$
***Verschlüsselung* (*weitere Blöcke*)**:	$y_i = e_k(y_{i-1}) \oplus x_i, \quad i \geq 2$
***Verschlüsselung* (*erster Block*)**:	$x_1 = e_k(\mathrm{IV}) \oplus y_1$
***Verschlüsselung* (*weitere Blöcke*)**:	$x_i = e_k(y_{i-1}) \oplus y_i, \quad i \geq 2$

- Verwendung z.B. bei geringen Datenmengen (< Blockgröße)

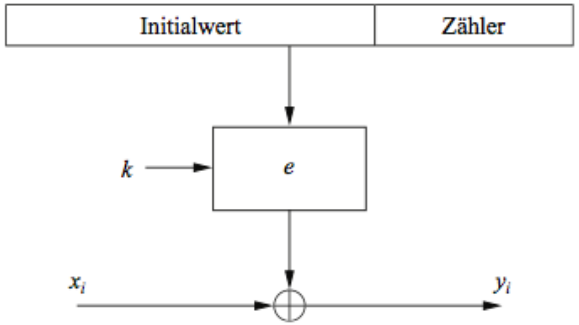
Übersicht

- Einsatzgebiete für Blockchiffren
- **Verschlüsselung mit Blockchiffren: Operationsmodi**
  - Electronic Code Book Modus (ECB)
  - Cipher Block Chaining Modus (CBC)
  - Output Feedback Modus (OFB)
  - Cipher Feedback Modus (CFB)
  - **Counter Modus (CTR)**
  - Galois Counter Modus (GCM)
- Genauere Betrachtung der ausführlichen Schlüsselsuche
- Erhöhen der Sicherheit von Blockchiffren

Blockchiffren

Counter Modus (CTR)

- Verwendung einer Blockchiffre als **Stromchiffre** (wie OFB und CFB Modi)
- Blockweise Erzeugung des Schlüsselstroms
- Eingang der Blockchiffre ist ein Zähler, welcher für jeden neuen Schlüsselstromblock inkrementiert wird



- Anders als beim CFB und OFB Modus kann der CTR Modus parallelisiert werden, d.h. die Verschlüsselung des zweiten Blocks kann vor Abschluss der ersten starten
  - Gut geeignet für Anwendungen mit hohem Datendurchsatz

Verschlüsselung:	$y_i = e_k(\text{IV} \mid\mid \text{CTR}_i) \oplus x_i, \quad i \geq 1$
Entschlüsselung:	$x_i = e_k(\text{IV} \mid\mid \text{CTR}_i) \oplus y_i, \quad i \geq 1$

Übersicht

- Einsatzgebiete für Blockchiffren
- **Verschlüsselung mit Blockchiffren: Operationsmodi**
  - Electronic Code Book Modus (ECB)
  - Cipher Block Chaining Modus (CBC)
  - Output Feedback Modus (OFB)
  - Cipher Feedback Modus (CFB)
  - Counter Modus (CTR)
  - **Galois Counter Modus (GCM)**
- Genauere Betrachtung der ausführlichen Schlüsselsuche
- Erhöhen der Sicherheit von Blockchiffren

Blockchiffren

Galois Counter Modus (GCM)

- Berechnet zusätzlich einen *Message Authentication Code* (MAC), d.h., eine kryptografische Checksumme einer Nachricht
- Der GCM bietet zwei Services:
  - Authentizität
    - Der Empfänger kann sicher den Ursprung der Nachricht nachweisen
  - Integrität
    - Der Empfänger kann sicher nachweisen, dass niemand die Nachricht bei der Übertragung verändert hat

Blockchiffren

GCM: Verschlüsselung

- Ableitung eines Startwertes für den Zähler aus dem IV und einer Seriennummer
- Erhöhung und anschließende Verschlüsselung des Zählers und XORierung mit dem ersten Klartextblock
- Für nachfolgende Klartextblöcke wird der Zähler erhöht und verschlüsselt

Blockchiffren

GCM: Authentisierung

- Durchführung einer verketteten Multiplikation im endlichen Körper
- Ableitung eines temporären Authentisierungsparameters g_i für jeden Klartext
  - g_i berechnet sich als XOR des aktuellen Klartextes und dem letzten g_{i-1} und der Multiplikation mit einer Konstanten H
  - H wird durch Verschlüsselung eines auf Null gesetzten Eingangs mit der Blockchiffre berechnet
- Alle Multiplikationen werden in dem 128 Bit endlichen Körper $\mathrm{GF}(2^{128})$ durchgeführt

Blockchiffren
GCM: Zusammenfassung

Verschlüsselung:

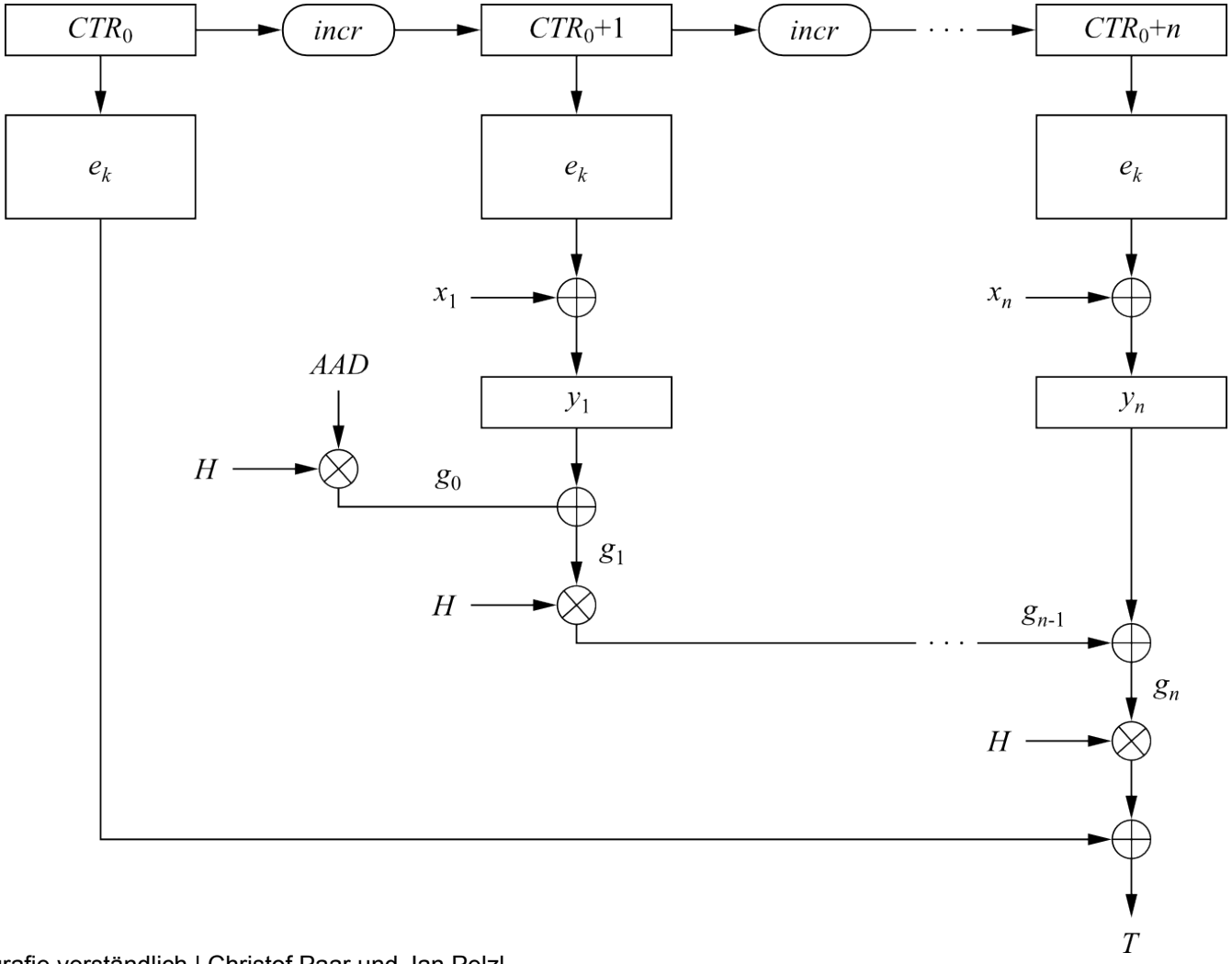
a. Ableitung eines Zählerwertes CTR_0 aus IV und Berechnung von $\mathrm{CTR}_1 = \mathrm{CTR}_0 + 1$
b. Berechnung des Chiffrats: $y_i = e_k(\mathrm{CTR}_i) \oplus x_i, \quad i \geq 1$

Authentisierung:

a. Berechnung des Unterschlüssels für die Authentisierung $H = e_k(0)$
b. Berechnung von $g_0 = AAD \times H$ (Multiplikation im endlichen Körper)
c. Berechnung von $g_i = (g_{i-1} \oplus y_i) \times H, \; 1 \leq i \leq n$ (Multiplikation im endlichen Körper)
d. Authentisierungs-Tag: $T = (g_n \times H) \oplus e_k(\mathrm{CTR}_0)$

Blockchiffren

GCM: Schematischer Ablauf



Übersicht

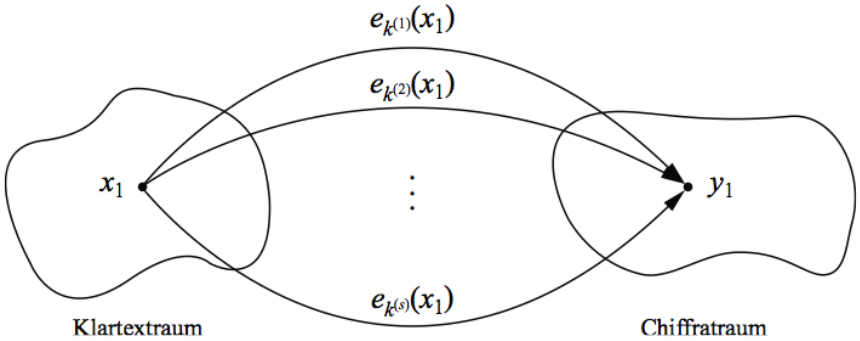
- Einsatzgebiete für Blockchiffren
- Verschlüsselung mit Blockchiffren: Operationsmodi
  - Electronic Code Book Modus (ECB)
  - Cipher Block Chaining Modus (CBC)
  - Output Feedback Modus (OFB)
  - Cipher Feedback Modus (CFB)
  - Counter Modus (CTR)
  - Galois Counter Modus (GCM)
- **Genauere Betrachtung der ausführlichen Schlüsselsuche**
- Erhöhen der Sicherheit von Blockchiffren

Blockchiffren
Ausführliche Schlüsselsuche

- Einfache ausführliche Schlüsselsuche, wenn ein Paar (x_1,y_1) bekannt ist:

$$DES_{k^{(i)}}(x_1) \overset{?}{=} y_1, \quad i = 0,1,\ldots,2^{56}-1$$

- Für die meisten Blockchiffren ist eine solche Suche jedoch komplizierter!
- Ein Brute-Force-Angriff kann falsche positive Ergebnisse produzieren (*false positive)*
  - Gefundene Schlüssel k_i stimmen nicht mit dem richtigen Schlüssel überein



  - Die Wahrscheinlichkeit hängt von der Größe des Schlüsselraums und des Klartextraums ab
  - Ein Brute-Force-Angriff ist immer noch *möglich*, es werden jedoch mehrere Klartext/Chiffrat-Paare benötigt

Blockchiffren

Ausführliche Schlüsselsuche: Beispiel

- Annahme: Blockchiffre mit Blockgröße 64 Bit und 80 Bit Schlüssellänge
- Verschlüsselung eines Klartextes x_1 mit allen möglichen 2^{80} Schlüsseln ergibt 2^{80} Chiffrate
  - Es existieren jedoch nur 2^{64} verschiedene
- Beim Ausprobieren aller Schlüssel für einen gegebenes Klartext/ Chiffrat-Paar finden wir $2^{80}/2^{64} = 2^{16}$ Schlüssel, welche die Abbildung $e_k(x_1) = y_1$ erfüllen

> Bei gegebener Blockchiffre mit k Bit Schlüssellänge und n Bit Blockgröße und bei t Klartext/Chiffrat-Paaren $(x_1, y_1), \ldots, (x_t, y_t)$, ist die Anzahl zu erwartender *falscher* Schlüssel (welche die Paare korrekt verschlüsseln):
>
> $$2^{k-tn}$$

- In diesem Beispiel ist die Wahrscheinlichkeit bei zwei Klartext/ Chiffrat – Paaren $2^{80-2\cdot 64} = 2^{-48}$
  - In der Praxis können wir annehmen, dass zwei Klartext/ Chiffrat – Paare ausreichen sind

Übersicht

- Einsatzgebiete für Blockchiffren
- Verschlüsselung mit Blockchiffren: Operationsmodi
  - Electronic Code Book Modus (ECB)
  - Cipher Block Chaining Modus (CBC)
  - Output Feedback Modus (OFB)
  - Cipher Feedback Modus (CFB)
  - Counter Modus (CTR)
  - Galois Counter Modus (GCM)
- Genauere Betrachtung der ausführlichen Schlüsselsuche
- **Erhöhen der Sicherheit von Blockchiffren**

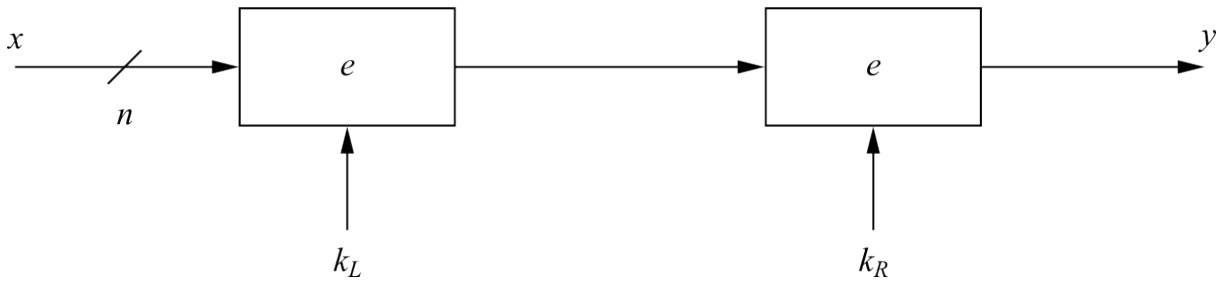
Blockchiffren

Erhöhung der Sicherheit

- Motivation: Erhöhung der Sicherheit von Blockchiffren in bestimmten Fällen, z.B. wenn nur eine Chiffre wie DES verfügbar ist
- Zwei mögliche Ansätze
  - Mehrfachverschlüsselung
    - Theoretisch sehr sicher, **manchmal** in der Praxis jedoch fast wirkungslos
    - Key Whitening

Blockchiffren
Zweifachverschlüsselung

- Ein Klartext x wird erst mit Schlüssel k_L und das resultierende Chiffrat mit Schlüssel k_R verschlüsselt:

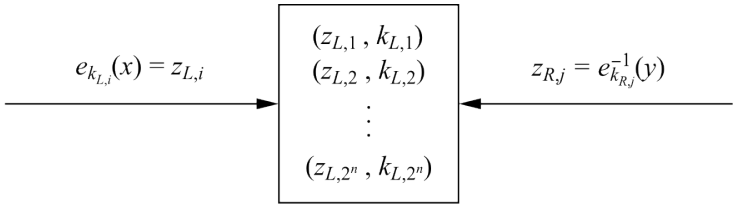


- Bei einer Schlüssellänge von k Bit würde eine ausführliche Schlüsselsuche $2^k \cdot 2^k = 2^{2k}$ Ver- oder Entschlüsselungen benötigen

Blockchiffren

Zweifachverschlüsselung: Meet-in-the-Middle Angriff

- Ein Meet-in-the-Middle Angriff benötigt $2^k+2^k = 2^{k+1}$ Operationen!



  - **Phase I**: Für gegebenes (x_1, y_1) Durchführung eines Brute-Force-Angriffs für die **linke Verschlüsselung** für alle $k_{L,i}$, i=1,2, ..., 2^k und Speicherung aller Ergebnisse in einer Tabelle mit 2^k Einträgen (je $n+k$ Bit)
    - Die Tabelle sollte nach den Ergebnissen der Verschlüsselung ($z_{L,i}$) sortiert werden
  - **Phase II**: Durchführung eines Brute-Force-Angriffs für die **rechte** Verschlüsselung (Verwendung der Entschlüsselungsfunktion) und Prüfung für jedes $z_{R,i}$ ob $z_{R,i}$ gleich einem Wert $z_{L,i}$ aus der Tabelle der ersten Phase ist
- Rechentechnische Komplexität

Anzahl der Ver- und Entschlüsselungen:	$2^k + 2^k = 2^{k+1}$
Anzahl der Speicherstellen:	2^k

- **Zweifachverschlüsselung ist kaum sicherer, als Einfachverschlüsselung!**

Blockchiffren
Dreifachverschlüsselung

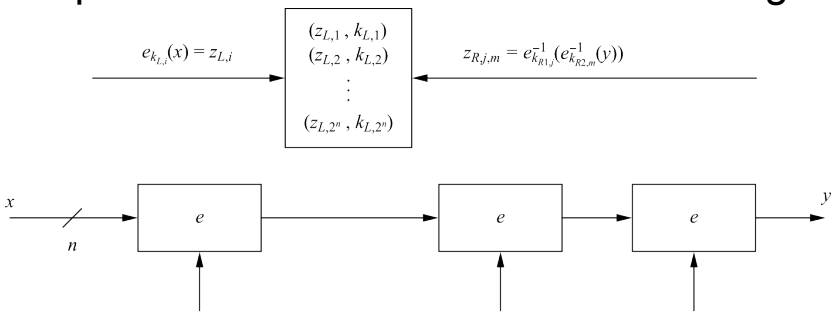
- Dreimalige Verschlüsselung eines Blocks hintereinander

$$y = e_{k3}\,(e_{k2}\,(e_{k1}\,(x)))$$

- Praktisch häufig verwendete Variante: EDE (Encryption-Decryption-Encryption)

$$y = e_{k3}\,(e^{-1}{}_{k2}\,(e_{k1}\,(x)))$$

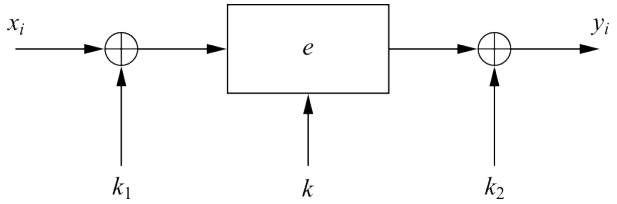
  - Vorteil: Wahl von $k1{=}k2{=}k3$ führt einfache DES-Verschlüsselung durch
- Wir können immer noch einen Meet-in-the-Middle-Angriff durchführen, welcher die *effektive Schlüssellänge* der Dreifachverschlüsselung von $3k$ auf $2k$ reduziert!
  - Beispiel: Im Falle von 3DES muss ein Angreifer 2^{112} Tests durchführen



- **Dreifachverschlüsselung verdoppelt die effektive Schlüssellänge!**

Blockchiffren
Key Whitening

- Härtung von Blockchiffren gegen Brute-Force-Angriffe
- Verwendung von zwei zusätzlichen „whitening“ Schlüsseln k_1 und k_2 zusätzlich zum regulären Schlüssel k, um den Klartext und das Chiffrat mit XOR zu maskieren:



- Stärkt die Chiffre nicht gegen analytische Angriffe wie lineare und differentielle Kryptanalyse
- Kein “Heilmittel” für inhärent schwache Chiffren
- Vernachlässigbarer rechentechnischer Zusatzaufwand
- Hauptanwendung bei analytische starken Chiffren, welche eine zu kurze Schlüssellänge haben, insbesondere DES
  - DESX ist eine Variante von DES mit Key Whitening

Lessons Learned

- Es gibt zahlreiche Modi, Blockchiffren zu betreiben. Die einzelnen Betriebsmodi haben jeweils spezielle Vor- und Nachteile
- Einige Modi wandeln eine Blockchiffre in eine Stromchiffre
- Es gibt Modi, welche neben der Verschlüsselung auch Authentisierung bereitstellen, d.h., eine kryptografische Checksumme schützt vor Manipulation der Nachricht
- Der einfache ECB Modus hat unabhängig von der zugrundeliegenden Chiffre Schwachstellen
- Der Counter Modus erlaubt Parallelisierung der Verschlüsselung und eignet sich gut für Anwendungen mit hohem Datendurchsatz
- Zweifachverschlüsselung mit einer gegebenen Blockchiffre erhöht die Sicherheit gegen Brute-Force-Angriffe kaum
- Dreifachverschlüsselung mit einer gegebenen Blockchiffre *verdoppelt* in etwa die Schlüssellänge
- Triple DES (3DES) hat eine effektive Schlüssellänge von 112 Bit
- Key Whitening erhöht die Schlüssellänge von DES ohne großen rechentechnischen Zusatzaufwand