Kryptographie

Vorlesung 1: Einführung

Babeş-Bolyai Universität, Department für Informatik, Cluj-Napoca
csacarea@cs.ubbcluj.ro

Organisatorisches

Literatur

- J. Buchmann, Einführung in die Kryptographie
- A. Menezes, P. Oorschot, S. Vanstone, Handbook of Applied Cryptography
- S. Goldwasser, M. Bellare, Lecture Notes on Cryptography, MIT, online, 19962008
- O. Goldreich, Foundations of Cryptography Volume 1 (Basic Tools), Cambridge University Press, 2001
- O. Goldreich, Foundations of Cryptography Volume 2 (Basic Applications), Cambridge University Press, 2004

Sprechstunden

Nach Vereinbarung

Agenda

- Einführung
- Klassische Kryptoverfahren
- Angriffe und Kryptanalysis
- Elektromechanische Verfahren (Enigma)
- Moderne Kryptographie

Wozu Kryptosysteme?

Sichere Übertragung geheimer Botschaften

- Übertragungskanäle sind oft unsicher
  - Nachricht könnte evtl. abgehört werden
  - Originaltext zu übertragen ist unsicher
- Verschlüsselung macht Botschaft unlesbar
  - Unbefugte sollen abgehörte Nachricht nicht entschlüsseln können
  - Zieladressat muss Originaltext leicht wiederherstellen können

KRYPTOVERFAHREN

- Vertraulichkeit: Nachricht kann von Dritten nicht gelesen werden; Geheimhaltung, Anonymität (z.B. im Internet), Unbeobachtbarkeit (von Transaktionen)
- Integrität: von Nachrichten und Daten; Fälschung/Manipulation der Nachricht ist nicht möglich
- Zurechenbarkeit: Authentikation, Unabstreitbarkeit, Identifizierung; Nachweis, dass Nachricht vom angegebenen Sender stammt
- Verfügbarkeit: von Daten, von Rechenressourcen, von Informationsdienstleistungen.
- Verbindlichkeit: Sender kann Urheberschaft nicht nachträglich leugnen

Wichtige Begriffe

- Kryptographie: Lehre von der Geheimhaltung von Informationen durch die Verschlüsselung von Daten. Im weiteren Sinne: Wissenschaft von der Übermittlung, Speicherung und Verarbeitung von Daten in einer von potentiellen Gegnern bedrohten Umgebung.
- Kryptoanalysis: Erforschung der Methoden eines unbefugten Angriffs gegen ein Kryptoverfahren (Zweck: Vereitelung der mit seinem Einsatz verfolgten Ziele)
- Kryptoanalyse: Analyse eines Kryptoverfahrens zum Zweck der Bewertung seiner kryptographischen Stärken bzw. Schwächen.
- Kryptologie: Wissenschaft vom Entwurf, der Anwendung und der Analyse von kryptographischen Verfahren (umfasst Kryptographie und Kryptoanalyse).

Wichtige Begriffe

Kryptosysteme $\neq$ Codesysteme!!!

Kryptosysteme

Ein Kryptosystem Π wird durch folgende Komponenten beschrieben:

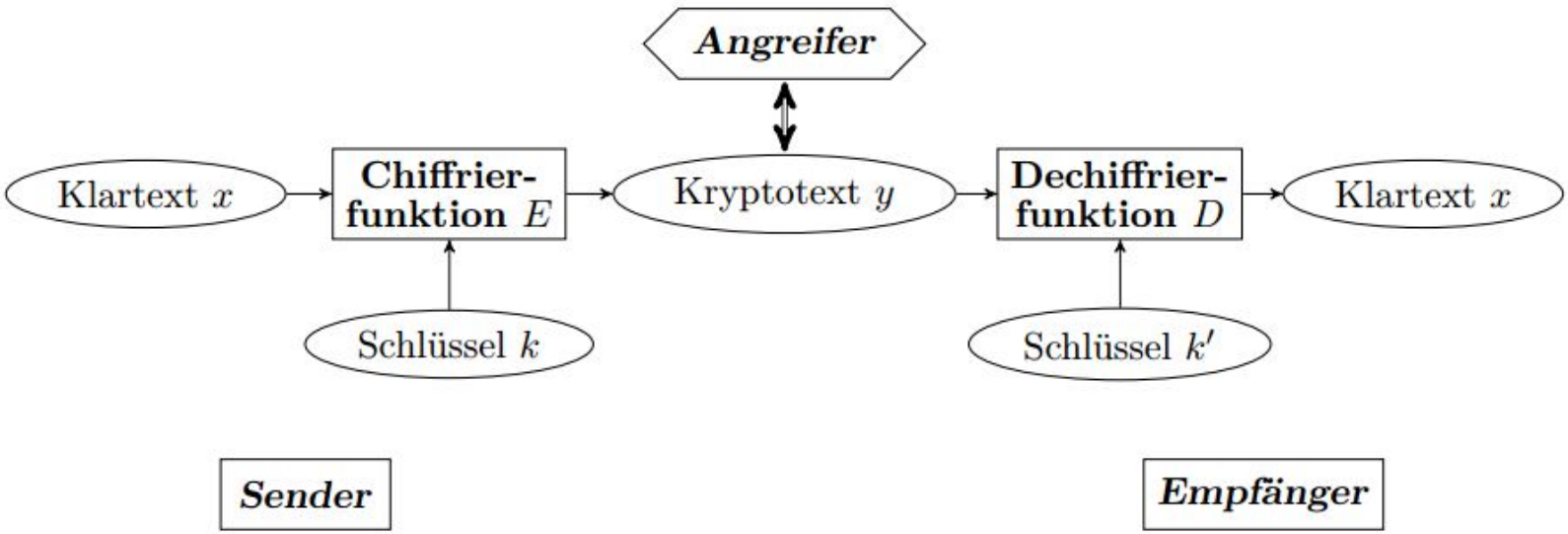
- A, das Klartextalphabet, B, das Kryptotextalphabet,
- K, der Schlüsselraum (key space),
  - Schlüsselgenerator `Gen`
- $M \subseteq A$, der Klartextraum (message space),
- $C \subseteq B$, der Kryptotextraum (ciphertext space),
- $E\colon K \times M \to C$, die Verschlüsselungsfunktion (encryption function), `Enc`,
- $D\colon K \times C \to M$, die Entschlüsselungsfunktion (decryption function), `Dec` und
- $S \subseteq K \times K$, eine Menge von Schlüsselpaaren (k, k') mit der Eigenschaft, dass für jeden Klartext $x \in M$ folgende Beziehung gilt:

$$D(k', E(k, x)) = x.$$

KRYPTOSYSTEME

- Symmetrische Kryptosysteme: $S = \{(k, k) \mid k \in K\}$,
- Jeder Schlüssel $k \in K$ generiert eine Chiffrierfunktion $E_k : x \mapsto E(k, x)$ und eine Dechiffrierfunktion $D_k : y \mapsto D(k, y) \rightarrow$ Schlüssel als Parameter!
- Die Gesamtheit dieser Abbildungen wird auch Chiffre (englisch cipher) genannt. (Daneben wird der Begriff *Chiffre* auch als Bezeichnung für einzelne Kryptotextzeichen oder kleinere Kryptotextsequenzen verwendet.)

KRYPTOSYSTEM



Kerckhoffs Prinzip (1883)

Forderung Kerckhoffs Prinzip

Die Sicherheit eines Verschlüsselungsverfahrens Π darf ausschließlich auf der Geheimhaltung des Schlüssels beruhen. D.h. alle Ingredienten $A, K, \texttt{Gen}, M, C, E, D$ sind bekannt. Die Schlüssel sind aber nicht bekannt!

Anmerkungen:

- Schlüssel lassen sich besser geheimhalten als Algorithmen.
- Schlüssel lassen sich besser austauschen als Algorithmen.
- Schlüssel lassen sich besser verwalten als Algorithmen.
- Öffentliche Untersuchung von Π durch Experten ist erforderlich.

Klassifizierung der Verschlüsselungsverfahren

1. Substitution: Zeichen aus dem Klartextalphabet werden mit Zeichen aus einem (eventuell verschiedenes) Cyphertextalphabet ersetzt.
2. Transposition: Klartext- und Cyphertextalphabet sind gleich. Zeichen behalten ihre Bedeutung, ändern aber ihre Position im Text.

Diese Begriffe sind nicht streng voneinander getrennt, da jede Substitution auch eine Transposition ist und andersrum! (Weshalb?)

Klassifizierung der Verschlüsselungsverfahren

1. Monoalphabetisch: Ein einziges Alphabet wird für die Verschlüsselung verwendet.
2. Polyalphabetisch: Einem Buchstaben, bzw. Zeichen, wird jeweils ein anderer Buchstabe, bzw. Zeichen zugeordnet. Im Gegensatz zur monoalphabetischen Substitution werden für die Zeichen des Klartextes mehrere Geheimtextalphabete verwendet.

Formale Beschreibung der Chiffren

1. Alle klassischen Chiffren lassen sich durch mathematische Funktionen formal beschreiben
2. Wichtig: die Verschlüsselungsfunktion und die Entschlüsselungsfunktion sind beide bijektiv!
3. Es gibt auch Ausnahmen, aber die werden später diskutiert!

Einfache Kryptosysteme

Verschlüsselungen, die *von Hand* durchführbar sind

- Verschiebungschiffre (Shift Cipher): $E(x,k) = x + k \mod n$
  - Zyklische Verschiebung der Buchstaben im Alphabet
- Affin-Lineare Chiffre (Affine Cipher): $E(x,(a,k)) = ax + k \mod n$
  - Sprunghafte Verschiebung durch Verwendung affiner Funktionen
  - Wann ist $E(x,a)$ eine **echte** Verschlüsselungsfunktion, d.h. bijektiv?

Einfache Kryptosysteme

Verschlüsselungen, die *von Hand* durchführbar sind

- Substitutionschiffre (Substitution Cipher)
  - Ersetzung von Buchstaben durch Permutation des Alphabets
- Vigenere Chiffre (Vigenere Cipher)
  - Verschiebung von Buchstabengruppen mit Schlüsselwort

Einfache Kryptosysteme

Verschlüsselungen, die *von Hand* durchführbar sind

- Hill Chiffre (Hill Cipher)
  - Codierung eines Buchstabenblocks durch Linearkombinationen
- Permutationschiffre (Permutation Cipher)
  - Permutiere Elemente von Buchstabengruppen innerhalb des Textes
- Strom Chiffren (Stream Ciphers)
  - Verschiebungschiffren mit ständig wechselnden Schlüsseln

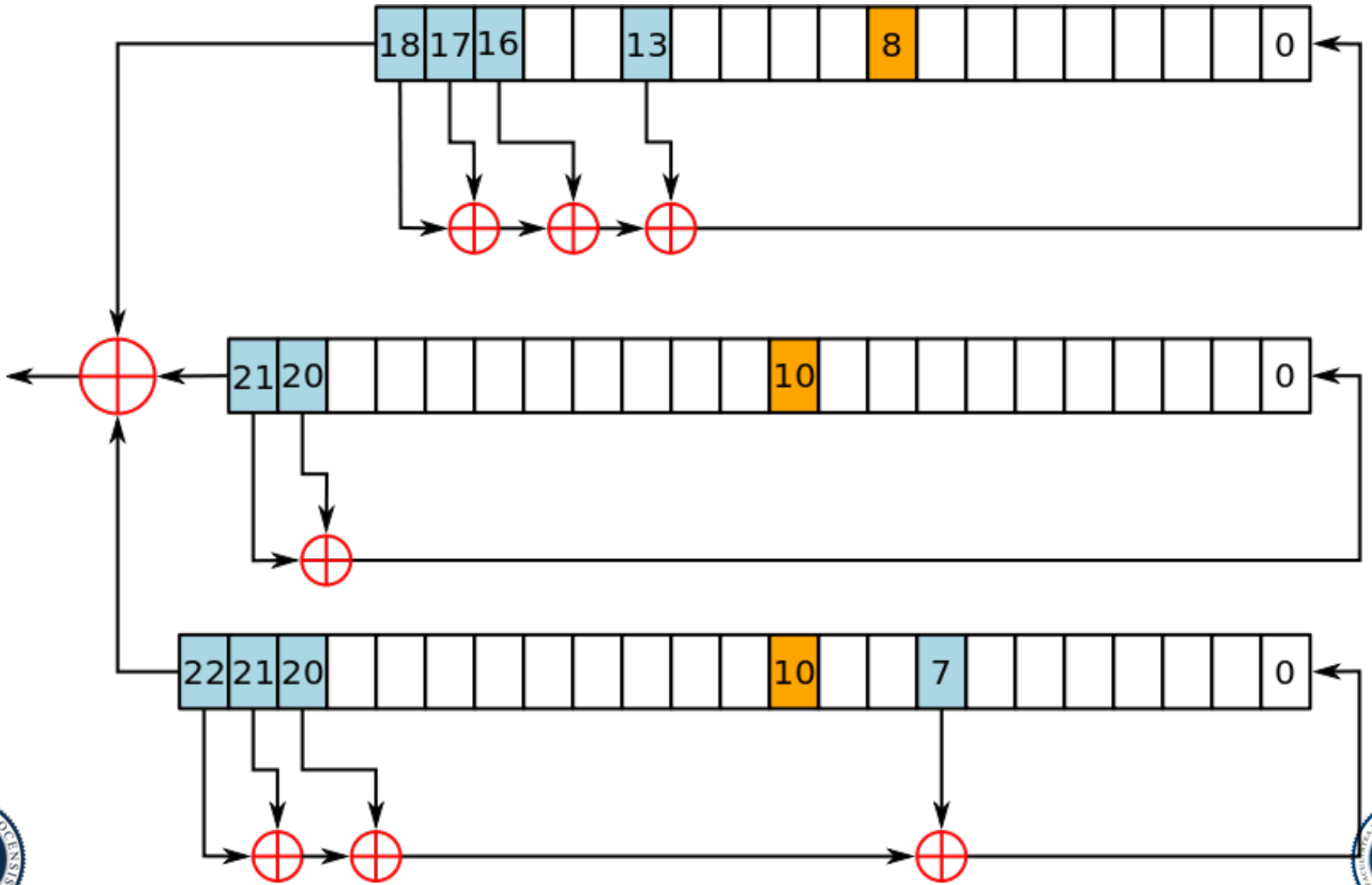
Stromchiffre

- Sei A ein beliebiges Alphabet und sei $M = C = A^l$ für eine natürliche Zahl $l \geq 1$.
- Seien K und $\overline{K}$ Schlüsselräume.
- Eine Stromchiffre wird durch eine Verschlüsselungsfunktion $E\colon \overline{K} \times M \to C$ und einen Schlüsselstromgenerator $g\colon K \times A \to \overline{K}$ beschrieben.
- Der Generator g erzeugt aus einem externen Schlüssel $k \in K$ für einen Klartext $x = x_0 \ldots x_{n-1}, x_i \in M$, eine Folge $\overline{k}_0, \ldots, \overline{k}_{n-1}$ von internen Schlüsseln $\overline{k}_i = g(k, x_0 \ldots x_{i-1}) \in \overline{K}$, unter denen x in den Kryptotext

$$E_g(k, x) = E(\overline{k}_0, x_0) \ldots E(\overline{k}_{n-1}, x_{n-1})$$

überführt wird.

A5/1



Schlüsselstrom Chiffre

- Klartext x ist zu verschlüsseln
- Schlüsselwort $k = k_0 \dots k_{d-1}$ wird so oft wiederholt, bis der dabei entstehende Schlüsselstrom $\overline{k} = k_0, k_1, \dots, k_{d-1}, k_0 \dots$ die Länge von x erreicht.
- Dann werden x und $\overline{k}$ zeichenweise addiert, um den zugehörigen Kryptotext y zu bilden.
- Aus diesem kann der ursprüngliche Klartext x zurückgewonnen werden, indem man den Schlüsselstrom $\overline{k}$ wieder subtrahiert.

- Vigenere
- Beaufort
- Autokey

Vigenere Verschlüsselung

Chiffrierung:

	VIGENERE	(*Klartext* x)
$+$	WIEWIEWI	(*Schlüsselstrom* $\hat{k}$)
	RQKAVINM	(*Kryptotext* y)

Dechiffrierung:

	RQKAVINM	(*Kryptotext* y)
$-$	WIEWIEWI	(*Schlüsselstrom* $\hat{k}$)
	VIGENERE	(*Klartext* x)

Beaufort Verschlüsselung

Chiffrierung:

	WIEWIEWI	(*Schlüsselstrom*)
−	**BEAUFORT**	(*Klartext*)
	XMEQNSNB	(*Kryptotext*)

Dechiffrierung:

	WIEWIEWI	(*Schlüsselstrom*)
−	**XMEQNSNB**	(*Kryptotext*)
	BEAUFORT	(*Klartext*)

AUTOKEY

- Bei Vigenere und Beaufort wird aus einem Schlüsselwort $k = k_0 \dots k_{d-1}$ ein periodischer Schlüsselstrom $\bar{k} = \bar{k}_0 \dots \bar{k}_{n-1}$ erzeugt:
  - Es gilt $\bar{k}_i = \bar{k}_{i+d}$ für alle $i = 0, \dots, n-d-1$.
- Da eine kleine Periode das Brechen der Chiffre erleichtert, sollte entweder ein Schlüsselstrom mit sehr großer Periode oder noch besser ein fortlaufender Schlüsselstrom zur Chiffrierung benutzt werden.
- Ein solcher nichtperiodischer Schlüsselstrom lässt sich beispielsweise ohne großen Aufwand erzeugen, indem man an das Schlüsselwort den Klartext oder den Kryptotext anhängt (sogenannte Autokey Chiffrierung).

Autokey Verschlüsselung

Klartext-Schlüsselstrom:

	VIGENERE	(*Klartext*)
+	WIEVIGEN	(*Schlüsselstrom*)
	RQKZVKVR	(*Kryptotext*)

Kryptotext-Schlüsselstrom:

	VIGENERE	(*Klartext*)
+	WIERQKVD	(*Schlüsselstrom*)
	RQKVDOMH	(*Kryptotext*)

SCHLÜSSELSTROMGENERATOREN

Stromchiffre	Chiffrierfunktionen	Schlüsselstromgenerator
Vigenère	$E(\hat{k}, x) = x + \hat{k}$	$g(k_0 \dots k_{d-1}, x_0 \dots x_{i-1}) = k_{(i \bmod m)}$
Beaufort	$E(\hat{k}, x) = \hat{k} - x$	$g(k_0 \dots k_{d-1}, x_0 \dots x_{i-1}) = k_{(i \bmod m)}$
Autokey mit Klartext-Schlüsselstrom	$E(\hat{k}, x) = x + \hat{k}$	$g(k_0 \dots k_{d-1}, x_0 \dots x_{i-1}) = \begin{cases} k_i, & i < d \\ x_{i-d}, & i \geq d \end{cases}$
Autokey mit Kryptotext-Schlüsselstrom	$E(\hat{k}, x) = x + \hat{k}$	$g(k_0 \dots k_{d-1}, x_0 \dots x_{i-1}) = \begin{cases} k_i, & i < d \\ y_{i-d}, & i \geq d \end{cases}$ $= k_{(i \bmod d)} + \sum_{j=1}^{\lfloor i/d \rfloor} x_{i-jd}$

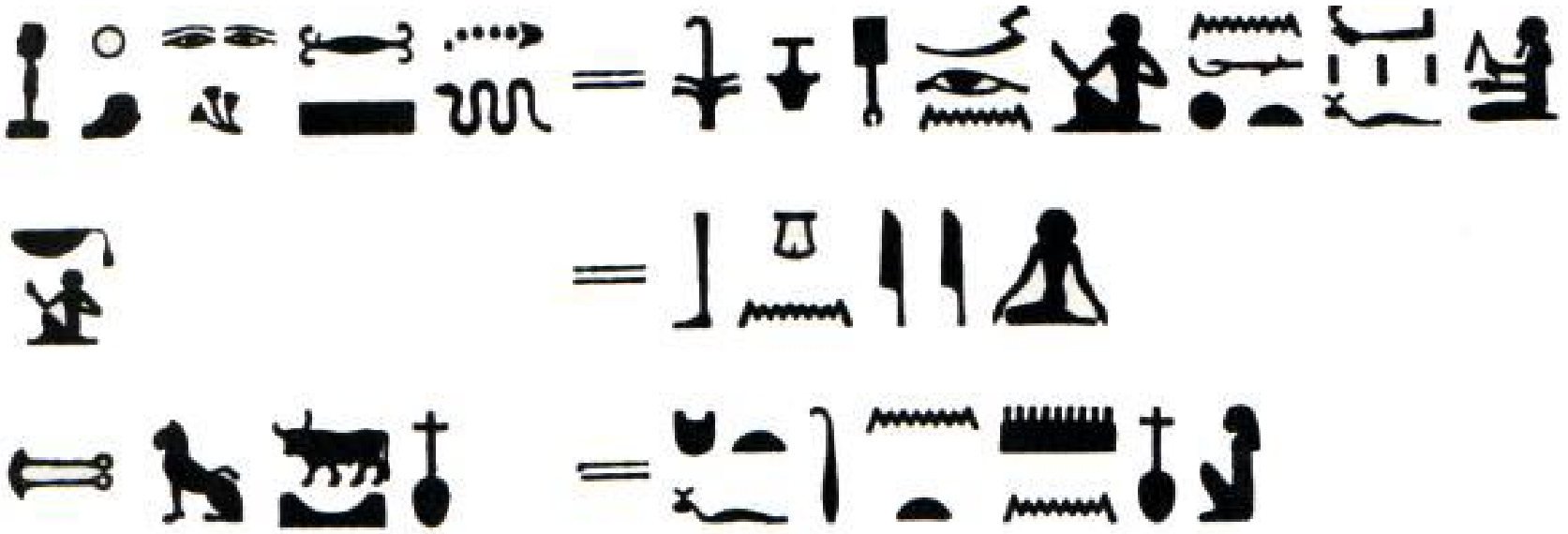
Stromchiffre Klassifizierung

- synchron: Vigenere, Beaufort
- asynchron: Autokey

Substitutionen

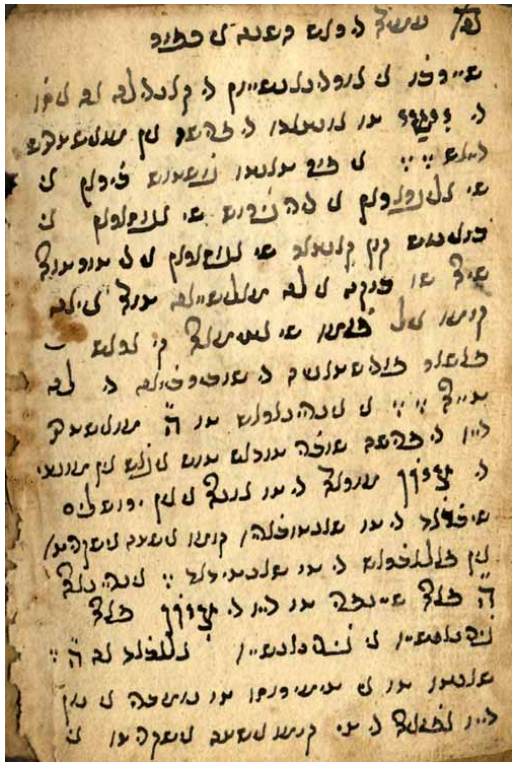
- monopartit
- bipartit
- pluripartit

Kryptographie Timeline: 1900 v. C. Knumhotep

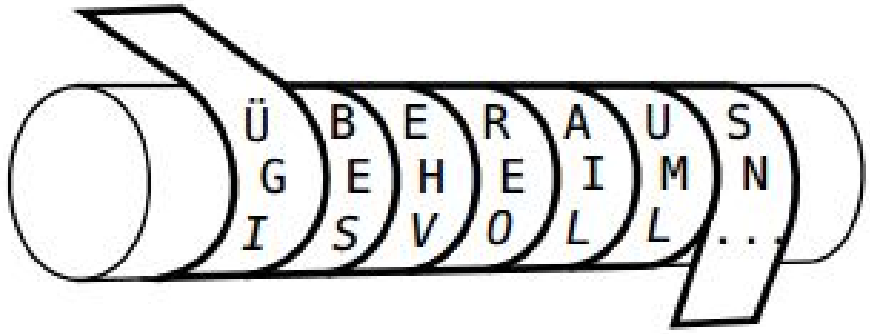


Kryptographie Timeline: 1500 v. C. Mesopotamien

KRYPTOGRAPHIE TIMELINE: 500 v. C. ATBASH



Kryptographie Timeline: 487 v. C. Skytale



ÜBERAUS GEHEIMNISVOLL ...

$\rightsquigarrow$ *ÜGI...BES...EHV...REO...AIL...UML...SN...*

Skytale

- Schlüssel = Stabumfang bzw. die Anzahl k der Zeilen, mit denen der Stab beschrieben wird.
- Findet der gesamte Klartext x auf der Skytale Platz und beträgt seine Länge ein Vielfaches von k, so geht x bei der Chiffrierung in den Kryptotext.

  $E(k, x_1 \dots x_{km}) =$

  $x_1 x_{m+1} x_{2m+1} \dots x_{(k-1)m+1} x_2 x_{m+2} x_{2m+2} \dots x_{(k-1)m+2} \dots x_m x_{2m} x_{3m} \dots x_{km}$

  über.

Skytale als Spaltentransposition

Schreibe x zeilenweise in eine $k \times m$ Matrix und lese es spaltenweise:

$$\begin{array}{cccc} x_1 & x_2 & \dots & x_m \\ x_{m+1} & x_{m+2} & \dots & x_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{(k-1)m+1} & x_{(k-1)m+2} & \dots & x_{km} \end{array}$$

- Ist die Klartextlänge kein Vielfaches von k, so kann der Klartext durch das Ein- bzw. Anfügen von sogenannten Blendern (Füllzeichen) verlängert werden.
- Damit der Empfänger diese Füllzeichen nach der Entschlüsselung wieder entfernen kann, ist lediglich darauf zu achten, dass sie im Klartext leicht als solche erkennbar sind.

Skytale - Transpositionschiffre

Transpositionen verändern nur die Reihenfolge der einzelnen Klartextzeichen.

Transposition

Definition

Sei $A = B$ ein beliebiges Alphabet und für eine natürliche Zahl $l \geq 2$ sei $M = C = A^l$. Bei einer Blocktranspositionschiffre wird durch jeden Schlüssel $k \in K$ eine Permutation π beschrieben, so dass für alle Zeichenfolgen $x_1 \dots x_l \in M$ und $y_1 \dots y_l \in C$

$$E(k, x_1 \dots x_l) = x_{\pi(1)} \dots x_{\pi(l)}$$

und

$$D(k, y_1 \dots y_l) = y_{\pi^{-1}(1)} \dots y_{\pi^{-1}(l)}$$

gilt.

Eine Blocktransposition mit Blocklänge l lässt sich durch eine Permutation $\pi \in S_l$ (also auf der Menge $\{1, \dots, l\}$) beschreiben.

Beispiel

Eine Skytale, die mit 4 Zeilen der Länge 6 beschrieben wird, realisiert beispielsweise folgende Blocktransposition:

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
$\pi(i)$	1	7	13	19	2	8	14	20	3	9	15	21	4	10	16	22	5	11	17	23	6	12	18	24

BEISPIEL

Für die Entschlüsselung muss die zu π inverse Permutation π^{-1} benutzt werden. Wird π durch Zyklen $(i_1 i_2 i_3 \ldots i_n)$ dargestellt, wobei i_1 auf i_2, i_2 auf i_3 usw. und schließlich i_3 auf i_1 abgebildet wird, so ist π^{-1} sehr leicht zu bestimmen.

i	1	2	3	4	5	6
$\pi(i)$	4	6	1	3	5	2

i	1	2	3	4	5	6
$\pi^{-1}(i)$	3	6	4	1	5	2

Beispiel

- Die Permutation π hat folgende Zyklendarstellung:

$$\pi = (143)(26)(5) \text{ oder } \pi = (143)(26),$$

wenn Einerzyklen weggelassen werden.

- Die inverse Permutation ist

$$\pi^{-1} = (341)(62) \text{ oder } (134)(26),$$

wenn wir jeden Zyklus mit seinem kleinsten Element beginnen lassen und die Zyklen nach der Größe dieser Elemente anordnen.

Beispiel

Matrix-Transposition

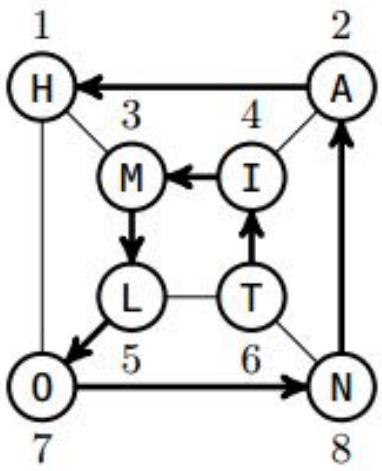
- Der Klartext wird zeilenweise in eine $k \times m$-Matrix eingelesen
- Der Kryptotext wird spaltenweise gemäß einer Spaltenpermutation π, die als Schlüssel dient, ausgelesen.
- Für $\pi = (143)(26)$ wird also zuerst Spalte $\pi(1) = 4$, dann Spalte $\pi(2) = 6$ und danach Spalte $\pi(3) = 1$ usw. und zuletzt Spalte $\pi(6) = 2$ ausgelesen.

3	6	4	1	5	2
D	I	E	S	E	R
K	L	A	R	T	E
X	T	I	S	T	N
I	C	H	T	S	E
H	R	L	A	N	G

DIESER KLARTEXT IST NICHT SEHR LANG
$\rightsquigarrow$ *SRSTA RENEG DKXIH EAIHL ETTSN ILTCR*

Beispiel: Weg-Transposition

- Der Schlüssel ist eine Hamiltonlinie in einem Graphen mit den Knoten $1, \ldots, l$ benutzt.
- Eine Hamiltonlinie ist eine Anordnung aller Knoten, in der je zwei aufeinanderfolgende Knoten durch eine Kante verbunden sind.
- Der Klartextblock $x_1 \ldots x_l$ wird gemäß der Knotennumerierung in den Graphen eingelesen und der zugehörige Kryptotext entlang der Hamiltonlinie wieder ausgelesen.



HAMILTON $\rightsquigarrow$ *TIMLONAH*

Beispiel: Weg-Transposition

- Jede Blocktransposition läßt sich durch eine Hamiltonlinie in einem geeigneten Graphen realisieren.
- Der Vorteil, eine Hamiltonlinie als Schlüssel zu benutzen, besteht darin, dass man sich den Verlauf einer Hamiltonlinie bildhaft vorstellen und daher besser einprägen kann als eine Zahlenfolge.

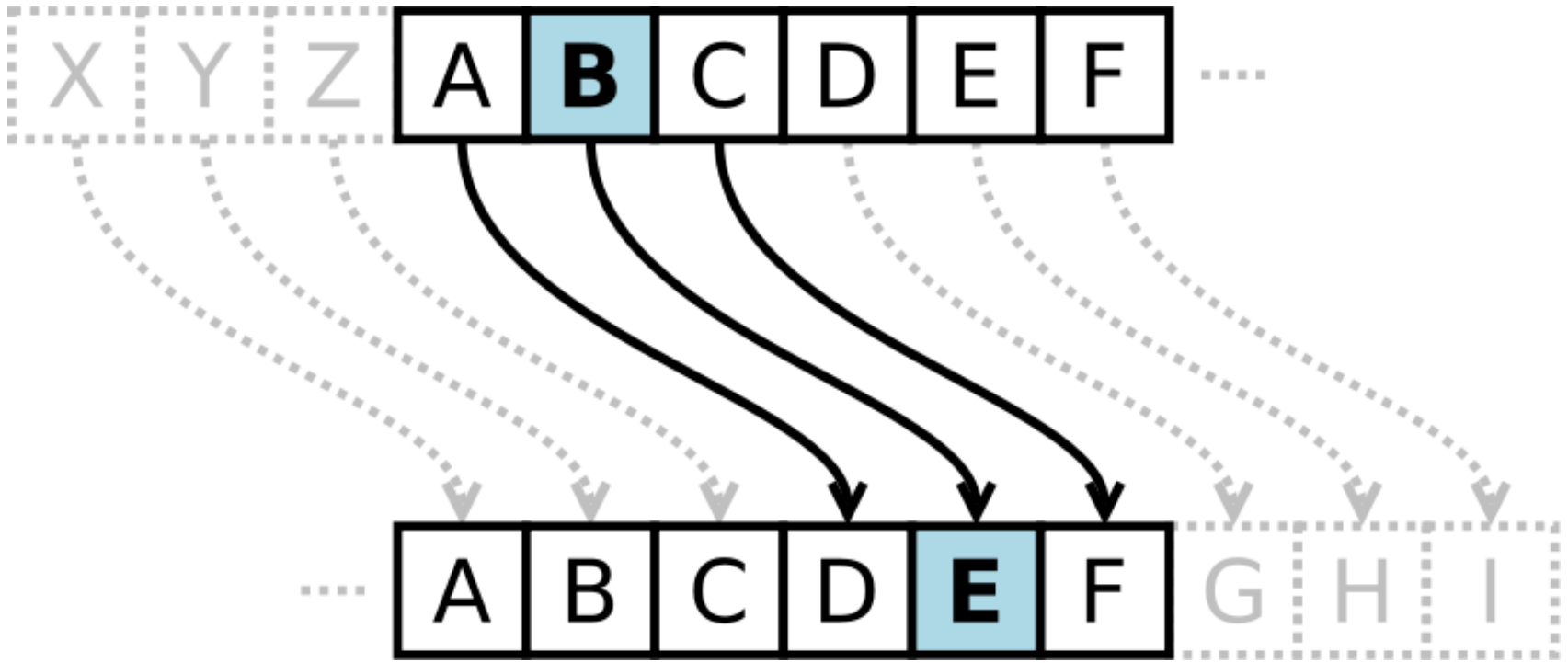
MATRIXTRANSPOSITION

Schlüsselwort für σ	C	A	E	S	A	R
i	1	2	3	4	5	6
$\sigma(i)$	3	1	4	6	2	5
Zyklendarstellung von σ	(1	3	4	6	5	2)

DIE BLOCKLAENGE IST SECHS ⇝
EDBOIL LCANKE IGSSET EXCSYH

- Ordne Schlüsselwort alphabetisch
  - CAESAR $\rightarrow$ AACERS
  - Alternativ kann man auch alle im Schlüsselwort wiederholt vorkommenden Buchstaben streichen, was im Fall des Schlüsselworts CAESAR auf eine Blocklänge von 5 führen würde.

Kryptographie Timeline: 50-60 v. C. Caesar



Verschiebungschiffre

- Buchstaben werden um festen Betrag verschoben
  - Chiffretext entsteht durch Vorwärtsverschieben
  - Aus ENDE UM ELF wird AJ AWQIWAHB
  - Originaltext durch einfaches Rückwärtsschieben ermittelbar
- Programmierbar mit Modulararithmetik
  - Bei n Buchstaben erhält jeder Buchstabe eine Zahl zwischen 0 und $n-1$
  - Schlüssel K ist eine Zahl zwischen 0 und $n-1$
  - Ver- und Entschlüsselung wird Addition/Subtraktion modulo n

$$e_K(x) = x + K \mod n, d_K(y) = y - K \mod n$$

  - Im Beispiel:

Verschiebungschiffre

- Buchstaben werden um festen Betrag verschoben
  - Chiffretext entsteht durch Vorwärtsverschieben
  - Aus ENDE UM ELF wird AJ AWQIWAHB
  - Originaltext durch einfaches Rückwärtsschieben ermittelbar
- Programmierbar mit Modulararithmetik
  - Bei n Buchstaben erhält jeder Buchstabe eine Zahl zwischen 0 und $n-1$
  - Schlüssel K ist eine Zahl zwischen 0 und $n-1$
  - Ver- und Entschlüsselung wird Addition/Subtraktion modulo n

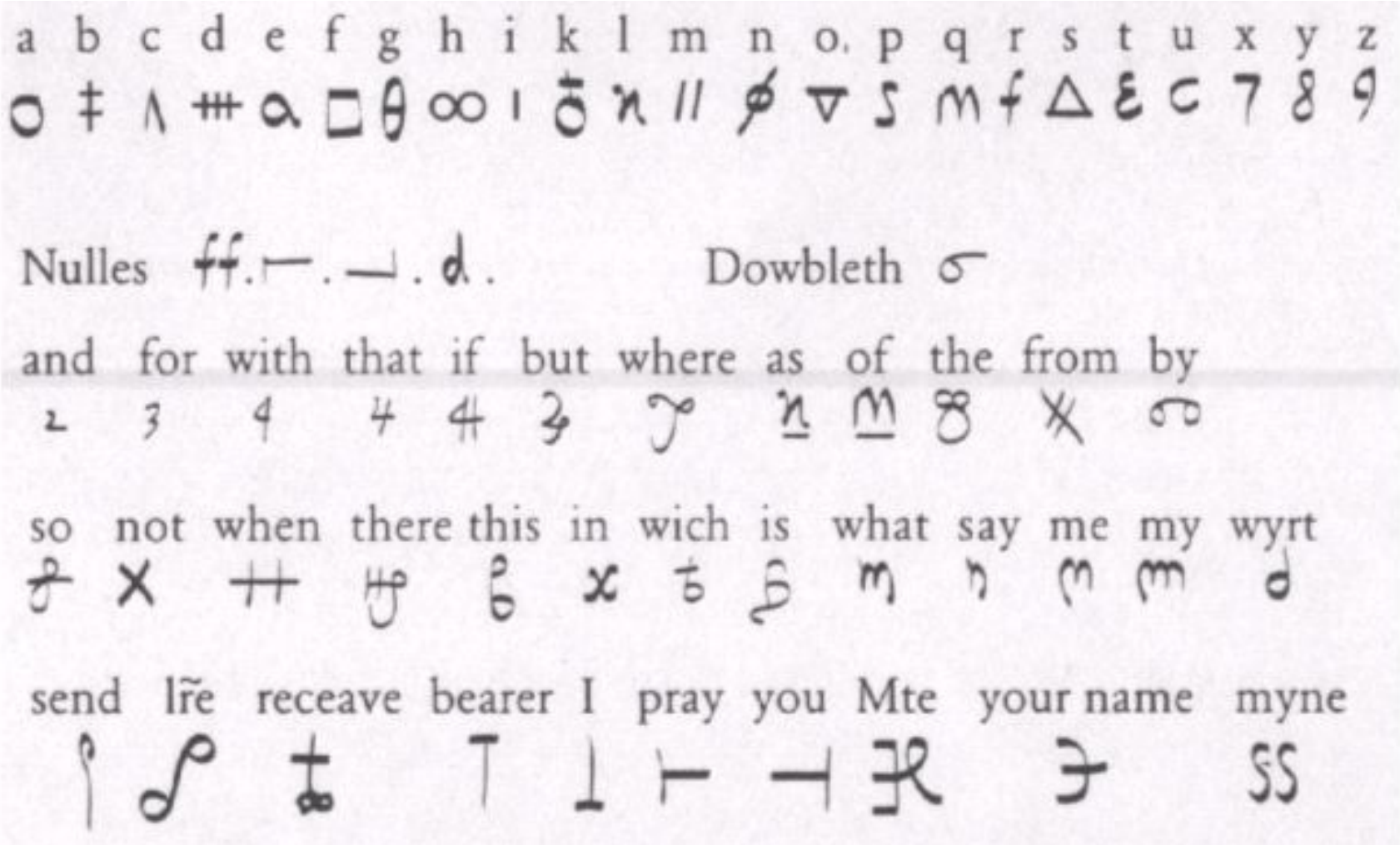
$$e_K(x) = x + K \mod n, d_K(y) = y - K \mod n$$

  - Im Beispiel: $n = 27, K = 23$

Verschiebungschiffren sind leicht zu knacken

- Brute-force Attacke: Ausprobieren aller Schlüssel
  - Einfache, aber gefährliche Attacke auf Verschlüsselungssysteme
  - Computer ermoglichen Überprüfung von Milliarden von Schlüsseln
  - Sicherheit nur bei extrem großer Anzahl möglicher Schlüssel ($\geq$ 128bit)
- Verschiebungschiffre hat maximal n Schlüssel
  - Austesten aller n Entschlüsselungen erzeugt Texte
  - Der Originaltext ist einer der erzeugten Texte
  - Nur wenige erzeugte Texte sind sprachlich akzeptabel (Wörterbuch)
  - Akzeptable Texte können *von Hand* untersucht werden
  - Aus AJ AWQIWAHB wird schrittweise ENDE UM ELF (K = 23)

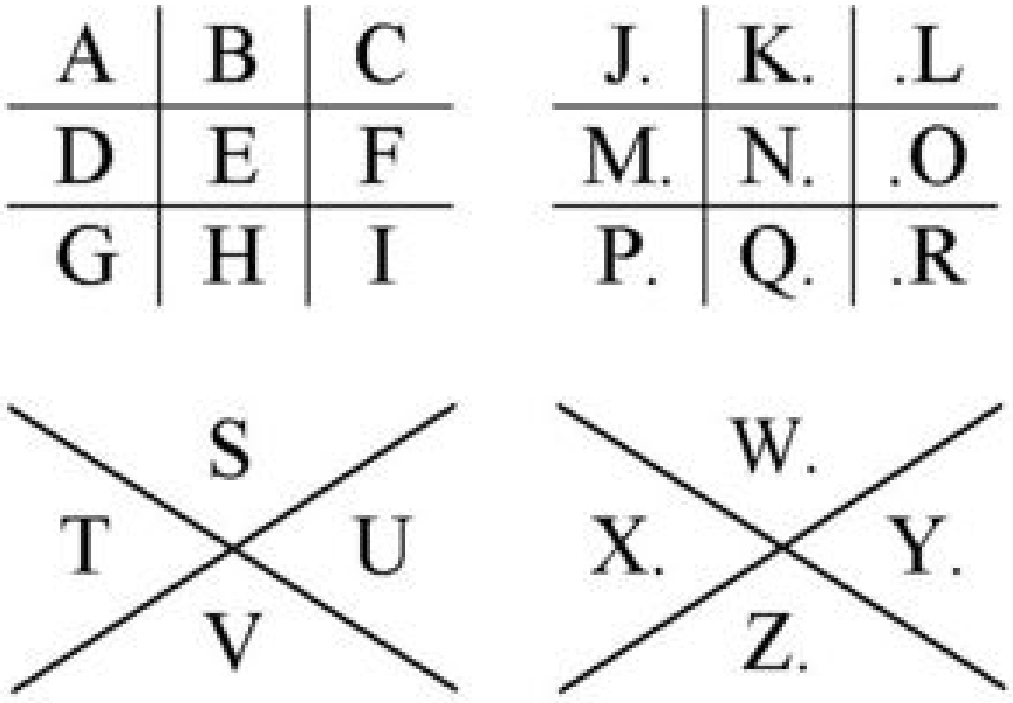
Monoalphabetische Substitution



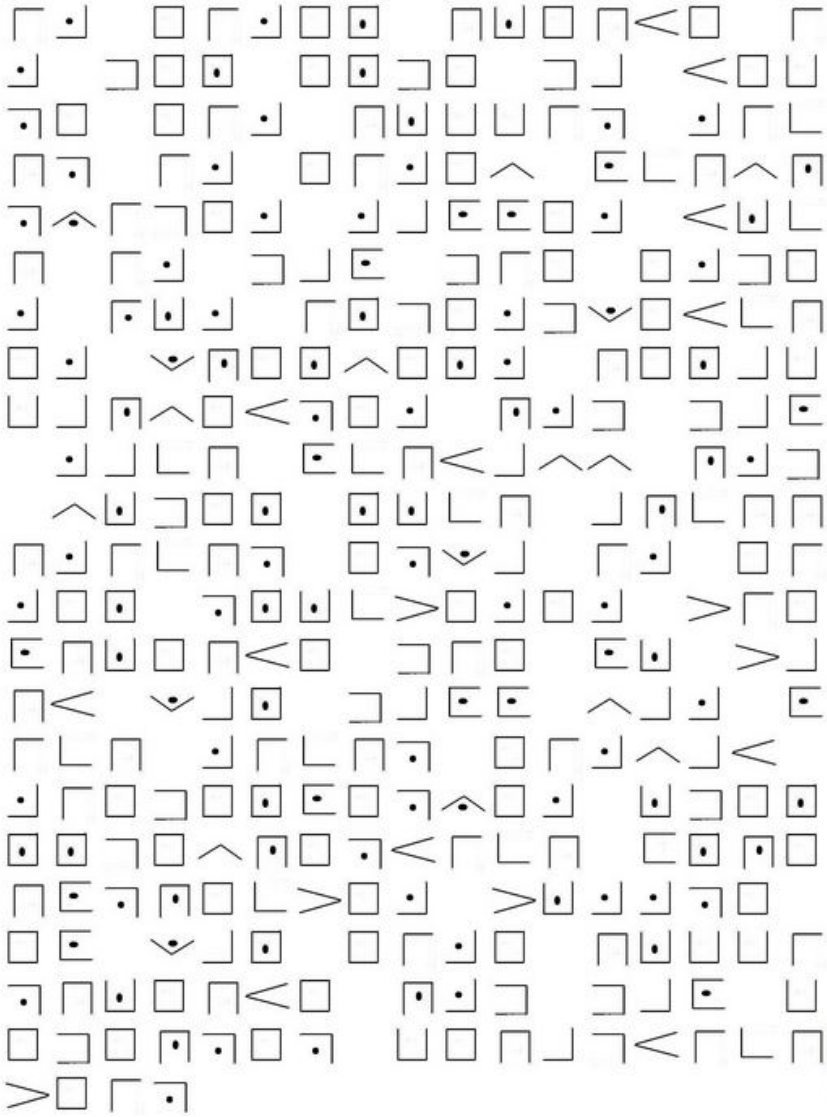
Monoalphabetische Substitution

COWCO FYNXO WCPOF FPOPD XOELO OWCRE EWLWQ
NLWCO WCOSV QNSHL AWMOC CDVVO CRQNW CPDVP
WO CP OCGRC WFMOC PÖOXQ NOCUF SOFCN OFDEE
DHSOX LOCHC PPDVC DQNQN XDSSH CPRPO FFRQN
HQN C WQNLO LÖDWC OWCOF LFRQB OCOCW OVNYN
XOPWO VRBDN XÖDFP DSDCV WQNCW QNLOW CSDXC
WOPOF VOLAO CRPOF MOSU LXWQN ÜFUNV LUQBO
CBRCC LOVÖD FOWCO REEWL NYNXO HCPPD VEOPO
HLOLO NDMXW QNBOW L

PigPen



PigPen



HINT

hdfks ljohw qhhgv dsodf hwrvw dbdqg brxkd yhwzh qwbvl
ariwk hpiur pdefw rabcw khilu vwqlq hsljoh wvvkd uhdvh
fwruh geraw khrwk huirx udukr pexvw khluq lqheu rwkhu
vwkhg rwhge rawkh odvwi rxuwk hukrp egrww khwhq
wklvq hljker uwrwk hohiw zlwkn dqgwr wkhul jkwzl wkowk
hvdph krogv wuxhi ruzwk hwzhq wbwkl ugdqg irxuw k

Polyalphabetische Substitutionen

Vigenere
Porta

Porta Chiffre

- Es werden 400 (!) unterschiedliche von Porta für diesen Zweck entworfene Kryptotextzeichen verwendet.
- Diese sind in einer 20×20-Matrix $M = (y_{ij})$ angeordnet, deren Zeilen und Spalten mit den 20 Klartextbuchstaben $A, \ldots, I, L, \ldots, T, V, Z$ indiziert sind.
- Zur Ersetzung des Buchstabenpaars $a_i a_j$ wird das in Zeile i und Spalte j befindliche Kryptotextzeichen

$$E(M, a_i a_j) = y_{ij}$$

benutzt.

Vigenere Chiffre

- Stammt aus dem 16. Jahrhundert
- Es handelt sich um ein monographisches polyalphabetisches Substitutionsverfahren.
- Der Klartext wird in Monogramme (Einzelzeichen) zerlegt und diese durch Geheimtextzeichen substituiert (ersetzt), die mithilfe eines Kennworts aus mehreren unterschiedlichen Alphabeten des Vigenere-Quadrats ausgewählt werden.
- Dabei handelt es sich um eine quadratische Anordnung von untereinander stehenden verschobenen Alphabeten.

Vigenere Chiffre

Definition

Sei A ein beliebiges Alphabet. Die Vigenere Chiffre chiffriert unter einem Schlüssel $k = k_0, \ldots, k_{d-1} \in K = A$ einen Klartext $x = x_0 \ldots x_{n-1}$ beliebiger Länge zu

$$E(k, x) = y_0 \ldots y_{n-1},$$

wobei $y_i = x_i + k(i \bmod d)$ ist, und dechiffriert einen Kryptotext $y = y_0 \ldots y_{n-1}$ zu

$$D(k, y) = x_0 \ldots x_{n-1},$$

wobei $x_i = y_i - k(i \bmod d)$ ist.

Vigenere Quadrat

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

VIGENERE VERSCHLÜSSELUNG

$$E(\mathit{WIE}, \mathtt{VIGENERE}) = \underbrace{\mathtt{V}+\mathit{W}}_{R}\ \underbrace{\mathtt{I}+\mathit{I}}_{Q}\ \underbrace{\mathtt{G}+\mathit{E}}_{K}\ \underbrace{\mathtt{E}+\mathit{W}}_{A}\ \underbrace{\mathtt{N}+\mathit{I}}_{V}\ \underbrace{\mathtt{E}+\mathit{E}}_{I}\ \underbrace{\mathtt{R}+\mathit{W}}_{N}\ \underbrace{\mathtt{E}+\mathit{I}}_{M}$$
$$= \mathit{RQKAVINM}$$

Vigenere Chiffre: Geschichtliches

- Die Methode geht zurück auf die Tabula recta, in der die Buchstaben des Alphabets in Zeilen geschrieben und bei jeder Zeile jeweils um einen Platz weiter nach links verschoben werden.
- Diese wurde durch den deutschen Benediktinerabt Johannes Trithemius (1462–1516) im Jahr 1508 im fünften Band seines in lateinischer Sprache geschriebenen sechsbändigen Werkes Polygraphiae libri sex (Sechs Bücher zur Polygraphie) angegeben.
- In dem 1518 nach seinem Tode veröffentlichten Buch schlug er vor, nach jedem einzelnen Klartextbuchstaben zum nächsten Alphabet in seiner Tabula überzugehen und so alle verfügbaren Alphabete auszunutzen. Damit erfand er die progressive polyalphabetische Chiffrierung.
- Aber es war (noch) ein festes Verfahren ohne Schlüssel.

Vigenere Chiffre: Geschichtliches

- Dieser wurde im Jahr 1553 vom italienischen Kryptologen Giovan Battista Bellaso (ca. 1505–1568/81) in Form eines vom Verschlüssler frei zu wählenden Kennworts oder eines Kennsatzes vorgeschlagen. Gerne (und kryptographisch schwach, da leicht zu erraten) wurden damals lateinische Sinnsprüche benutzt wie beispielsweise VIRTVTI OMNIA PARENT (*Alles gehorcht der Tüchtigkeit*).
- Die Buchstaben des Kennsatzes bestimmen die Reihenfolge, in der die verschiedenen Alphabete aus der Tabula ausgewählt werden müssen. Sind alle verbraucht (also einmal benutzt worden, hier nach 18 Klartextbuchstaben), so beginnt man wieder von vorn. Es handelt sich somit um eine periodische polyalphabetische Substitution mit im Beispiel einer Periode von 18.
- Eigentlich ist die, nach Vigenere benannte Verschlüsselungsmethode, die Tritemius Methode mit Schlüsselwort.

ABC Chiffre

- Handschlüsselmethode → benutzt von dem kaiserlichen Heer im Ersten Weltkrieg, um geheime militärische Nachrichten mittels drahtloser Telegrafie zu übermitteln.
- Die Verschlüsselung: zweistufig → Vigenere-Chiffre mit dem festen Schlüssel ABC gefolgt von einer einfachen Spaltentransposition mit wechselndem Kennwort.
- Etwas später wurde das Verfahren zur ABCD-Chiffre erweitert, eine Modifikation mit kaum spürbarer Auswirkung.

Spaltentransposition

- Basiert auf der Transpositionsmethode.
- Die einzelnen Zeichen der Botschaft (zumeist Buchstaben) sind umsortiert, und zwar nach einer bestimmten Verfahrensvorschrift, die durch einen geheimen Schlüssel gesteuert wird.
- Dies steht im Gegensatz zur Substitutionsmethode, bei der jedes Klartextzeichen an seinem Platz bleibt, jedoch durch ein anderes Zeichen ersetzt wird.

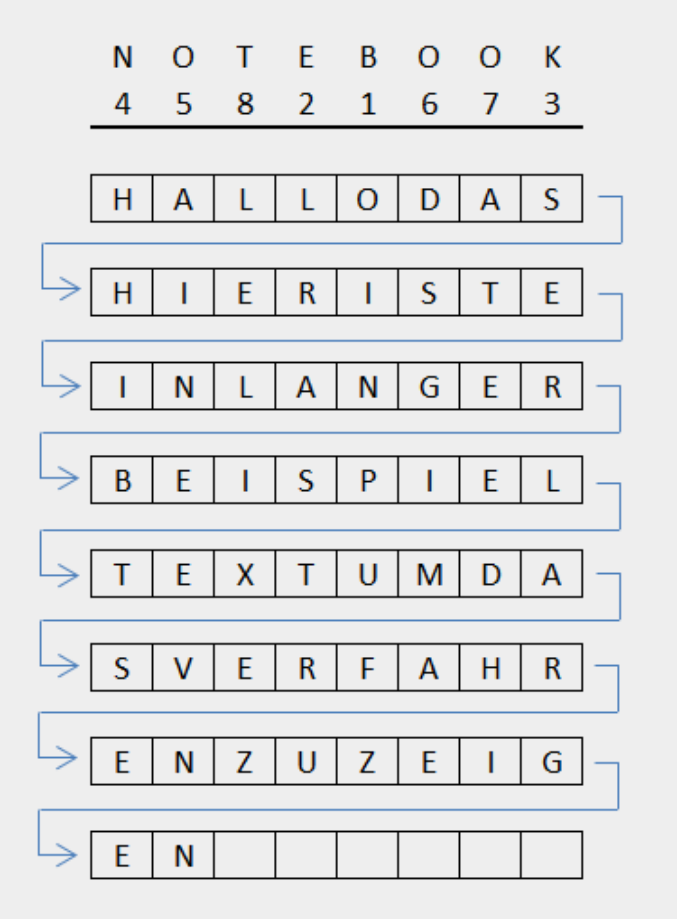
Spaltentransposition

- Der Klartext wird zeilenweise in einer Matrix eingetragen.
- Die Anzahl der Spalten ist vom Schlüssel gegeben.
- Die Spaltenanzahl entspricht der Anzahl der Buchstaben dieses Schlüsselworts.
- Anschließend wird der Klartext zeilenweise in die Matrix eingetragen.
- Als Geheimtext werden die einzelnen Buchstaben des Klartextes spaltenweise aus der Matrix ausgelesen, wobei die Reihenfolge des Auslesens der Spalten durch die alphabetischen Reihenfolge der Buchstaben des Kennworts bestimmt wird.

Doppelte Spaltentransposition

- Die einfache Spaltentransposition bietet keine große Sicherheit gegen unbefugte Entzifferung.
- Sie kann aber durch einen zweiten Verfahrensschritt zur doppelten Spaltentransposition, auch Doppelwürfel genannt, verbessert werden.
- $\rightarrow$ zweites unabhängiges Schlüsselwort mit unterschiedlicher Länge und fasst den oben angegebenen Geheimtext nur als Zwischentext auf, der in eine zweite Matrix (mit anderer Breite) erneut zeilenweise eingetragen wird und anschließend, entsprechend der Buchstabenreihenfolge des zweiten Kennworts, wieder spaltenweise ausgelesen wird.
- Dies ergibt den Geheimtext des doppelt spaltentransponierten Klartextes.

Beispiel



BEISPIEL

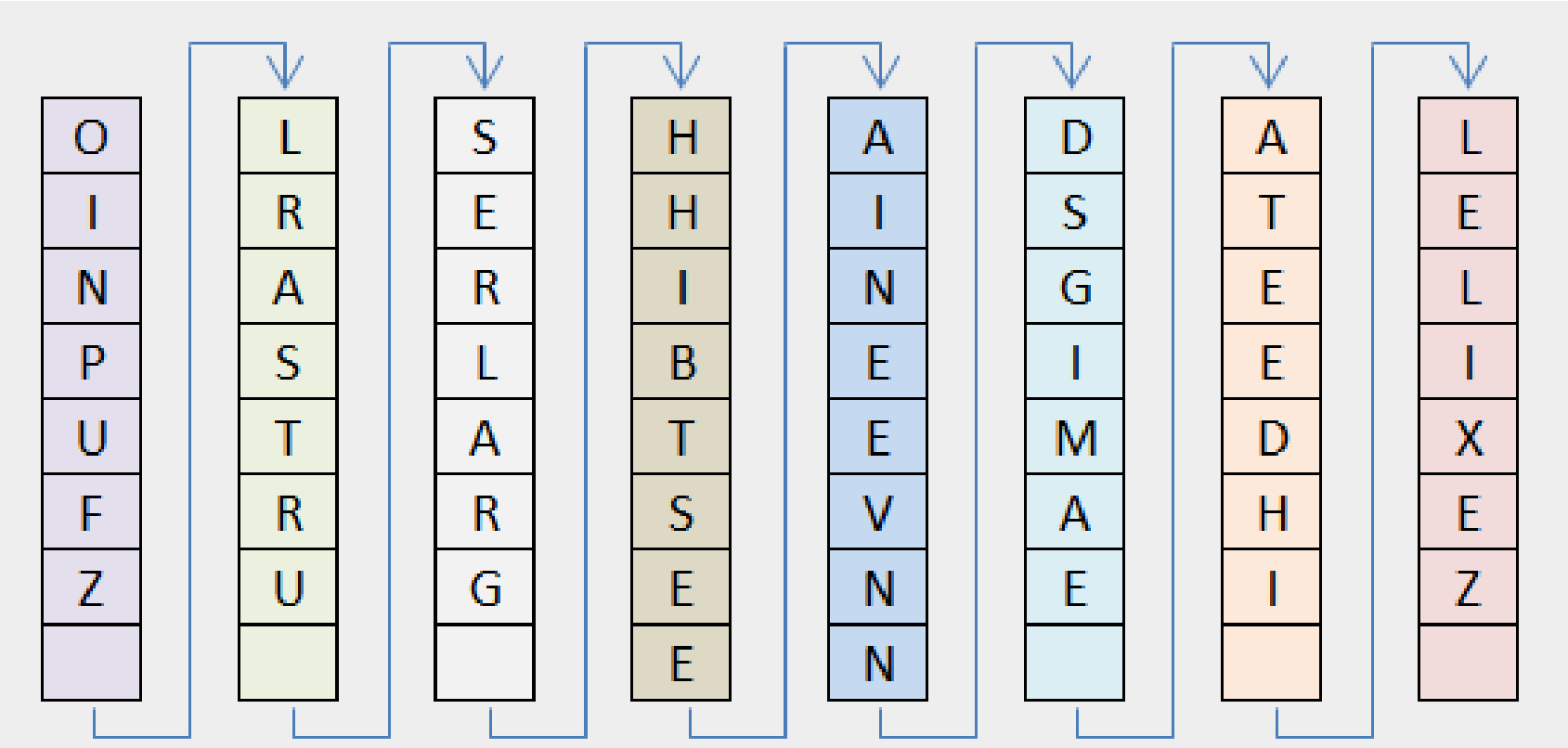
N	O	T	E	B	O	O	K
4	5	8	2	1	6	7	3

H	A	L	L	O	D	A	S
H	I	E	R	I	S	T	E
I	N	L	A	N	G	E	R
B	E	I	S	P	I	E	L
T	E	X	T	U	M	D	A
S	V	E	R	F	A	H	R
E	N	Z	U	Z	E	I	G
E	N						

B	E	K	N	O	O	O	T
1	2	3	4	5	6	7	8

O	L	S	H	A	D	A	L
I	R	E	H	I	S	T	E
N	A	R	I	N	G	E	L
P	S	L	B	E	I	E	I
U	T	A	T	E	M	D	X
F	R	R	S	V	A	H	E
Z	U	G	E	N	E	I	Z
			E	N			

BEISPIEL



Beispiel

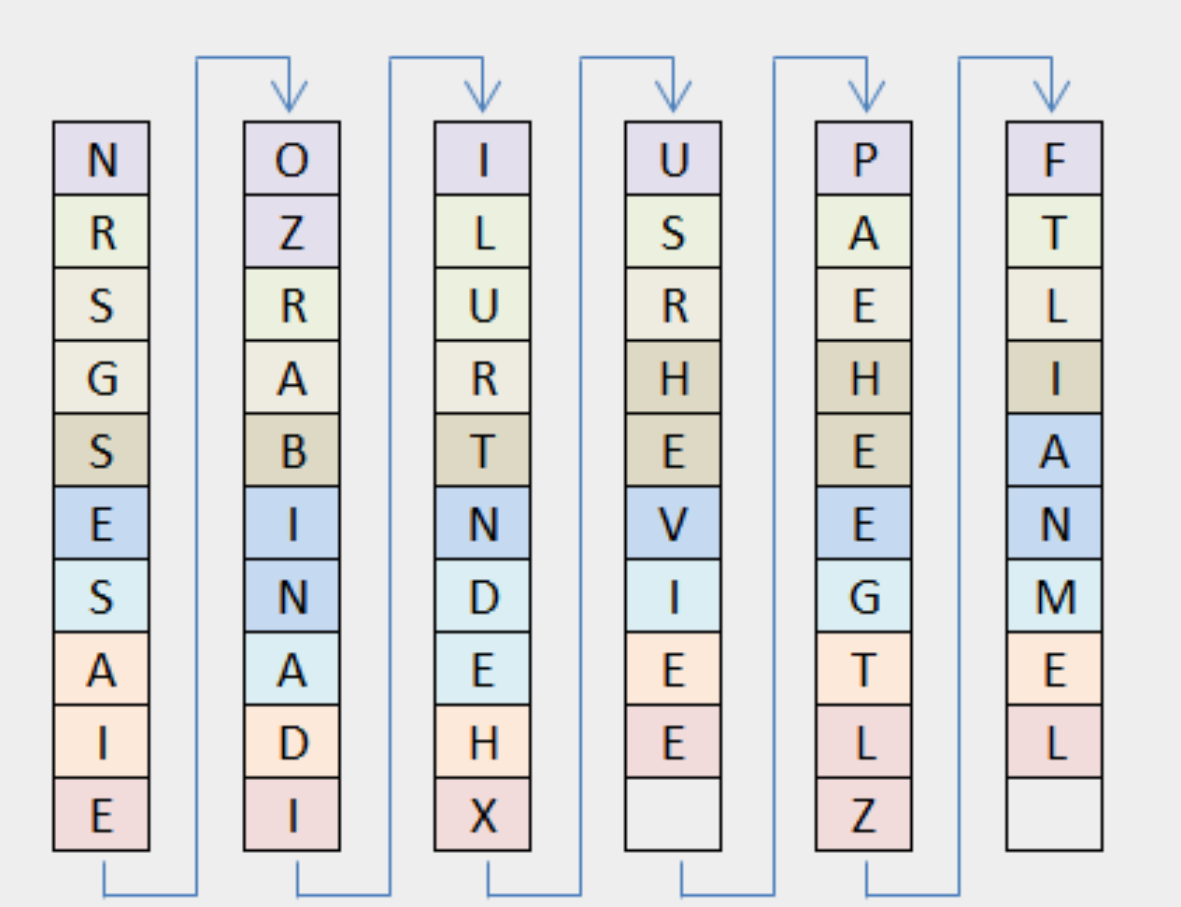
D	E	C	K	E	L
2	3	1	5	4	6

O	I	N	P	U	F
Z	L	R	A	S	T
R	U	S	E	R	L
A	R	G	H	H	I
B	T	S	E	E	A
I	N	E	E	V	N
N	D	S	G	I	M
A	E	A	T	E	E
D	H	I	L	E	L
I	X	E	Z		

C	D	E	E	K	L
1	2	3	4	5	6

N	O	I	U	P	F
R	Z	L	S	A	T
S	R	U	R	E	L
G	A	R	H	H	I
S	B	T	E	E	A
E	I	N	V	E	N
S	N	D	I	G	M
A	A	E	E	T	E
I	D	H	E	L	L
E	I	X		Z	

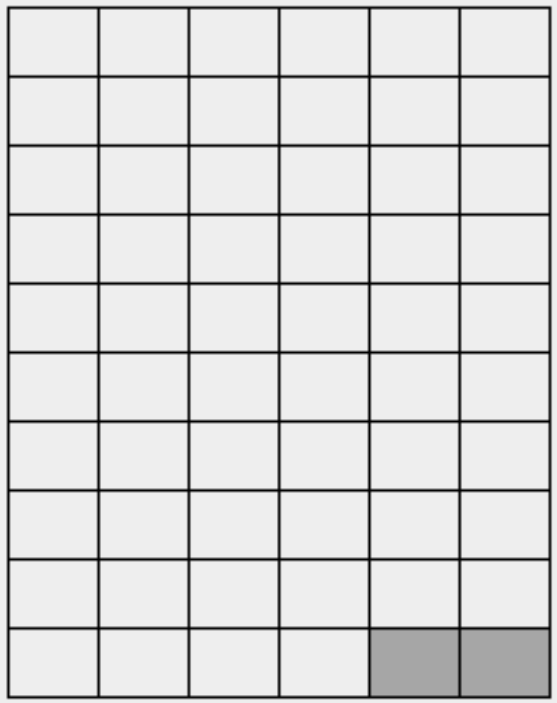
Beispiel



Beispiel

Entschlüsselung

D	E	C	K	E	L
2	3	1	5	4	6



Beispiel

Entschlüsselung

D	E	C	K	E	L
2	3	1	5	4	6

N	R	S	G	S	E
S	A	I	E	O	Z
R	A	B	I	N	A
D	I	I	L	U	R
T	N	D	E	H	X
U	S	R	H	E	V
I	E	E	P	A	E
H	E	E	G	T	L
Z	F	T	L	I	A
N	M	E	L		

O	I	N	P	U	F
Z	L	R	A	S	T
R	U	S	E	R	L
A	R	G	H	H	I
B	T	S	E	E	A
I	N	E	E	V	N
N	D	S	G	I	M
A	E	A	T	E	E
D	H	I	L	E	L
I	X	E	Z		

Beispiel

Entschlüsselung

O	I	N	P	U	F
Z	L	R	A	S	T
R	U	S	E	R	L
A	R	G	H	H	I
B	T	S	E	E	A
I	N	E	E	V	N
N	D	S	G	I	M
A	E	A	T	E	E
D	H	I	L	E	L
I	X	E	Z		

N	O	T	E	B	O	O	K
4	5	8	2	1	6	7	3

H	A	L	L	O	D	A	S
H	I	E	R	I	S	T	E
I	N	L	A	N	G	E	R
B	E	I	S	P	I	E	L
T	E	X	T	U	M	D	A
S	V	E	R	F	A	H	R
E	N	Z	U	Z	E	I	G
E	N						

ABC Chiffre: Geschichte

- Die ABC-Chiffre wurde an der Westfront noch im ersten Kriegsjahr am 18. November 1914 eingeführt.
- Auslöser waren Zeitungsartikel, wie beispielsweise im Le Matin, in dem berichtet wurde, dass die Franzosen das bisherige deutsche Verfahren gebrochen hätten und sie in der Lage seien, die geheimen deutschen Nachrichten mitzulesen.
- Bislang wurde eine doppelte Spaltentransposition verwendet.

ABC Chiffre: Verfahren

- Substitution (Ersetzung von Zeichen durch andere) + Transposition (Vertauschung der Anordnung der Zeichen).
- Für die erste Stufe wird der Klartext in Gruppen von drei Buchstaben geschrieben und der jeweils erste Buchstabe einer Dreiergruppe bleibt unverändert.
- Alle mittleren Buchstaben werden durch den im Alphabet folgenden Buchstaben ersetzt. Aus A wird B, aus B wird C, und so weiter, und aus Z wird A. Dies entspricht einer Caesar-Verschiebung um eins.
- Die letzten Buchstaben jeder Dreiergruppe werden durch den im Alphabet folgenden übernächsten Buchstaben ersetzt. Aus A wird C, aus B wird D, und so weiter. Aus Y wird A und aus Z wird B. Dies entspricht einer Caesar-Verschiebung um zwei.

ABC Chiffre: Verfahren

- Man erhält so nach der ersten Stufe der Verschlüsselung einen Zwischentext.
- Zum gleichen Ergebnis kommt man auch, wenn man den Klartext nach dem Vigenere-Verfahren mit dem Kennwort ABC verschlüsselt. Vorteil dieses recht einfachen kryptographischen Verfahrens ist, dass es ohne irgendwelche Hilfsmittel im Kopf durchgeführt werden konnte. Nachteilig ist die geringe kryptographische Sicherheit, die es bietet.

ABC Chiffre: Verfahren

Zweite Stufe

- Im Gegensatz zu der beim Doppelwürfel zuvor verwendeten doppelten Spaltentransposition, begnügte man sich hier mit einer einfachen Spaltentransposition. Der Zwischentext wurde zeilenweise in eine rechteckige Matrix geschrieben, deren Breite durch die Länge eines Kennworts vorgegeben war.
- Der Zwischentext wurde zeilenweise in diese Matrix eingetragen und anschließend spaltenweise wieder ausgelesen.
- Dabei wurden die Spalten nicht regelmäßig von links nach rechts eine nach der anderen genommen, sondern, gesteuert durch die alphabetische Reihenfolge der Buchstaben des Kennworts, mehr oder weniger unregelmäßig ausgelesen.

ABC Chiffre: Entschlüsselung

- Auf der Empfangsseite wurden die aufgenommenen Morsezeichen als Buchstaben spaltenweise in ein Rechteck mit bekannter Breite eingetragen.
- Die Länge des Kennworts gibt die benötigte Breite des Rechtecks.
- Die Spalten wurden nicht von links nach rechts sondern in der durch die alphabetische Reihenfolge der Buchstaben des Kennworts vorgegebenen Reihenfolge gefüllt, wobei die Länge der Spalten, also die Höhe des Rechtecks, durch Division der Länge des Funkspruchs durch die Länge des Kennworts und gegebenenfalls Aufrunden auf die nächste natürliche Zahl bestimmt wurde.

ABC Chiffre: Entschlüsselung

- Anschließend wurde der spaltenweise eingetragene Geheimtext zeilenweise ausgelesen und man erhielt den ursprünglichen Zwischentext wieder zurück.
- Nun musste nur noch die Caesar-Verschiebung rückgängig gemacht werden.
- Der Zwischentext wurde dazu in Dreiergruppen geschrieben.
- Anschließend wurden alle mittleren Buchstaben jeder Gruppe durch die im Alphabet unmittelbar davor liegenden ersetzt und alle hinteren Buchstaben jeder Gruppe durch die im Alphabet um zwei Plätze davor liegenden substituiert. So erhielt man den ursprünglichen Klartext wieder zurück.

POLYBIUS 200 v. C.

	0	1	2	3	4
0	A	B	C	D	E
1	F	G	H	I	J
2	K	L	M	N	O
3	P	Q	R	S	T
4	U	V	W	X/Y	Z

POLYBIOS $\rightsquigarrow$ 3024214301132433

Pluripartite Substitutionen

- ADFGVX
- BIFID
- Four-Square
- Playfair

ADFGX

- ADFGX und ADFGVX (auch: ADGFX beziehungsweise ADGFVX; eigentlich Geheimschrift der Funker 1918, kurz GedeFu 18) sind manuelle Verschlüsselungsverfahren, die die deutschen Militärs im Ersten Weltkrieg einsetzten.
- Sie dienten dazu, Nachrichten mittels drahtloser Telegrafie geheim zu übermitteln.
- Die Verschlüsselung geschieht zweistufig und basiert auf einer Substitution, gefolgt von einer Transposition.
- ADFGX wurde zum ersten Mal am 1. März 1918 an der deutschen Westfront eingesetzt.
- ADFGVX ist der Nachfolger von ADFGX und wurde ab dem 1. Juni 1918 benutzt.

ADFGX: Verschlüsselung - erste Stufe

- Die Klartextzeichen werden monoalphabetisch durch Zeichenpaare ersetzt, die nur aus den Buchstaben A, D, F, G und X bestehen.
- Dies geschieht mit Hilfe eines Polybios-Quadrats nach folgendem Schema:
- In einer Matrix aus fünf Zeilen und fünf Spalten wird ein geheimer Schlüssel in Form eines Kennworts eingetragen, beispielsweise KRYPTOTEST.
- Dabei werden im Kennwort mehrfach auftretende Buchstaben nur einmal verwendet: KRYPTOES.

ADFGX: Verschlüsselung - erste Stufe

- Der Rest des Quadrats wird mit den übrigen Buchstaben des Alphabets (häufig in revertierter Reihenfolge, also beginnend mit Z) aufgefüllt.
- Da das übliche lateinische Alphabet aus 26 Buchstaben besteht, eine $5x5$-Matrix jedoch nur 25 Plätze bietet, lässt man einen Buchstaben weg
- Zusätzlich werden an den oberen und den linken Rand des Polybios-Quadrats die fünf Buchstaben A, D, F, G und X geschrieben.

ADFGX: Verschlüsselung - zweite Stufe

- Der Zwischentext wird zeilenweise in einer zweiten Matrix eingetragen.
- Die Breite der Matrix ergibt sich aus der Länge eines zweiten Schlüsselworts.
- Tatsächlich wurden Schlüssel der Länge 15 bis 22 und Matrizen mit entsprechender Breite verwendet.
- Dieses zweite Kennwort, zum Beispiel BEOBACHTUNGSLISTE, wird über die zweite Matrix geschrieben.
- Die Buchstaben dieses Schlüssels können in alphabetischer Reihenfolge nummeriert werden.
- Das A bekommt die Nummer 1, das B am Anfang die Nummer 2, das zweite B die Nummer 3 und so weiter bis schließlich zum U, das die Nummer 17 erhält.

ADFGX: Verschlüsselung - zweite Stufe

- Nachdem der Zwischentext zeilenweise in die Matrix eingetragen wurde, wird er nun spaltenweise wieder ausgelesen.
- Dabei wird die Reihenfolge der Spalten durch die alphabetische Reihenfolge der einzelnen Buchstaben des Kennworts bestimmt, die der Deutlichkeit halber unterhalb des Kennworts vermerkt ist.
- Das Auslesen beginnt also mit der fünften Spalte (Kennwortbuchstabe A) und endet mit der neunten Spalte (Kennwortbuchstabe U).

ADFGVX

	A	D	F	G	V	X
A	K	Z	W	R	1	F
D	9	B	6	C	L	5
F	Q	7	J	P	G	X
G	E	V	Y	3	A	N
V	8	O	D	H	0	2
X	U	4	I	S	T	M

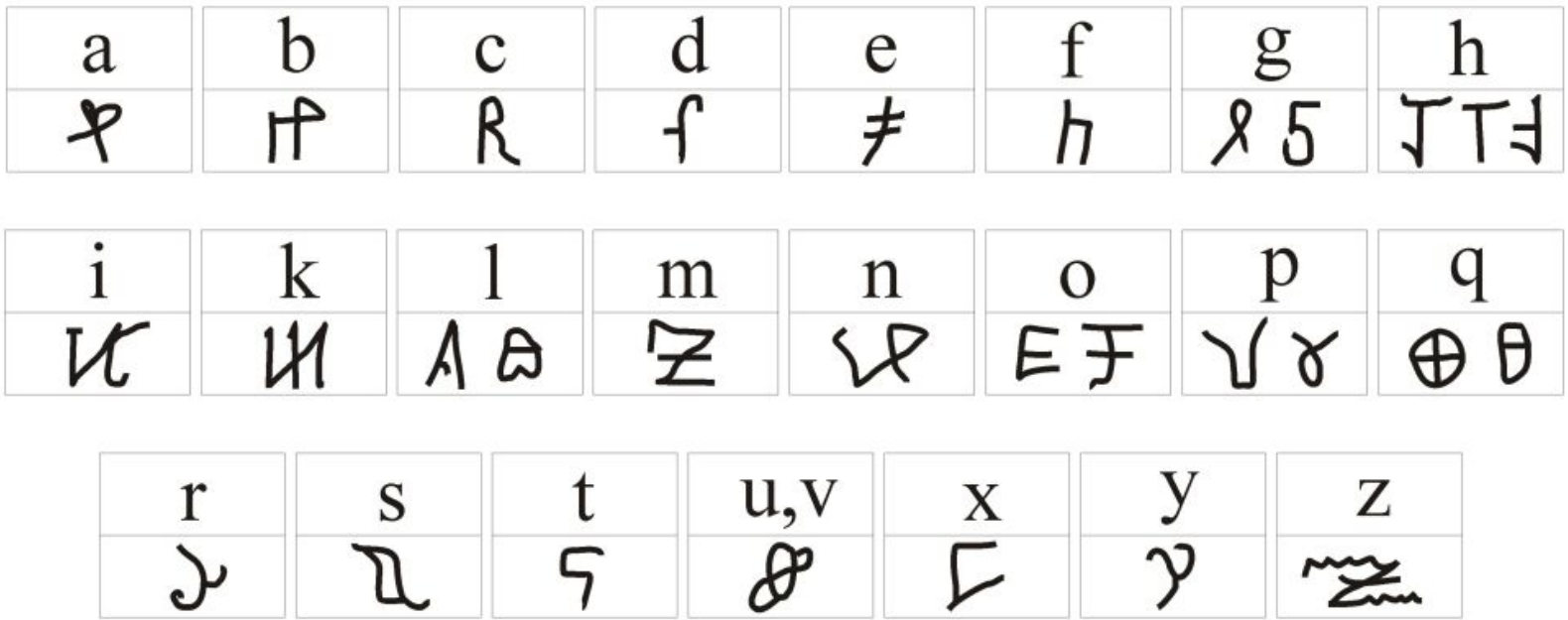
Alphabetum Kaldeorum

- Das Alphabetum Kaldeorum ist eine der bekanntesten Geheimschriften des Mittelalters. Sein Name verweist auf das Volk der Chaldäer, die in der mittelalterlichen Ideenwelt für geheimnisvolles und magisches Wissen standen.
- Überliefert ist es in vollständiger Fassung, zusammen mit anderen nichtlateinischen Alphabeten, in einer Handschrift aus dem Jahre 1428, die sich heute in der Universitätsbibliothek München befindet;
- Seine Ursprünge liegen jedoch in deutlich früherer Zeit, wie einige erhaltene Beispiele für die praktische Verwendung belegen.

Alphabetum Kaldeorum

Alphabetum Kaldeorum

(nach einer Handschrift von 1428, München, Univ.-Bibl. Cod. 4° 810, fol. 41v)



Buch-Verschlüsselung

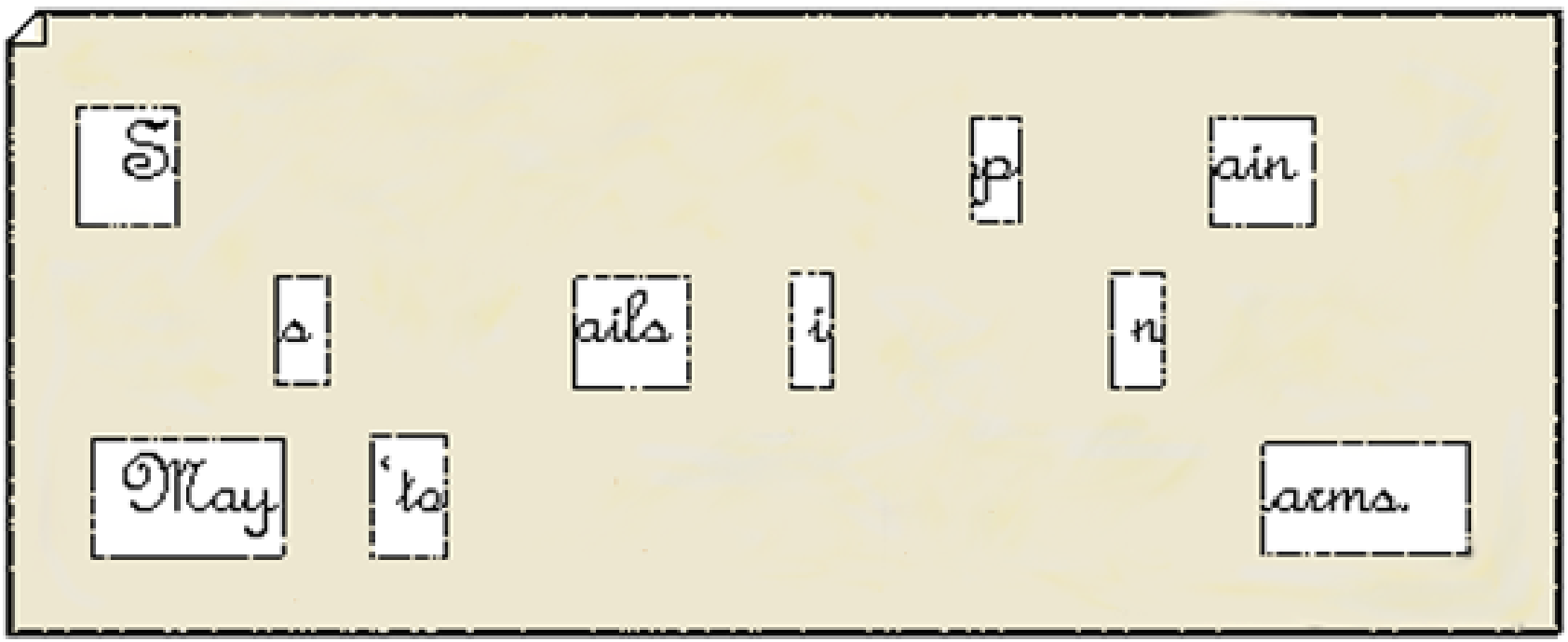
- Ist eine symmetrische Verschlüsselung, bei der man durch Angeben der Seitenzahl in einem Buch sowie der Zeilennummer und der Positionsnummer von Buchstaben auf einer Seite des Buchs Nachrichten verschlüsseln und anschließend geheim übermitteln kann.
- Der Begriff Buch bezeichnet hier ein beliebiges Schriftstück, das dem Nachrichtensender und dem Empfänger vorliegt; es kann sich um ein beliebiges Textdokument handeln. Das Buch stellt die Grundlage zur Verschlüsselung dar und übernimmt die Funktion des Schlüssels.

Cardan-Gitter

- Das etwa um das Jahr 1550 von dem italienischen Mathematiker Gerolamo Cardano erdachte, nach ihm benannte Cardan-Gitter spielte in der frühen Neuzeit eine bedeutende Rolle bei der Verschlüsselung von Botschaften. Aus Sicht der modernen Kryptographie handelt es sich um ein Steganographieverfahren.
- Auf eine Schreibunterlage (Pergament, Papier etc.) wird ein Gitter gezeichnet. Einige der Felder der so entstandenen Tabelle werden dann aus dem Träger ausgeschnitten. Somit entsteht eine gelöcherte Vorlage, also eine Schablone, hier ein sogenanntes individuelles Cardan-Gitter.

Cardan-Gitter

Sir John regards you well and spekes again that
all as rightly 'vails him is yours now and ever.
May he 'tone for past d'lays with many charms.



Cardan-Gitter

- Um nun einen Text mit Hilfe der Schablone zu verschlüsseln, wird das individuelle Cardan-Gitter auf ein leeres Stück Papier gelegt, und nur an den Stellen, an denen die Schablone löcherig ist, die in Wortstücke, Silben, Buchstaben oder sonstige Transkriptionen zerlegte Botschaft, eingetragen.
- Der Rest der Tabelle kann mit beliebigen Daten gefüllt werden.
- Zur Entschlüsselung der Botschaft benötigt man das individuelle Cardan-Gitter.
- Heutzutage wird die Funktionalität des Cardan-Gitters noch häufig im Zusammenhang mit der Steganographie genutzt.

Blockchiffre

Sei A ein beliebiges Alphabet und es gelte $M = C = A^l, l \geq 1$. Eine Blockchiffre realisiert für jeden Schlüssel $k \in K$ eine bijektive Abbildung g auf A^l und es gilt

$$E(k, x) = g(x) \text{ und } D(k, y) = g^{-1}(y)$$

für alle $x \in M$ und $y \in C$. Im Fall $l = 1$ spricht man auch von einer einfachen Substitutionschiffre.

Polyalphabetische Substitution

- Polyalphabetischen Chiffrierverfahren operieren auf Klartextblöcken einer festen Länge l, die sie in Kryptotextblöcke einer festen Länge l' überführen, wobei meist $l = l'$ ist.
- Da diese Blöcke jedoch vergleichsweise kurz sind, kann der Klartext der Chiffrierfunktion ungepuffert zugeführt werden.
- Man nennt die einzelnen Klartextblöcke in diesem Zusammenhang auch nicht *Blöcke* sondern *Zeichen* und spricht von sequentiellen Chiffren oder von Stromchiffren.

Chiffrierscheibe

- Zwei runde Metallscheiben, die auf einer gemeinsamen Achse sitzen und so verbunden sind, dass sich die kleinere auf der größeren drehen kann.
- Scheiben dieser Art gibt es seit dem 15. Jahrhundert. Die Entwicklung der ersten Chiffrierscheibe wird Leon Battista Alberti zugeschrieben.
- Am äußeren Rand der Scheiben sind jeweils unterschiedliche Alphabete oder Symbole angegeben. Durch Verdrehen der Scheiben gegeneinander verschieben sich diese Alphabete, was zur Verschlüsselung genutzt wird.

Chiffrierscheibe

Jefferson-Walze

- Die Jefferson-Walze ist ein Hilfsmittel zur Chiffrierung und Decodierung von Botschaften. Sie wurde von Thomas Jefferson um 1790 entwickelt.
- Das Chiffrenrad ist ein 4,8 Zentimeter dicker und 14,4 Zentimeter langer Zylinder aus Holz.
- Dieser Zylinder besteht aus 36 nummerierten Scheiben, die 0,4 Zentimeter breit sind und deren Randflächen in 26 gleich große Abschnitte für die 26 Buchstaben aufgeteilt sind.
- Die Reihenfolge der Scheiben ist entscheidend für die Ver- und Entschlüsselung und muss beim Sender und Empfänger gleich sein.

Jefferson-Walze

- Der Text wird in einer Zeile eingestellt und die Walze arretiert.
- Die Scheiben zeigen 25 verschlüsselte Zeilen, aus denen der Sender eine für die Übermittlung auswählen kann.
- Der Empfänger stellt die Scheiben seines Zylinders so ein, dass er die gleiche Buchstabenfolge wie die Botschaft in einer Zeile erhält.
- Unter den anderen 25 Zeilen befindet sich dann auch die Klarbotschaft.

JEFFERSONWALZE

Playfair

- Erfunden 1854 von Charles Wheatstone: jedes Buchstabenpaar des Klartextes durch ein anderes Buchstabenpaar ersetzt wird.
- Sie gehört damit zur Klasse der bigraphischen Verfahren.
- Berühmt wurde sie unter dem Namen eines guten Bekannten von Wheatstone, Lord Lyon Playfair, der diese Methode zur Benutzung beim britischen Militär empfahl.
- Die Playfair-Verschlüsselung wurde erstmals im Krimkrieg eingesetzt und war bis zum Ersten Weltkrieg, in modifizierter Form sogar noch während des Zweiten Weltkriegs, in Gebrauch.

Playfair

- Zum Zeitpunkt ihrer Erfindung war die Playfair-Verschlüsselung im Vergleich zu den damals üblichen, auf der Verschlüsselung von Einzelzeichen basierenden Methoden ein sehr sicheres Verfahren.
- Dies änderte sich jedoch im frühen 20. Jahrhundert. So konnten ab Mitte 1915 die von den Briten mit Playfair verschlüsselten Nachrichten von der deutschen Gegenseite häufig entziffert werden, umgekehrt brachen britische Codeknacker im englischen Bletchley Park die von deutschen Militärs etwas abgewandelten Playfair-Verschlüsselungen im Zweiten Weltkrieg.

Playfair Verschlüsselung

- Monoalphabetisch
- Bigraphisch: Blöcke der Länge 2

Playfair Quadrat

- Schlüsselwort wird in einem 5×5 Quadrat eingetragen, danach die restlichen Buchstaben
- Klartext Bigramme $\rightarrow$ Geheimtext Bigramme

VERSCHLÜSSELUNG

- Beide Buchstaben stehen in derselben Spalte oder in derselben Zeile → es werden jeweils die unteren beziehungsweise rechten Nachbarbuchstaben als Geheimbuchstaben genommen.
- Die Buchstaben stehen am Rand des Playfair-Quadrats → es wird einfach am anderen Rand fortgesetzt.
- Die beiden Buchstaben stehen in unterschiedlichen Zeilen und Spalten → man ersetzt den ersten Klarbuchstaben durch den in derselben Zeile aber in der Spalte des zweiten liegenden.
- Der zweite Klarbuchstabe wird durch den in derselben Zeile aber in der Spalte des ersten Klarbuchstabens ersetzt.
- Das Klartextpaar bildet also die diagonal gegenüber liegenden Ecken eines Rechtecks.

Beispiel

- Klartext Laboulaye lady will lead to Cibola temples of gold
- Bigramme: LA BO UL AY EL AD YW IL LX LE AD TO CI BO LA TE MP LE SO FG OL DX

Beispiel: Playfair Quadrat

D	E	A	T	H
B	C	F	G	I
K	L	M	N	O
P	Q	R	S	U
V	W	X	Y	Z

VESCHLÜSSELUNG

- Geheimtext: ME IK QO TX CQ TE ZX CO MW QC TE HN FB IK ME HA KR QC UN GI KM AV

Spreizung

- Spreizung (englisch straddling) ist eine in der Kryptologie bei der Verschlüsselung von Texten benutzte Methode.
- Dabei werden Klartextzeichen durch Geheimtextzeichen unterschiedlicher Länge ersetzt.
- Spreizung wird insbesondere bei Handschlüsseln, also manuell (mit Bleistift und Papier) durchgeführten Verschlüsselungsverfahren verwendet, speziell bei den sogenannten Spionage-Chiffren

Spreizung

- Die 26 Großbuchstaben des lateinischen Alphabets werden in drei Zeilen und zehn Spalten einer Tabelle geschrieben.
- Man beginnt mit einem Kennwort, das die häufigsten Buchstaben enthält, wie beispielsweise ERNSTL und füllt den Rest der Tabelle mit den übrigen Buchstaben auf, im einfachsten Fall in alphabetischer Reihenfolge.
- Wichtig ist, in der ersten Zeile der Tabelle zwei Felder frei zu lassen.
- In der letzten Zeile bleiben nach Eintragen aller Buchstaben noch zwei Felder zur freien Verfügung, die mit Sonderzeichen (hier · und /) gefüllt werden können.
- Diesen lassen sich bei Bedarf Sonderfunktionen zuordnen, wie Buchstaben-Ziffernumschaltung, können aber auch einfach nur Blender sein.

Beispiel

	0	1	2	3	4	5	6	7	8	9
	E	R	N	S	T	L	A	B		
8	C	D	F	G	H	I	J	K	M	O
9	P	Q	U	V	W	X	Y	Z	.	/

Verschlüsselung

straddling checkerboard, gespreiztes Schachbrett

- Diese Tabelle erlaubt die monoalphabetische Substitution der Buchstaben durch Zahlen, wobei die Buchstaben in der ersten Zeile durch einziffrige Zahlen und die Buchstaben in den anderen beiden Zeilen durch zweiziffrige Zahlen ersetzt werden.
- Diese Besonderheit, nämlich dass die Klartextzeichen durch Geheimtextzeichen unterschiedlicher Länge ersetzt werden, wird als Spreizung bezeichnet. Die so entstehende Chiffre heißt gespreizt.

Hill Chiffre

Sei $A := \{a_0, \ldots, a_{m-1}\}$ ein beliebiges Alphabet und für eine natürliche Zahl $l \geq 2$ sein $M = C = A^l$. Bei der Hill-Chiffre ist $K = \{k \in \mathbb{Z}_m^{l \times l} \mid \text{ggt}(\det(k), m) = 1\}$ und es gilt

$$E(k, x) = xk \text{ und } D(k, y) = yk^{-1}.$$

Satz

Sei A ein Alphabet und sei $k \in \mathbb{Z}_m^{l \times l}$ $(l \geq 1, m = ||A||)$. Die Abbildung $f : A^l \to A^l$ mit

$$f(x) = xk,$$

ist genau dann injektiv, wenn $\text{ggt}(\det(k), m) = 1$ ist.

Beispiel

Benutzen wir zur Chiffrierung von Klartextblöcken der Länge $l = 4$ über dem lateinischen Alphabet A_{lat} die Schlüsselmatrix

$$k = \begin{pmatrix} 11 & 13 & 8 & 21 \\ 24 & 17 & 3 & 25 \\ 18 & 12 & 23 & 17 \\ 6 & 15 & 2 & 15 \end{pmatrix}.$$

so erhalten wir beispielsweise für den Klartext HILL

Hill-Chiffre

$$(HILL)\begin{pmatrix} 11 & 13 & 8 & 21 \\ 24 & 17 & 3 & 25 \\ 18 & 12 & 23 & 17 \\ 6 & 15 & 2 & 15 \end{pmatrix} = (NERX)$$


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!


WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.