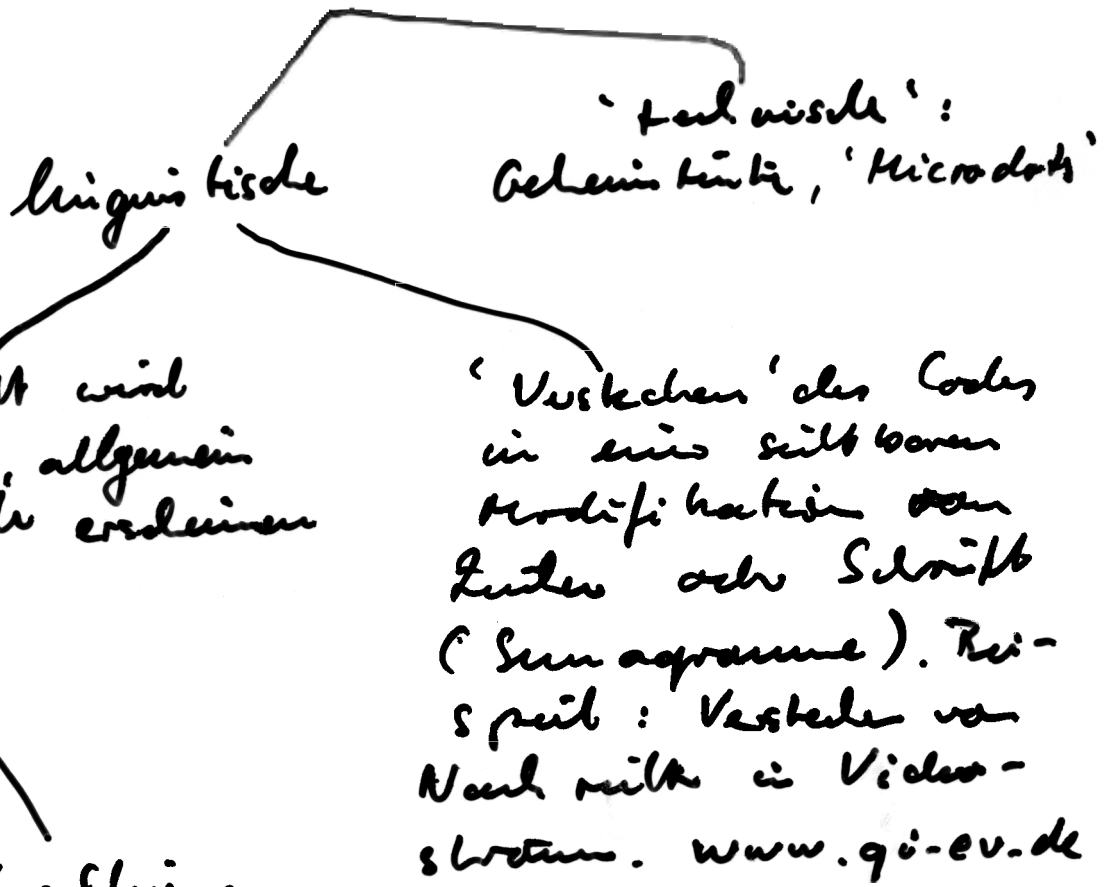
Kryptographie

macht eine Nachricht für Unbefugte unlesbar

Kryptanalyse macht versucht, solche Nachrichten zu entschlüsseln

Steganographie zielt darauf ab, die Existenz einer Nachricht (auf/über ein Medium) zu verbergen. Man unterscheidet



Im folgenden nur Betrachtung der Kryptographie

Definitionen:

- Verschlüsselung ist durch Schlüssel parametrisierte Codierung
- Sicherheit: Ein Verfahren kann (mit unterschiedlichem Schlüssel) nicht eindeutig verwendet werden.

M: Klartext zeichenvorrat, M^*: Klartextraum ('plain text')
C: Geheimtext zeichenvorrat, C^*: Geheimtextraum ('cipher text')

K: Schlüsselmenge. Jedes Element $e \in K$ bezeichnet einen Schlüssel, der zu einer Transformation $E_e: M^* \to C^*$ führt.

ist die Chriffrierstransformation. E_e muß eine bijektive Funktion (Bijektion) sein, wenn aus jedem Geheimtext eindeutig der Klartext wiederum ableitbar sein soll.

Spezielle Bijektion: Permutation einer Menge M mit n Elementen. Funktion $p: M \to M$

Beispiel: $M = \{1, 2, 3, 4, 5\}$. Dann ist eine Permutation z.B.

$p(1) = 3$, $p(2) = 5$, $p(3) = 4$, $p(4) = 2$, $p(5) = 1$

- Verschlüsselungsverfahren ('encryption scheme')
  $(M^*, C^*, K, \{E_e\}, \{D_d\})$ mit der Menge der

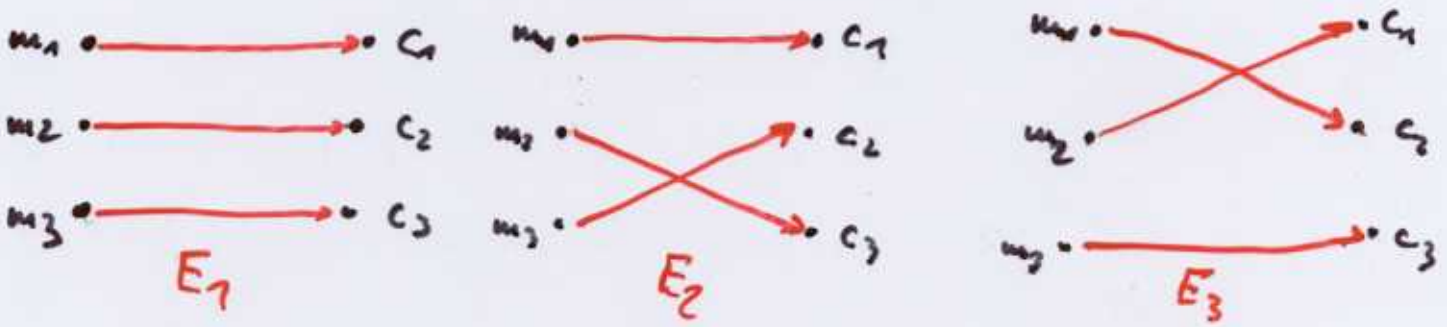
Verschlüsselungstransformation $\{E_e\}$ und der der Entschlüsselungstransformation $\{D_d\}$. $d, e \in K$

Bemerkung: Im Prinzip können E und D auch fest sein, aber unpraktisch (s.o.)

Beispiel für E:

Sei $M = \{m_1, m_2, m_3\}$, $C = \{c_1, c_2, c_3\}$

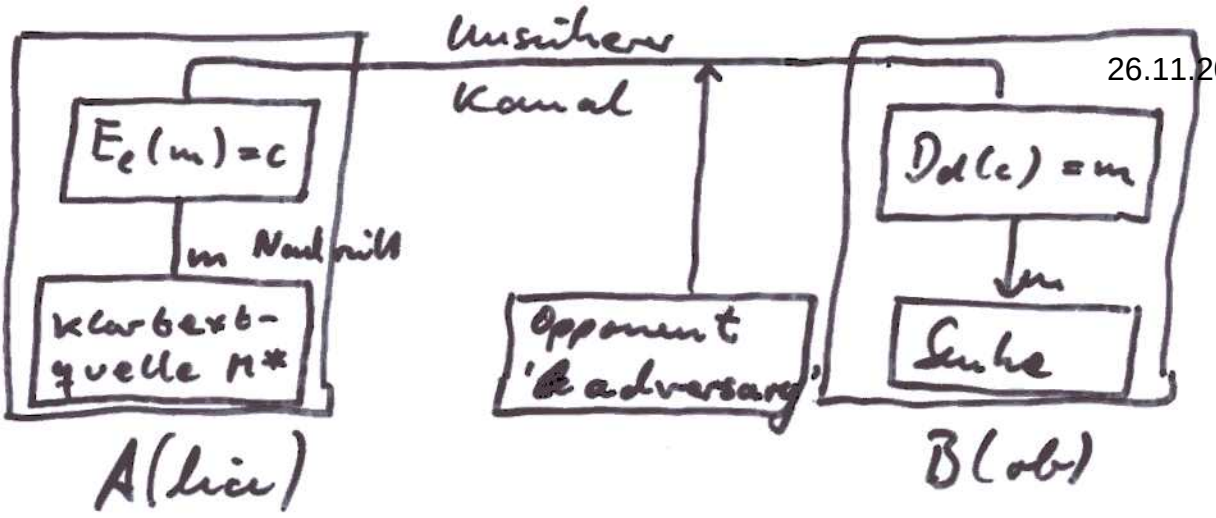
Dann gibt es 3! Bijektionen $E_{1\ldots6} : M \to C$, die durch einen Schlüssel aus der Menge $K = \{1, 2, \ldots, 6\}$ ausgewählt werden können.



analog für $E_4 \ldots E_6$

$E_3(m_1) = c_2$
$E_3(m_2) = c_1$
$E_3(m_3) = c_3$

Damit Darstellung von Kommunikation über unsichere Kanäle



⇒ B guten Verfahren ist alles bekannt, außer dem Schlüsselpaar e

Gemeint sind unterschiedliche Verfahren zur Chiffrierung, einfach

mono alphabetische Chiffrierung

Def.: Sei A ein Alphabet von q Symbolen und M die Menge aller Wörter mit ℓ Symbolen aus A. Die Menge K (Schlüsselmenge) sei die Menge aller Permutationen über A. Definiere $e \in K$ eine Transformation E_e. Dann ist die Verschlüsselung vorschrift

$$E_e(m) = (e(m_1) \; e(m_2) \; \ldots \; e(m_\ell)) = c_1 c_2 \ldots c_\ell = c$$

mit $d = e^{-1}$ (inverse Permutation) mit

$$m = D_d(c) = (d(c_1) \; d(c_2) \; \ldots \; d(c_\ell))$$

Beispiel:

a) Verschiebung des Alphabets um k Zeichen

	gallia	est	omnis	divisa
+3	jdoold	hvw	rpqlv	glylvd

b) 'ROT-13': Verschiebung um 13 Buchstaben (Alphabet-äquivalent, involutorisch). Verwendung z.B. in news-groups, um kontinuierlich Textpassagen nicht unmittelbar freizugeben

⇝ Kryptanalyse durch Frequenzbestimmung der Zeichen im Geheimtext

Weitere Verfahren

a) Code-Wort-Methode Addition eines CW modulo (card(M))

	gallia	est	omnis	divisa
⊕	cleopa	t rac	l e opat	r a cleop
	JHQLYB		TACJL	RELGNGQ

Krypt analyse (a) Länge des CW ermitteln
(b) Frequenz analyse für jedes n-te Zeichen

b) Statt Kennung CW wird (zuvor auf) bekannten Text verwendet

als zarathustra
⊕ in principio erat

JZSP QJUJIQISYIBT

c) Vernam - Chiffrierung. Bis heute das einzige unbrechbare und praktisch durchführbare Verschlüsselungsverfahren

- Zufallstext, der mindestens genauso lang ist wie der Klartext → Notwendigkeit absolut 'zufälliger' Zufallszahlengeneratoren
- Sender und Empfänger verwenden diesen Schlüssel nur einmal.

Elementarer Beweis der Unbrechbarkeit:

Zu jeder möglichen Interpretation des Klartextes gibt es einen Schlüssel, der den gegebenen Geheimtext erzeugt.

Beispiel Geheimtext

JZSPQJUJIQISYIBTDM

+ Schlüssel: cezkcjhvrjdeyaxbmm

'guten morgen herr x'

+ Schlüssel: ilwmiytcipomyjtosm

'anschlag auf ziel a'