**Blockchiffren**

klartextalphabet: \( A \)

chiffrealphabet: \( B \)

Schlüsselraum: \( K \)

meist: \( A = B = \{0, 1\}^n \)

\( f(m, k) = c \)

\( E_{c_k}(m) = c \)

**Blockchiffre**

\( f: A^n \times K \rightarrow B^n \)

\( m = n : \) Blocklänge

\( f^{-1}(c, k) = m \)

\( D_{c_k}(c) = m \)
Blockchiffren sind
- langsamer als Stromchiffren
- "sicherer"
- flexibler (verschiedene Betriebsmodi)

Achtung!
Verschlüsselungsverfahren garantierten Geheimhaltung, aber nicht Integrität oder Authentizität.
Betriebsmodi von Blockchiffren

Eigenschaften:

1. Fehlerfortpflanzung vs. Selbstkorrektur (Bitflip)
2. Synchronisation (Bitslip, Verschieben von Blockgrenzen)
3. Wahlfreier Zugriff beim Entschlüsseln
4. Malleability
Electronic Codebook Mode (ECB)

\[
m = m_1 \downarrow \quad m_2 \downarrow \quad m_3 \downarrow \quad m_4 \ldots \downarrow \quad m_r
\]

\[
k \rightarrow \text{ENC} \quad k \rightarrow \text{ENC} \quad \vdots \quad \vdots \quad \vdots
\]

\[
c = c_1 \downarrow \quad c_2 \downarrow \quad c_3 \downarrow \quad c_4 \ldots \downarrow \quad c_r
\]

Nachteil: gleiche Klartextblöcke \(\rightarrow\) gleiche Chiffriertblöcke

1. Fehler bleibt im Block
2. Keine Synchronisation (außer ganze Blöcke verschwinden)
3. Problemlos möglich
4. Blöcke tauschen, ersetzen, löschen, hinzufügen möglich
Cipher Block Chaining Mode (CBC)

$m = m_1 \oplus m_2 \oplus m_3 \cdots \oplus m_r$

$C = IV \rightarrow C_1 \rightarrow C_2 \rightarrow C_3 \cdots \rightarrow C_r$

4. Reihenfolge ändern nicht möglich, Bitflip siehe 1.

- Bitflip i-te Stelle
  $C_i$ zeigt $m_i$ kaputt

1. Bitflip → 1 Block kaputt, Bitflip im nachfolgenden Block
2. keine Synchronisation
3. möglich (früher anfangen) nur lesen!
Output Feedback Mode (OFB)

XOR zweier Chiffren, die mit dem gleichen IV (und gleicher k) verschlüsselt wurden geben XOR der Klartexte.

1. Keine Fehlerfortpflanzung bei IV: Chiffre kaputt
2. Keine Synchronisation
3. Kein (Schreiben durch Bitflip ...)
4. Strom chiffre
Counter Mode (CTR)

1. keine Fehlerfortpflanzung
2. keine Synchronisation
3. möglich
4. Stromklassifizierung
Nachtrag:

Cipher Feedback Mode (CFB)

1. Fehler bleibt solange Bitflip im Schieberegister
2. \( l=1 \): Selbstsynchronisation
3. möglich
4. Stromstörungen