II.1 Verschlüsselungsverfahren

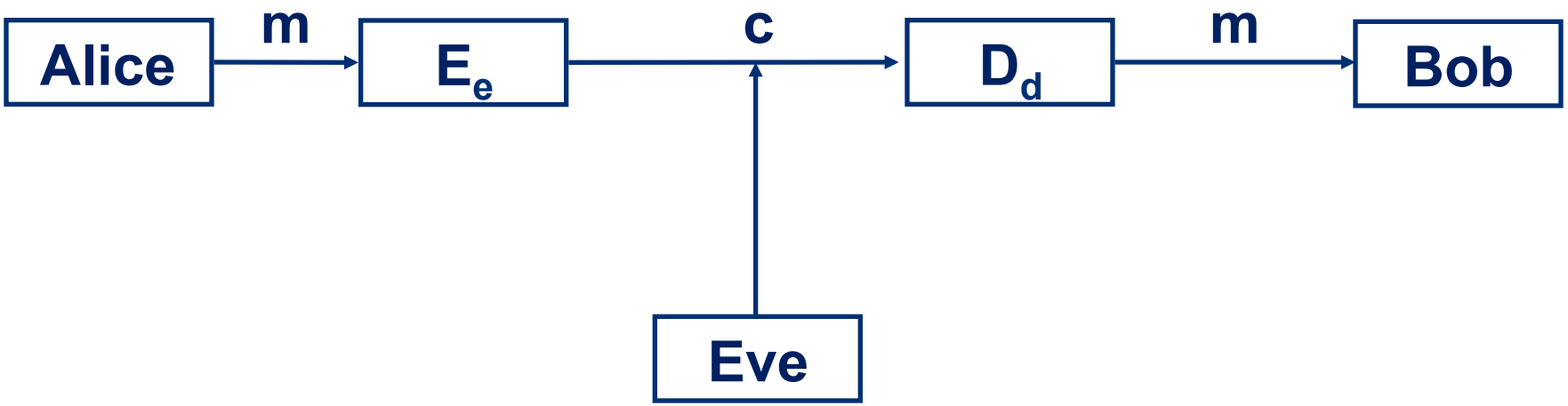
Definition 2.1 Ein Verschlüsselungsverfahren ist ein 5-Tupel (P,C,K,E,D), wobei

1. P die Menge der Klartexte ist.
2. C die Menge der Chiffretexte ist.
3. K die Menge der Schlüssel ist.
4. $E=\{E_k : k \in K\}$ eine Menge von Verschlüsselungsfunktionen $E_k : P \to C$ ist.
5. $D=\{D_k : k \in K\}$ eine Menge von Entschlüsselungsfunktionen $D_k : C \to P$ ist.
6. Zu jedem $e \in K$ existiert ein $d \in K$, so dass für alle $m \in P$

$$D_d(E_e(m)) = m.$$

Schlüssel e,d mit dieser Eigenschaft heißen **Schlüsselpaare**.

Schema Verschlüsselung



$m :=$ Klartext

$c :=$ Chiffretext

$e,d \in K$ mit $D_d(E_e(m)) = m$

Caesar-Chiffre

$P = C = \{a, b, \ldots, z\} \triangleq \{0, 1, \ldots, 25\}.$

$K = \{0, 1, \ldots, 25\}$

$$E_e : \{0, 1, \ldots, 25\} \rightarrow \{0, 1, \ldots, 25\}$$
$$x \mapsto x + e \bmod 26$$

$$D_d : \{0, 1, \ldots, 25\} \rightarrow \{0, 1, \ldots, 25\}$$
$$x \mapsto x - d \bmod 26$$

Schlüsselpaare (e, d): $e = d$.

One-time-pad (OTP)

$P = C = K = \{0,1\}^n, n \in \mathbb{N}.$

$$E_e: \quad \{0,1\}^n \quad \to \quad \{0,1\}^n$$
$$x = x_1 \dots x_n \quad \mapsto \quad x_1 \oplus e_1 \dots x_n \oplus e_n, \quad e = e_1 \dots e_n$$

$$D_d: \quad \{0,1\}^n \quad \to \quad \{0,1\}^n$$
$$x = x_1 \dots x_n \quad \mapsto \quad x_1 \oplus d_1 \dots x_n \oplus d_n$$

Schlüsselpaare (e,d): $e = d$.

Permutations-Chiffre

$P = C = \Sigma^n, n \in \mathbb{N}, |\Sigma| < \infty;$

$K = S_n :=$ Menge der Permutationen auf $\{1,\ldots,n\}$.

$$E_\pi : \quad \Sigma^n \quad \to \quad \Sigma^n$$

$$s_1 \ldots s_n \quad \mapsto \quad s_{\pi(1)} \ldots s_{\pi(n)};$$

$$D_\pi : \quad \Sigma^n \quad \to \quad \Sigma^n$$

$$s_1 \ldots s_n \quad \mapsto \quad s_{\pi(1)} \ldots s_{\pi(n)};$$

Schlüsselpaare $(e,d) : e = \pi, d = \pi^{-1}$

Hill-Chiffre

$m,n \in \mathbb{N}$, $P = C = \mathbb{Z}_m^n$; wobei $\mathbb{Z}_m := \mathbb{Z}/(m\mathbb{Z})$

$$K = \left\{ A \in \mathbb{Z}_m^{n\times n} : ggT\left(\det(A), m\right) = 1 \right\}.$$

$$E_A : \mathbb{Z}_m^n \to \mathbb{Z}_m^n, v \mapsto A \cdot v \mod m;$$

$$D_A : \mathbb{Z}_m^n \to \mathbb{Z}_m^n, v \mapsto A \cdot v \mod m.$$

$$A \in \mathbb{Z}_m^{n\times n}, \operatorname{adj}(A) := \left(c_{ij}\right)_{1\le i,j\le n} \text{ mit } c_{ij} = (-1)^{i+j} \det\left(A_{ji}\right)$$

A_{ji} := A ohne j-te Zeile, i-te Spalte

$$A' := \det(A)^{-1} \cdot \operatorname{adj}(A)$$

Satz 2.2 Es gilt $A'A = AA' = I_n \mod m$.

Schlüsselpaare (e,d): $e = A, d = A'$.

Lange Nachrichten

(P,C,K,E,D) Verschlüselungsverfahren.

Erweiterung auf P^* durch

$$E_e(a_1,\ldots,a_l) = E_e(a_1)\ldots E_e(a_l).$$

(Electronic Codebook Modus)

II.2 Symmetrische & asymmetrische Verfahren

auch Private-Key-Verfahren & Public-Key-Verfahren

Gilt für $e,d \in K$, dass $D_d(E_e(m)) = m$ für alle $m \in P$, so heißt (e,d) ein Schlüsselpaar.

Symmetrische Verfahren Für alle Schlüsselpaare (e,d)

- **e = d oder**
- **d kann aus e leicht berechnet werden.**

Asymmetrische Verfahren Für alle Schlüsselpaare (e,d)

- **d kann aus e nicht mit vertretbarem Aufwand berechnet werden.**

Konsequenzen

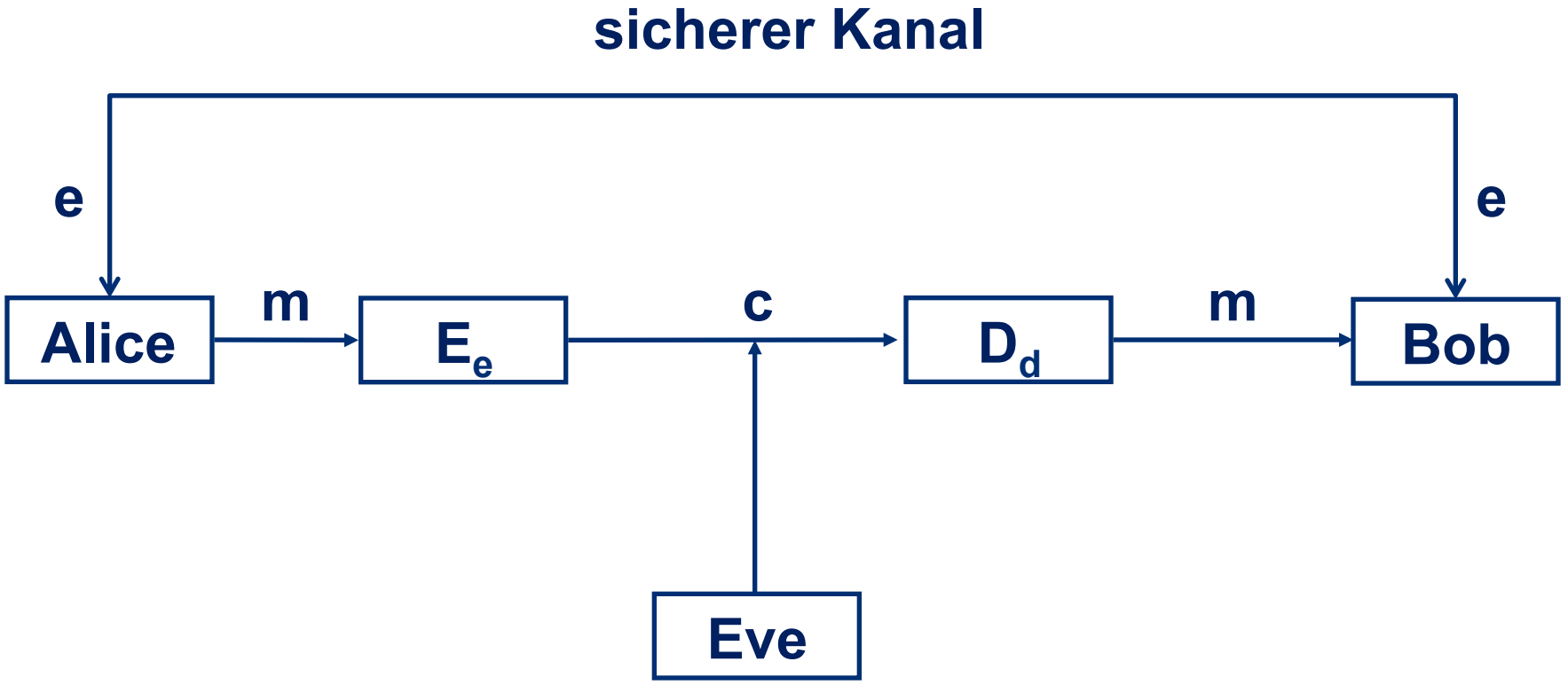
Symmetrische Verfahren

- e muss über sicheren Kanal ausgetauscht werden.
- e muss geheim gehalten werden.

Asymmetrische Verfahren

- e kann öffentlich sein.
- Kommunikation von A zu B benötigt anderes Schlüsselpaar als Kommunikation von B zu A.
- e heißt öffentlicher Schlüssel (public key).
- d heißt geheimer oder privater Schlüssel (private key).
- e und d häufig leicht unterschiedliches Format, aber Anpassung von Definition 2.1 (unwesentlich).

Symmetrische Verschlüsselung



II.3 Sicherheit von Verschlüsselung

Kerckhoffs Prinzip **Die Sicherheit eines symmetrischen Verschlüsselungsverfahrens darf nur auf der Geheimhaltung des Schlüssels beruhen und nicht auf der Geheimhaltung des Verfahrens selber.**

Sicherheit

Analyse der Sicherheit eines Verfahrens benötigt Wissen über

- **Ziele eines Angreifers**
- **Möglichkeiten eines Angreifers**

Ziele eines Angreifers

- **Berechnung des Schlüssels e**
- **Berechnung eines Klartextes m aus einem Chiffretext c**
- **Berechnung spezieller Informationen über m aus c**

Möglichkeiten eines Angreifers

- **Ciphertext-Only Angriff** Angreifer kennt nur Chiffretext c.
- **Known-Plaintext Angriff** Angreifer kennt Chiffretext c und Paare (m_i,c_i) von Klartexten und Chiffretexten unter dem gleichen Schlüssel e.
- **Chosen-Plaintext Angriff** Angreifer kann sich zu selbst gewählten Klartexten m_i die Chiffretexte c_i erzeugen lassen.
- **Chosen-Ciphertext Angriff** Angreifer kann sich zu selbst gewählten Chiffretexten c_i die Klartexte m_i erzeugen lassen.

Sicherheit

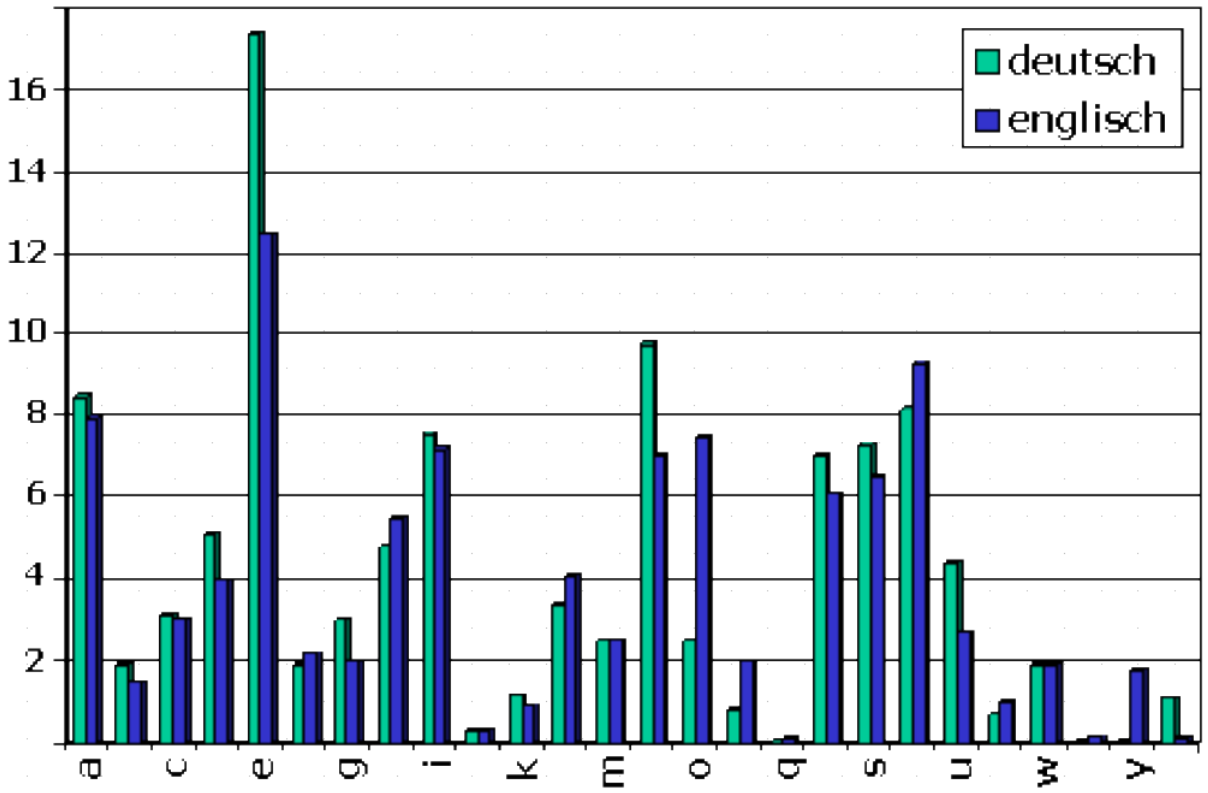
One-Time-Pad

- sicher gegen Ciphertext-Only-Angriffe
  (perfekte Geheimhaltung)
- nicht sicher gegen Known-Plaintext-Angriffe

Caesar-Chiffre

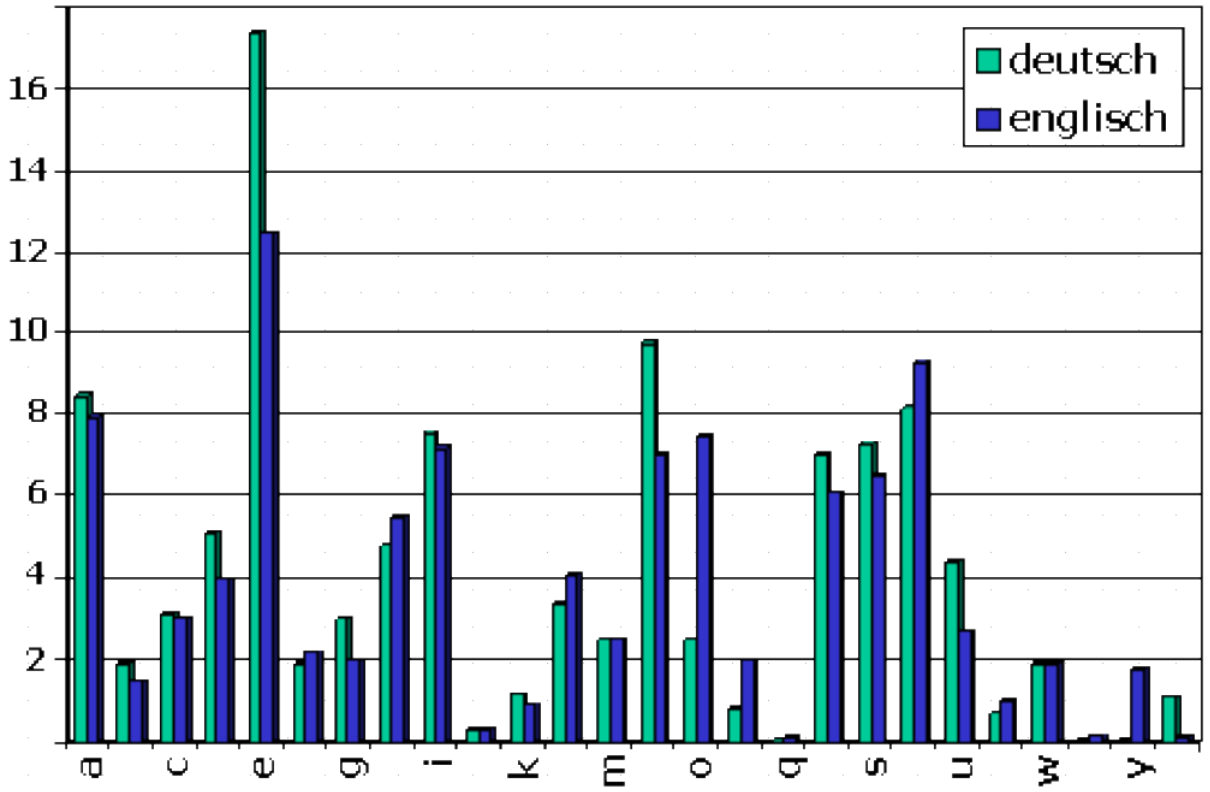
- bei langen Nachrichten nicht sicher gegen
  Ciphertext-Only-Angriffe

Buchstabenverteilung



Angriff auf Caesar-Chiffre

„f ltti lqfxx ns ymj gnxmtux mtxyjq ns ymj ijanqx xjfy“



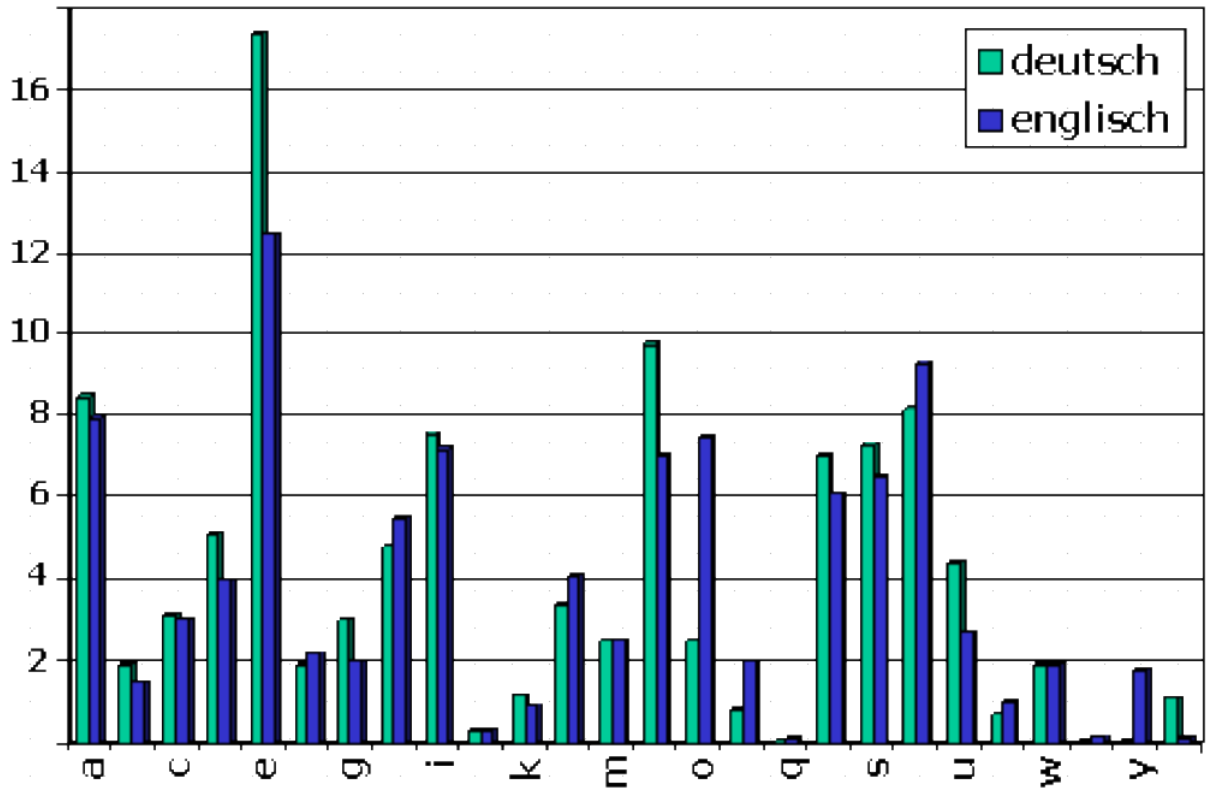
e wurde x und k=19?

e entspricht 4
x entspricht 23

„ m saap sxmee uz ftq nuetabe taefqx uz ftq pqhuxe eqmf“???

Angriff auf Caesar-Chiffre

„f ltti lqfxx ns ymj gnxmtux mtxyjq ns ymj ijanqx xjfy“



e wurde j und k=5?

e entspricht 4
j entspricht 9

„ a good glass in the bishops hostel in the devils seat “
(E.A. Poe)

Möglichkeiten eines Angreifers

- **Ciphertext-Only Angriff** Angreifer kennt nur Chiffretext c.
- **Known-Plaintext Angriff** Angreifer kennt Chiffretext c und Paare (m_i,c_i) von Klartexten und Chiffretexten unter dem gleichen Schlüssel e.
- **Chosen-Plaintext Angriff** Angreifer kann sich zu selbst gewählten Klartexten m_i die Chiffretexte c_i erzeugen lassen.
- **Chosen-Ciphertext Angriff** Angreifer kann sich zu selbst gewählten Chiffretexten c_i die Klartexte m_i erzeugen lassen.

Sicherheit

Asymmetrische Verfahren

- erlauben immer Chosen-Plaintext-Angriffe, da öffentlicher Schlüssel bekannt

Ununterscheidbare Verschlüsselungen

- Chiffretexte verraten keine Informationen über Klartexte bei Chosen-Ciphertext-Angriffen

II.4 Blockchiffren

Ziel Verschlüsselungsverfahren mit $P = \Sigma^*, |\Sigma| < \infty$, d.h.

Verfahren für Nachrichten beliebiger Länge.

Vorgehen

1. Verfahren für $P = \Sigma^n, n \in \mathbb{N}$ fest.
2. Aus diesem Verfahren Verschlüsselungsverfahren für $P = \Sigma^*$.

Definition 2.3 Ein Veschlüsselungsverfahren mit $P = C = \Sigma^n$, $n \in \mathbb{N}$ fest, heißt Blockchiffre. n heißt die Blocklänge.

Im Fall $n = 1$ heißt das Verschlüsselungsverfahren eine Substitutions-Chiffre.

Blockchiffren - Beispiele

Beispiel 1 Caesar-Chiffre ist eine Substitutions-Chiffre.

Beispiel 2 OTP mit $P = C = \{0,1\}^n$ ist Blockchiffre mit Blocklänge n.

Beispiel 3 (Vigenère-Chiffre) $m,n \in \mathbb{N}$, $P = C = K = \mathbb{Z}_m^n$.

$E_k : \mathbb{Z}_m^n \to \mathbb{Z}_m^n, v \mapsto v + k \mod m;$

$D_k : \mathbb{Z}_m^n \to \mathbb{Z}_m^n, v \mapsto v - k \mod m$

Blockchiffren - Beispiele

Beispiel 4 (Permutations-Chiffre) $n \in \mathbb{N}, |\Sigma| < \infty$;

$K = S_n :=$ Menge der Permutationen auf $\{1,\ldots,n\}$.

$E_\pi : \Sigma^n \to \Sigma^n, s_1 \ldots s_n \mapsto s_{\pi(1)} \ldots s_{\pi(n)}$;

$D_\pi : \Sigma^n \to \Sigma^n, s_1 \ldots s_n \mapsto s_{\pi(1)} \ldots s_{\pi(n)}$.

Schlüsselpaare $(e,d) : e = \pi, d = \pi^{-1}$

Blockchiffren - Beispiele

Beispiel 5 (Hill-Chiffre) $m,n \in \mathbb{N}$, $P = C = \mathbb{Z}_m^n$;

$$K = \left\{ A \in \mathbb{Z}_m^{n\times n} : ggT\left(\det(A), m\right) = 1 \right\}.$$

$$E_A : \mathbb{Z}_m^n \to \mathbb{Z}_m^n, v \mapsto A \cdot v \mod m;$$

$$D_A : \mathbb{Z}_m^n \to \mathbb{Z}_m^n, v \mapsto A' \cdot v \mod m.$$

$$A \in \mathbb{Z}_m^{n\times n}, \operatorname{adj}(A) := \left(c_{ij}\right)_{1\le i,j\le n} \text{ mit } c_{ij} = (-1)^{i+j} \det\left(A_{ji}\right)$$

$$A' := \det(A)^{-1} \cdot \operatorname{adj}(A)$$

Satz 2.2 Es gilt $A'A = AA' = I_n \mod m$.

Blockchiffren - Beispiele

Beispiel 6 (Affine-Chiffre) $m,n \in \mathbb{N}$, $P = C = \mathbb{Z}_m^n$;

$$K = \left\{ (A,b) \in \mathbb{Z}_m^{n\times n} \times \mathbb{Z}_m^n : ggT\left(\det(A), m\right) = 1 \right\}.$$

$$E_{(A,b)} : \mathbb{Z}_m^n \to \mathbb{Z}_m^n,$$

$$v \mapsto A \cdot v + b \bmod m;$$

$$D_{(A,b)} : \mathbb{Z}_m^n \to \mathbb{Z}_m^n,$$

$$v \mapsto A \cdot v + b \bmod m.$$

Schlüsselpaare $(e,d) : e = (A,b), d = \left(A^{-1}, -A^{-1} \cdot b\right)$

Blockchiffren

Satz 2.4 Die Verschlüsselungsfunktionen einer Blockchiffre mit $P = C = \Sigma^n$ sind Bijektionen auf Σ^n.

II.5 Verschlüsselungsmodi

Ziel Verschlüsselungsverfahren mit $P = \Sigma^*, |\Sigma| < \infty$, d.h., Verfahren für Nachrichten beliebiger Länge (über Σ).

Vorgehen

1. Verfahren für $P = \Sigma^n, n \in \mathbb{N}$ fest (Blockchiffre).
2. Aus dieser Blockchiffre Verschlüsselungsverfahren für $P = \Sigma^*$.

Zunächst 2. und $\Sigma = \{0,1\}$.

Beispiel

(P,C,K,E,D) Blockchiffre mit $P = C = \Sigma^n$.

ECB-Modus (electronic codebook mode) bei $m \in \Sigma^*$ und $e \in K$.

1. Ergänze m, so dass die Länge von m ein Vielfaches von n ist. Setze $m = m_1 m_2 \ldots m_l$ mit $m_i \in \Sigma^n$.
2. Berechne $c = E_e(m_1)E_e(m_2)\ldots E_e(m_l)$.

Im Allgemeinen nicht sicher – Caesar-Chiffre!

4 Modi

Verschlüsselungsmodi

1. Electronic Code Book Modus (ECB)
2. Cipher Block Chaining Modus (CBC)
3. Output Feedback Modus (OFB)
4. Cipher Feedback Modus (CFB)

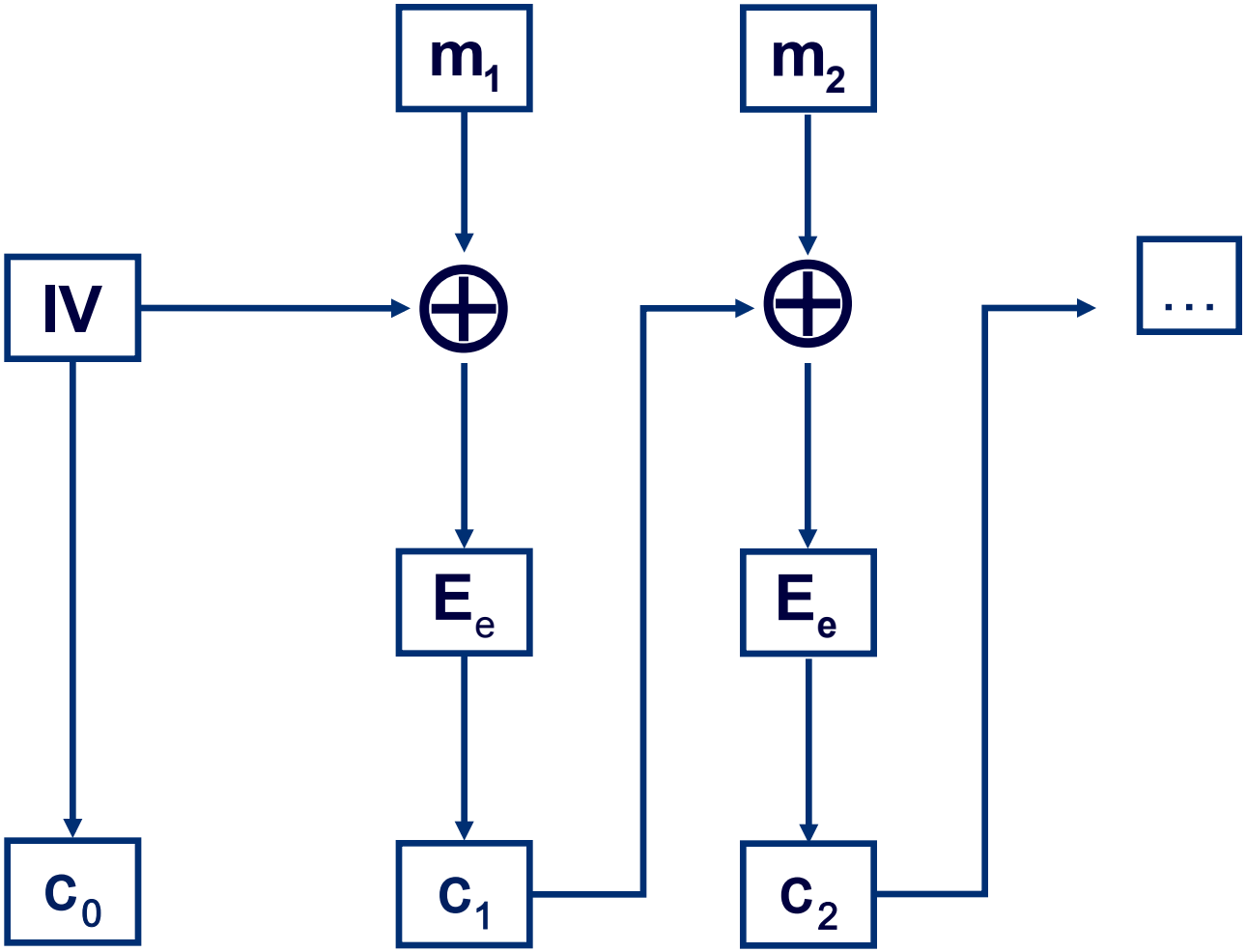
4 Modi

- (P,E,DE,D) Blockchiffre mit $P = C = \{0,1\}^n$.
- Nachricht $m = m_1 m_2 \ldots m_l, m_i \in \{0,1\}^n$.
- Initialisierungsvektor $IV \in \{0,1\}^n$.

1. ECB-Modus $c_i := E_e(m_i)$.
2. CBC-Modus $c_0 := IV, c_i := E_e(c_{i-1} \oplus m_i), i \geq 1$.
3. OFB-Modus $c_0 = z_0 := IV, z_i := E_e(z_{i-1}), c_i := z_i \oplus m_i, i \geq 1$.
4. CFB-Modus $c_0 := IV, c_i := E_e(c_{i-1}) \oplus m_i, i \geq 1$.

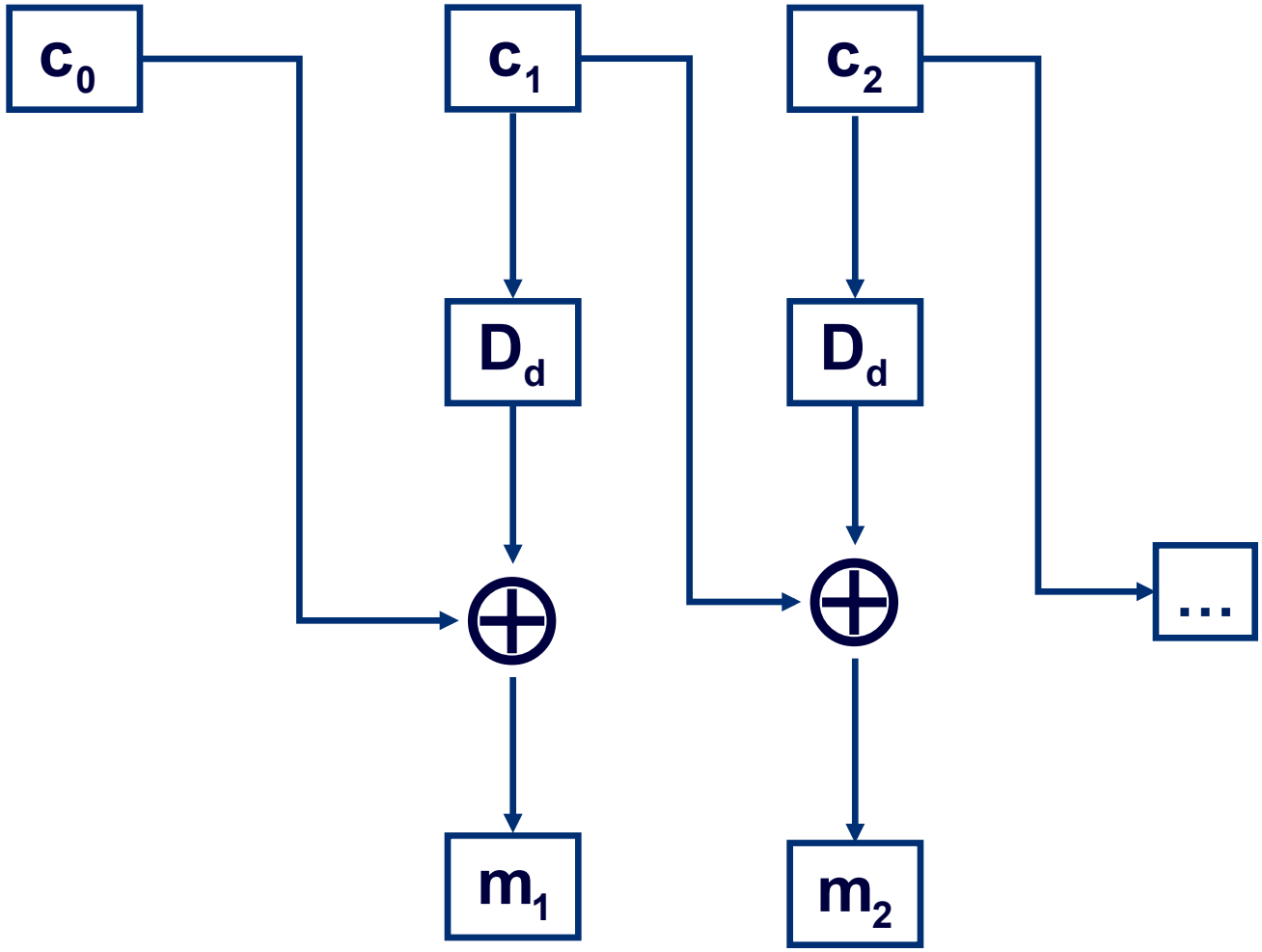
- Chiffretext jeweils $c_0 c_1 \ldots c_l$.

CBC - Verschlüsselung



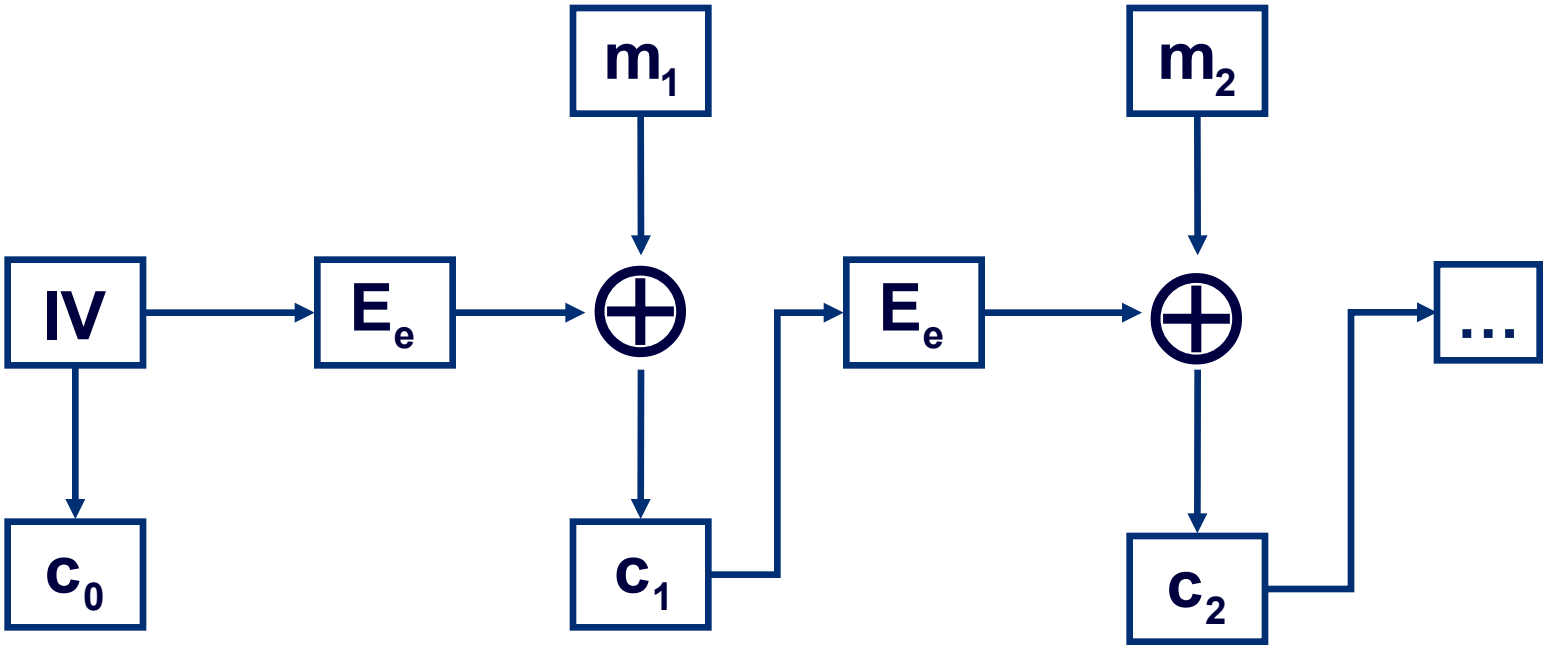
2. CBC-Modus $c_0 := IV, c_i := E_e(c_{i-1} \oplus m_i), i \geq 1.$

CBC - Entschlüsselung



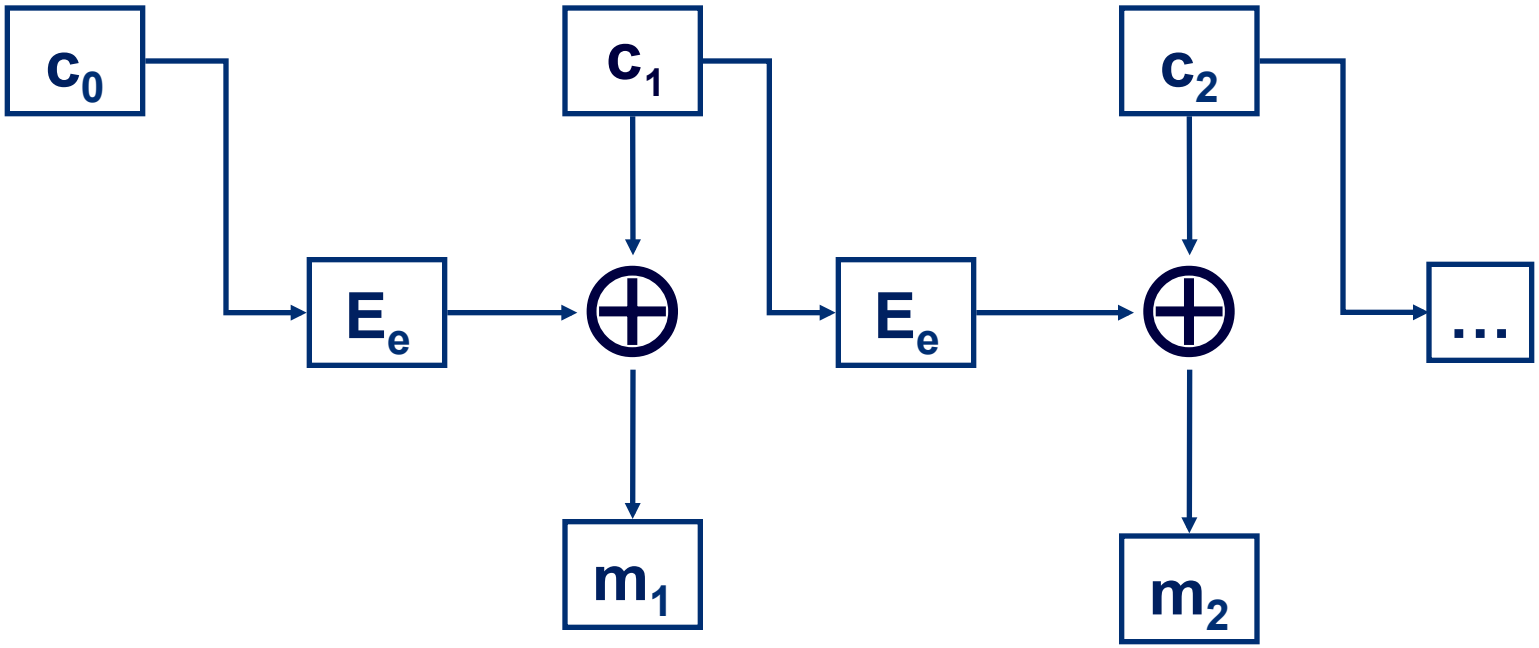
CBC-Entschlüsselung $c_0 = IV, m_i = D_d(c_i) \oplus c_{i-1}$

CFB - Verschlüsselung



4. CFB-Modus $c_0 := IV, c_i := E_e(c_{i-1}) \oplus m_i, i \geq 1.$

CFB - Entschlüsselung



CFB-Entschlüsselung $c_0 = IV, m_i = E_e(c_{i-1}) \oplus c_i$

II.5 Sichere Blockchiffren

- sichere Blockchiffren schwer zu konstruieren
- viele Vorschläge schnell gebrochen
- alle bisherigen Beispiele der Vorlesung sind in vielen Angriffsszenarien unsicher
- Konstruktion muss auf einigen allgemein anerkannten Prinzipien beruhen

Prinzipien

1. Kerckhoffs Prinzip
2. Schlüsselraum muss groß sein.
3. Konfusion muss groß sein.
4. Diffusion muss groß sein.
5. Muss sicher gegen bekannte Angriffe sein.

Konfusion und Diffusion

Konfusion Die Konfusion einer Blockchiffre ist groß, wenn die statistische Verteilung der Chiffretexte in so komplizierter Weise von der Verteilung der Klartexte abhängt, dass ein Angreifer diese Abhängigkeiten nicht ausnutzen kann.

Diffusion Die Diffusion einer Blockchiffre ist groß, wenn jedes Bit des Klartextes und jedes Bit des Schlüssels möglichst viele Bits des Chiffretexts beeinflusst.

(Claude Shannon, 1949)

Angriffsmethoden

1. erschöpfende Suche
2. lineare Kryptanalyse
3. differentielle Kryptanalyse
4. algebraische Kryptanalyse

Affin lineare Verfahren (Hill-Chiffre, Permutation-Chiffre)

- haben geringe Konfusion
- können durch lineare Kryptanalyse leicht gebrochen werden.