fhwedel
UNIVERSITY OF APPLIED SCIENCES

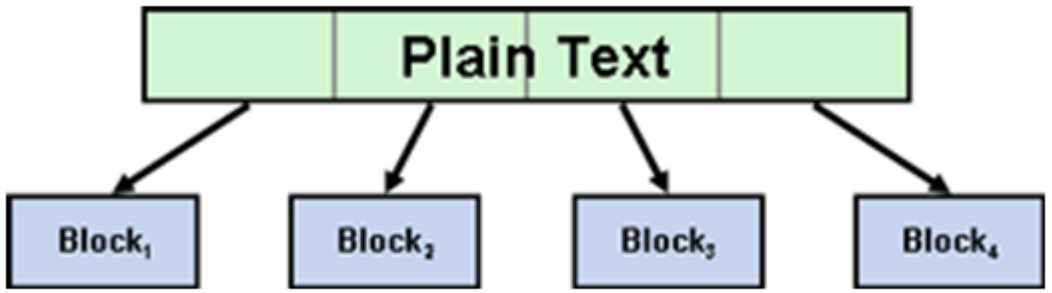
Inhalt

- Definition
- Allgemeiner Aufbau der Information
- Arbeitsweise
- Unterschiedliche Arten
- Kryptographische Modi

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Definition

- Verschlüsselungsverfahren
- Plaintext wird in gleichlange Blöcke zerlegt
- immer mit gleichem Schlüssel chiffriert



fhwedel
UNIVERSITY OF APPLIED SCIENCES

Allgemeiner Aufbau der Information

- 64 Bit-Blöcke oder Vielfache davon
- zu kurze Datenblöcke werden mit Paddings aufgefüllt
- der letzte Block beinhaltet die Info über die Länge der Codierung

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Arbeitsweise

A	B	XOR
wahr	wahr	falsch
wahr	falsch	wahr
falsch	wahr	wahr
falsch	falsch	falsch

- Logische Verknüpfungen
  - XOR – Operationen
  - Substitutionen
  - Permutation
  - Arithmetische Operationen der Dualarithmetik
- Verschlüsselungen in mehreren Runden
  - Verwirrung
  - Zerstreuung

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Unterschiedliche Arten

- Deterministische Blockchiffre
  - Chiffre-Textblöcke = Plaintextblöcke

- Indeterministische Blockchiffre
  - Chiffre-Textblöcke > Plaintextblöcke

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Kryptographische Modi

ECB

CBC

CFB

OFB

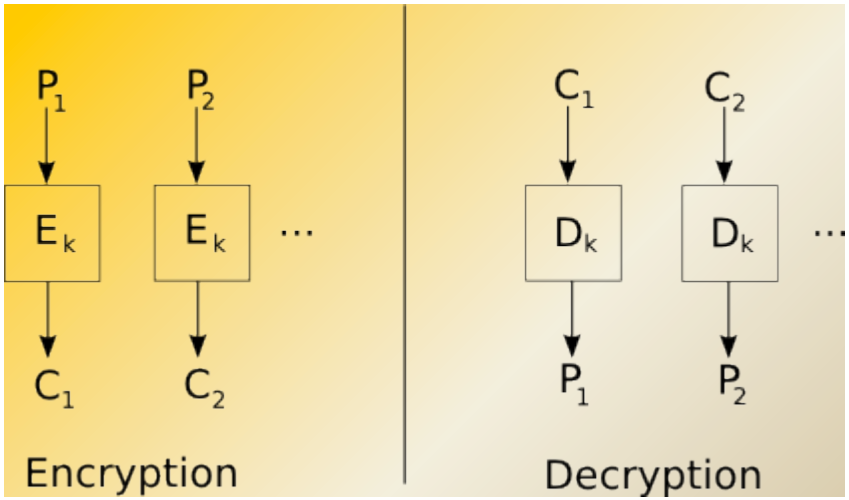
CTR

Kryptographische Modi

- Bestimmt die Verschlüsselung mehrerer Plaintextblöcke
- Definiert die Art des Verschlüsselungsalgorithmuses
- Unterschiedliche Sicherheitsstufen

fhwedel
UNIVERSITY OF APPLIED SCIENCES

ECB Electronic Code Book



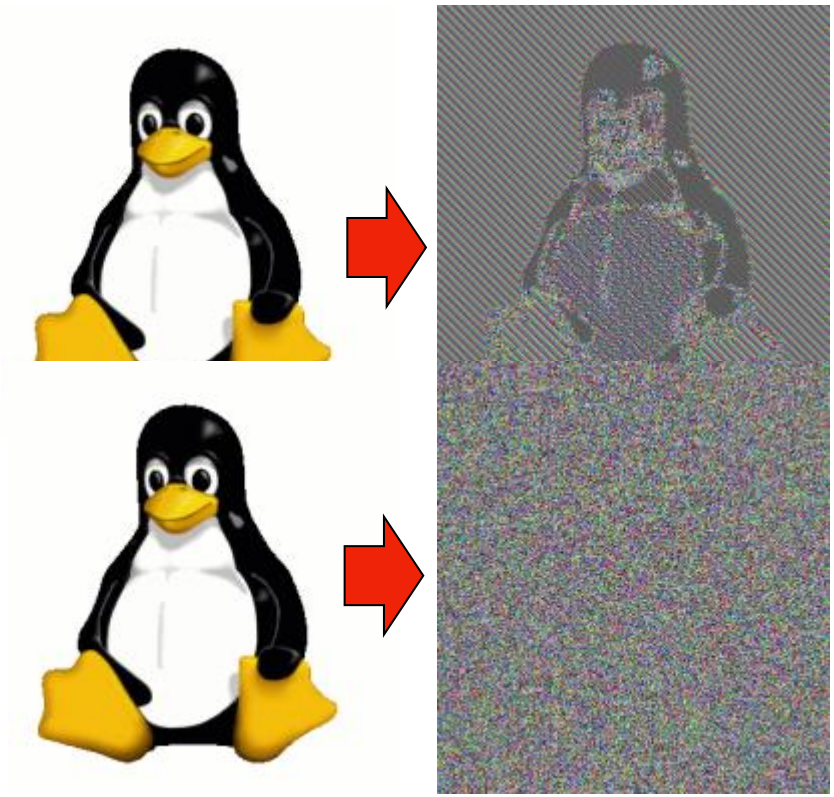
Unverkettet

- einfachster kryptographischer Mode (unverkettet)
- Plaintextblöcke unabhängig mit gleichem Schlüssel chiffriert
- Plaintextmuster bleiben erhalten

P = Plaintext (Klartext)
C = Ciphertext (Geheimtext)

fhwedel
UNIVERSITY OF APPLIED SCIENCES

ECB Electronic Code Book



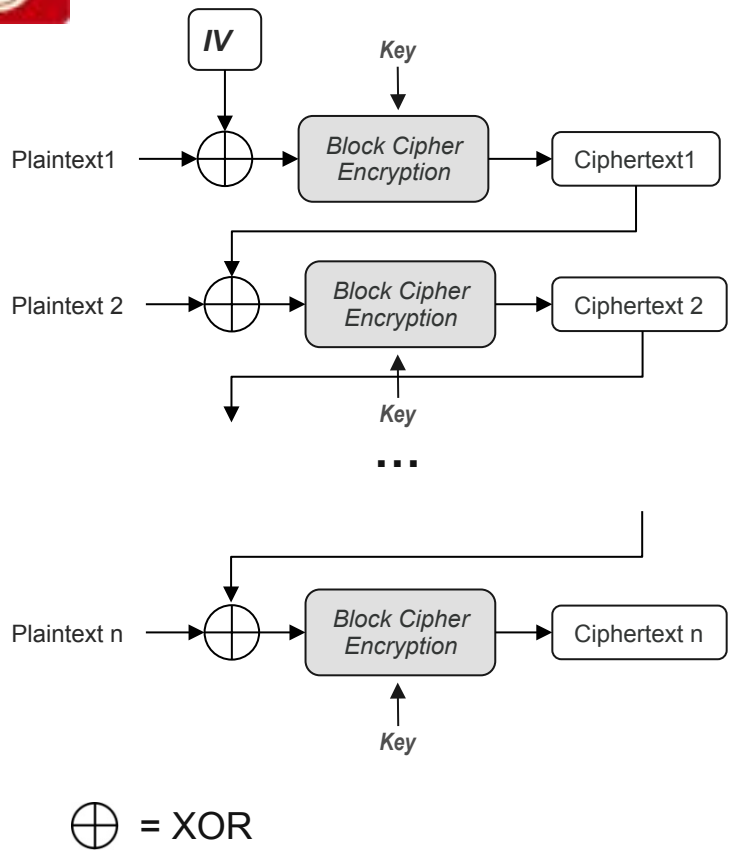
Unverkettet

- einfachster kryptographischer Mode (unverkettet)
- Plaintextblöcke unabhängig mit gleichem Schlüssel chiffriert
- Plaintextmuster bleiben erhalten

Sicherer, wenn verkettet …

fhwedel
UNIVERSITY OF APPLIED SCIENCES

CBC Cipher Block Chaining



⊕ = XOR

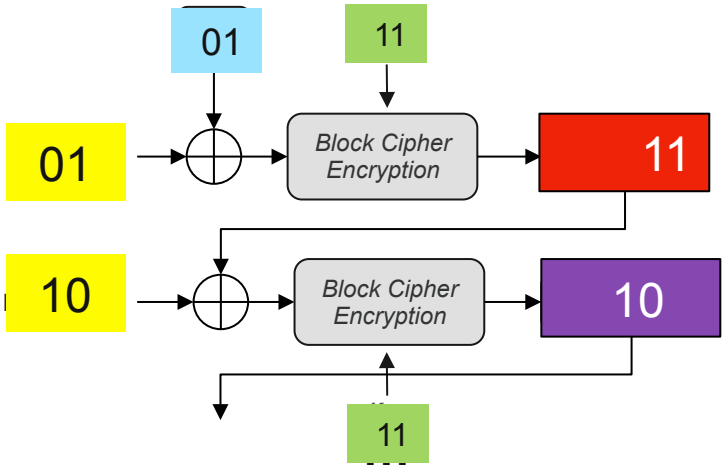
Einfache Rückkopplung

- Muster im Plaintext unkenntlich
- Erster Block mit Initialisierungs-vektor (*IV*) verknüpft
- Plaintextblöcke über XOR mit vor-herigem Cipher-Textblock verknüpft
- verketteter Textblock wird ver-schlüsselt = nächster Cipher-Textblock

fhwedel
UNIVERSITY OF APPLIED SCIENCES

CBC Cipher Block Chaining

Beispiel - Verschlüsselung



⊕ = XOR

Klartext

01 10

Aufgeteilt in Blöcke

01 = B_1, 10 = B_2

Schlüssel

11=k

Init. Vektor (IV)

01

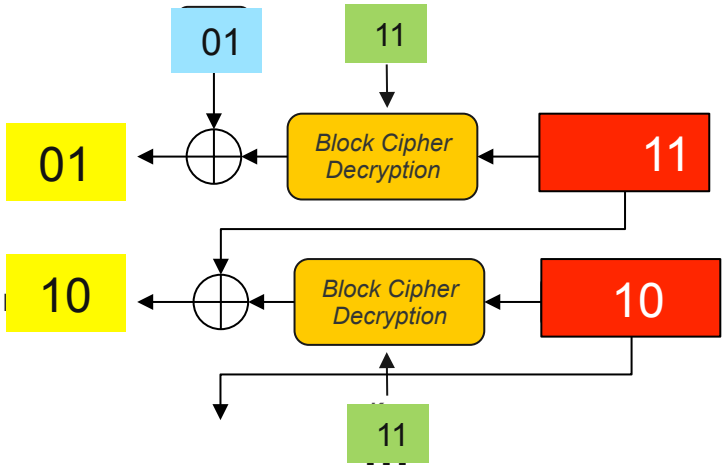
$$B_1 \oplus IV = 01 \oplus 01 = 00 = C'_1$$
$$C'_1 + k = 00 + 11 = 11 = C_1$$

$$B_2 \oplus C_1 = 10 \oplus 11 = 01 = C'_2$$
$$C'_2 + k = 01 + 11 = 10 = C_2$$

fhwedel
UNIVERSITY OF APPLIED SCIENCES

CBC Cipher Block Chaining

Beispiel - Entschlüsselung



⊕ = XOR

Ciphertext

11 10

Schlüssel

11=k

Init- Vektor (IV)

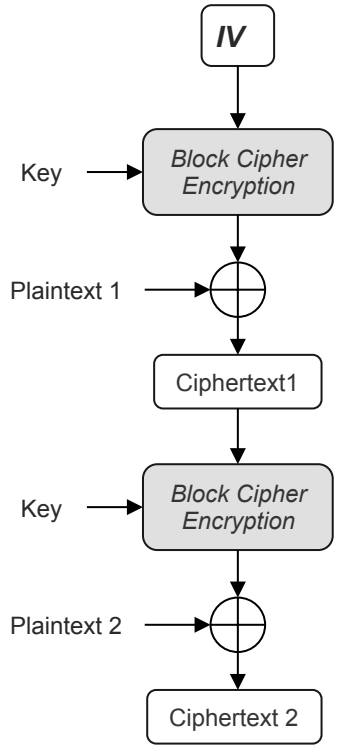
01

$$C_1 - k = 11 - 11 = 00 = C_1'$$
$$C_1' \oplus IV = 00 \oplus 01 = 01 = B_1$$

$$C_2 - k = 10 - 11 = 01 = C_2'$$
$$C_2' \oplus C1 = 01 \oplus 11 = 10 = B_2$$

fhwedel
UNIVERSITY OF APPLIED SCIENCES

CFB Cipher Feedback Mode



⊕ = XOR

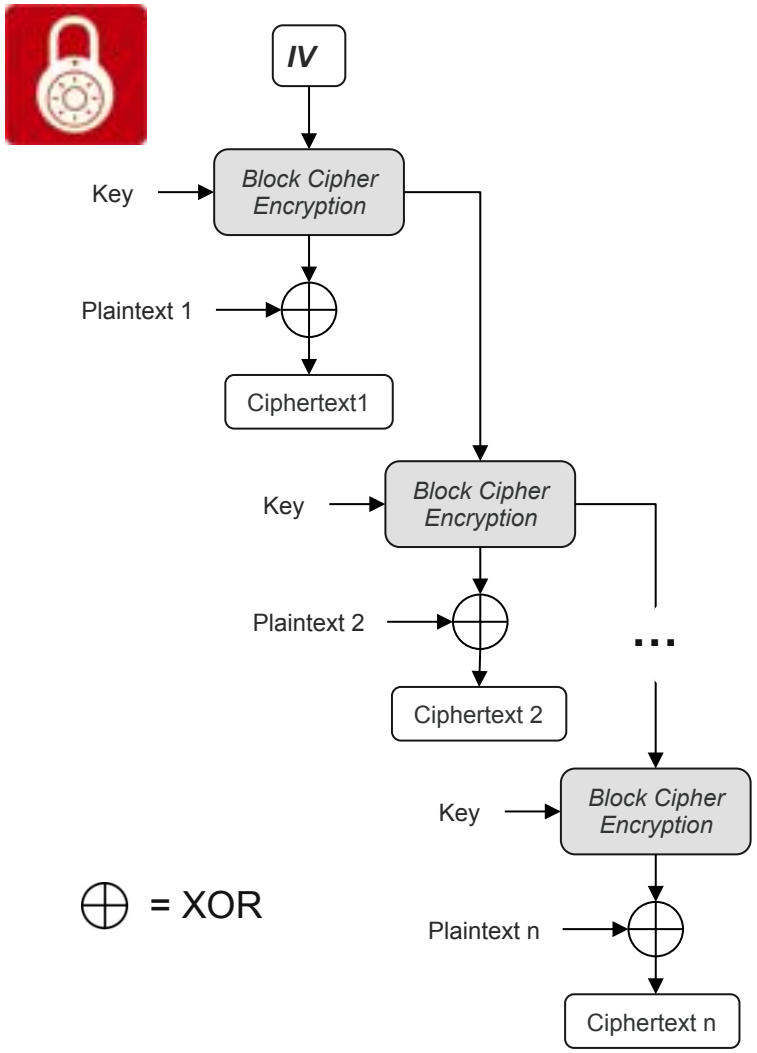
...

Rückkoppelung des Chiffre-Textblockes

- Initialisierungsvektor (*IV*) wird verschlüsselt
- Plaintextblöcke mit verschlüsseltem Initialisierungsvektor (*IV*) über XOR verknüpft = Cipher-Textblock
- Cipher-Textblock ersetzt (*IV)* im nächsten Block

fhwedel
UNIVERSITY OF APPLIED SCIENCES

OFB Output Feedback Mode

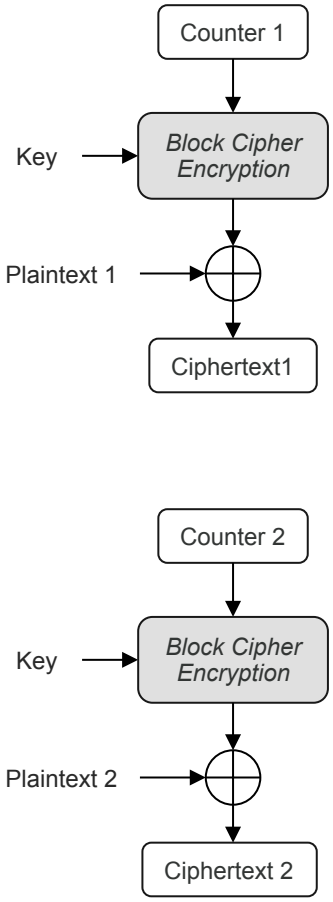


Neuverschlüsselung des temp. Schlüssels

- Initialisierungsvektor (*IV*) wird verschlüsselt
- XOR-Operator wird nur auf Plaintextblock angewandt
- Plaintextblöcke mit verschlüsseltem (*IV*) über XOR verknüpft = Cipher-Textblock
- verschlüsselter (*IV*) ersetzt (*IV*) im nächsten Block

fhwedel
UNIVERSITY OF APPLIED SCIENCES

CTR Counter Mode



Unabhängige Verschlüsselung

- kein Initialisierungsvektor (*IV*) dafür Counter
- XOR-Operator verkettet Plaintextblock mit Zwischenschlüssel = Cipher-Textblock
- jeder Block individuell, d.h. unverkettet

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Quellenverzeichnis

- ISO/IEC 10116:2006
- www.wikipedia.org/wiki/Blockverschlüsselung
- Comments to NIST concerning AES Modes of Operations

  Helger Lipmaa,Helsinki University of Technology (Finland) and University of Tartu (Estonia)
  Phillip Rogaway;University of California at Davis (USA) and Chiang Mai University (Thailand)
  David Wagner;University of California Berkeley (USA)
  http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ctr/ctr-spec.pdf
- Modes of Operation: Der Cipher Feedback Mode (CFB)

  Steffen Reith 7. Mai 2005
  www.thi.uni-hannover.de/fileadmin/lehre/ss05/kry/modes_op.pdf

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Quellenverzeichnis

- www.sec.in.tum.de/assets/lehre/ss09/kryptographie/Kapitel.4.pdf
- www.cryptoshop.com -- Suchwort: Blockchiffre
- What are the CFB and OFB modes?
  www.iks-jena.de/mitarb/lutz/security/cryptfaq/q83.html