

Verschlüsselungsmethoden

Dozent: Prof. Dr. Michael Eichberg

Version: 1.0.1

Quelle: Im Wesentlichen: *Cryptography and Network Security - Principles and Practice, 8th Edition, William Stallings*

Folien: [HTML] <https://delors.github.io/sec-klassische-verschluesselungsverfahren/folien.de.rs-t.html>

[PDF] <https://delors.github.io/sec-klassische-verschluesselungsverfahren/folien.de.rs-t.html.pdf>

Fehler melden: <https://github.com/Delors/delors.github.io/issues>

Definitionen

Klartext:

 *Plaintext*


Die Originalnachricht, die verschlüsselt werden soll.

Geheimtext oder Chiffretext oder **Kryptogramm**:

 *Ciphertext*


Die kodierte/verschlüsselte Nachricht.

Verschlüsselung:

 *Encryption*

Der Prozess der Umwandlung von Klartext in Geheimtext.

Entschlüsselung:

 *Decryption*

Der Prozess der Wiederherstellung des Klartextes aus dem Geheimtext.

Definitionen

Kryptographie:  *Cryptography*

Das Studiengebiet der Verschlüsselungsschemata.

Kryptoanalyse:  *Cryptanalysis*

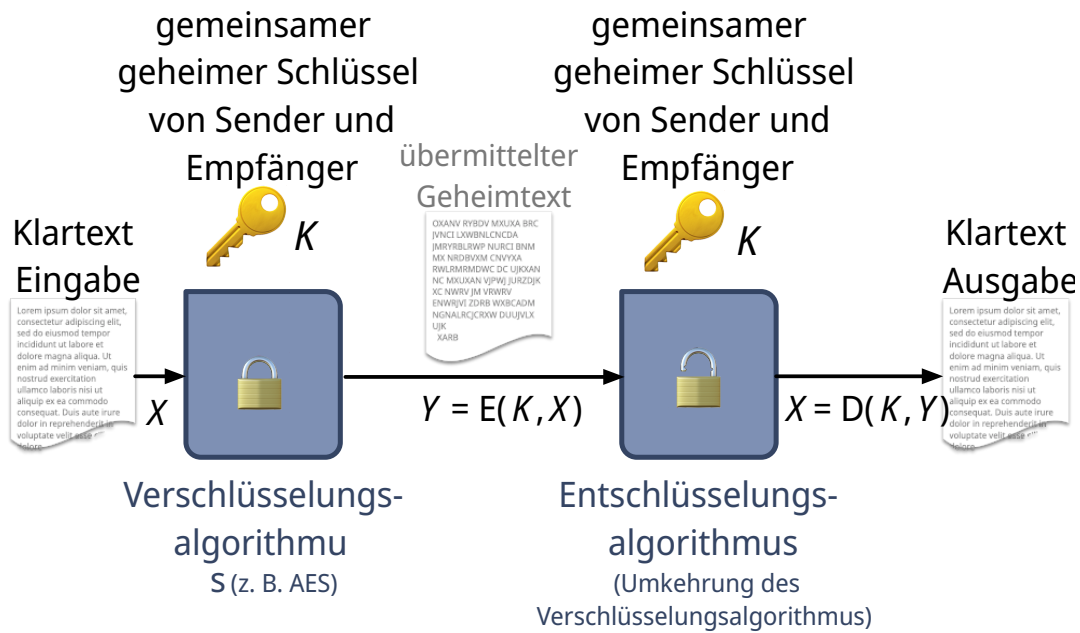
Methoden und Techniken, die zur Gewinnung von Informationen aus einer verschlüsselten Nachricht dienen.

Analyse von kryptographischen Verfahren.

Kryptologie:  *Cryptology*

Die Bereiche Kryptographie und Kryptoanalyse.

Vereinfachtes Modell der symmetrischen Verschlüsselung

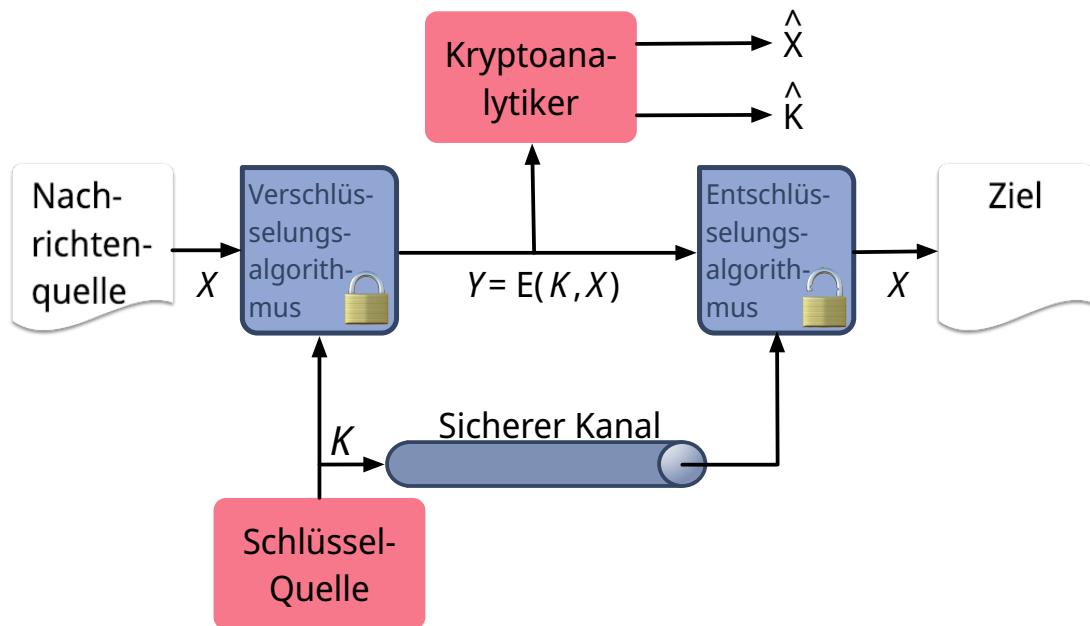


Symmetrisches Verschlüsselungsmodell

Es gibt zwei Voraussetzungen für die sichere Verwendung der herkömmlichen Verschlüsselung:

1. Ein starker Verschlüsselungsalgorithmus.
2. Effektive Schlüsselverwaltung:
 - a. Sender und Empfänger müssen Kopien des geheimen Schlüssels auf sichere Weise erhalten haben und
 - b. den Schlüssel sicher aufbewahren.

Modell eines symmetrischen Kryptosystems




Kryptografische Systeme können entlang dreier unabhängiger Dimensionen charakterisiert werden

1. Die Art der Operationen, die zur Umwandlung von Klartext in Chiffretext verwendet werden.

- Substitution
- Transposition (Vertauschungen)

Bemerkung

Eine Permutation ist eine Folge von Vertauschungen ( *Transposition*).

2. Die Anzahl der verwendeten Schlüssel.

Symmetrisch: Ein-Schlüssel-, **Secret-Key**-, konventionelle Verschlüsselung Asymmetrisch: Zwei-Schlüssel- oder **Public-Key**-Verschlüsselung

3. Die Art und Weise, in der der Klartext verarbeitet wird:

- Blockchiffre
- Stromchiffre

Kryptoanalyse und Brute-Force-Angriff

Kryptoanalyse

- Der Angriff beruht auf der Art des Algorithmus und einer gewissen Kenntnis der allgemeinen Merkmale des Klartextes.
- Der Angriff nutzt die Eigenschaften des Algorithmus aus, um zu versuchen, einen bestimmten Klartext zu entschlüsseln oder den verwendeten Schlüssel zu ermitteln.

Brute-force Angriff (*brachiale Gewalt*)

- Der Angreifer probiert jeden möglichen Schlüssel an einem Stück Chiffretext aus, bis er eine verständliche Übersetzung in Klartext erhält.
- Im Durchschnitt muss die Hälfte aller möglichen Schlüssel ausprobiert werden, um Erfolg zu haben.

Klassifizierung von Angriffen

| Art des Angriffs | dem Kryptoanalytiker bekannt |
|--------------------------|---|
| Ciphertext Only | <ul style="list-style-type: none">■ Verschlüsselungsalgorithmus und Chiffretext |
| Known Plaintext | <ul style="list-style-type: none">■ Verschlüsselungsalgorithmus und Chiffretext■ ein oder mehrere Klartext-Chiffretext-Paare, die mit dem geheimen Schlüssel verschlüsselt wurden |
| Chosen Plaintext | <ul style="list-style-type: none">■ Verschlüsselungsalgorithmus und Chiffretext■ Klartextnachricht, die vom Kryptoanalytiker gewählt wurde, zusammen mit dem zugehörigen Chiffretext, der mit dem geheimen Schlüssel verschlüsselt wurde. |
| Chosen Ciphertext | <ul style="list-style-type: none">■ Verschlüsselungsalgorithmus und Chiffretext■ Chiffretext, der vom Kryptoanalytiker gewählt wurde, zusammen mit dem zugehörigen entschlüsselten Klartext, der mit dem geheimen Schlüssel entschlüsselt wurde. |
| Chosen Text | <ul style="list-style-type: none">■ Verschlüsselungsalgorithmus und Chiffretext■ vom Kryptoanalytiker gewählte Klartextnachricht, zusammen mit dem zugehörigen Chiffretext, der mit dem geheimen Schlüssel verschlüsselt wurde.■ vom Kryptoanalytiker gewählter Chiffretext zusammen mit dem entsprechenden entschlüsselten Klartext, der mit dem geheimen Schlüssel erzeugt wurde. |

Sicherheit von Verschlüsselungsschemata

Bedingungslos Sicher (🚩 *Unconditionally Secure*)

- Unabhängig davon wie viel Zeit ein Gegner hat, ist es ihm unmöglich, den Geheimtext zu entschlüsseln, weil die erforderlichen Informationen nicht vorhanden sind.

Rechnerisch Sicher (🚩 *Computationally Secure*)

- Die Kosten für das Brechen der Chiffre übersteigen den Wert der verschlüsselten Informationen.
- Die zum Knacken der Chiffre benötigte Zeit übersteigt die Lebensdauer der Informationen.

? Frage

Wie lange könnte der Nutzen einer bestimmten Information andauern?

Brute-Force Angriff

- Es werden alle möglichen Schlüssel ausprobiert, bis eine verständliche Übersetzung des Chiffriertextes in Klartext erreicht wird.
- Im Durchschnitt muss die Hälfte aller möglichen Schlüssel ausprobiert werden, um Erfolg zu haben.
- Zur Durchführung des Brute-Force-Ansatzes ist ein gewisses Maß an Wissen über den zu erwartenden Klartext erforderlich. Es werden Mittel zur automatischen Unterscheidung von Klartext und „Müll“ benötigt.

? Frage

Was bedeutet somit *bis eine verständliche Übersetzung des Chiffriertextes in Klartext erreicht wird*? Wenn der Klartext zum Beispiel ein Bild, ein Video oder ein Computerprogramm ist?

Substitutionsverfahren

- Bei der Substitution werden die Buchstaben des Klartextes durch andere Buchstaben oder durch Zahlen oder Symbole ersetzt.
- Wenn der Klartext als eine Folge von Bits betrachtet wird, beinhaltet die Substitution das Ersetzen von Bitmustern des Klartextes durch Bitmuster des Geheimtextes.

Caesar Cipher

- Einfachste und früheste bekannte Verwendung einer Substitutions-Chiffre; verwendet von Julius Cäsar.
- Dabei wird jeder Buchstabe des Alphabets durch einen Buchstaben ersetzt, der drei Stellen weiter hinten im Alphabet steht.
- Am Ende des Alphabets wird wieder am Anfang begonnen. Somit folgt auf den Buchstabe Z der Buchstabe A.

| | |
|------------------|------------------------------|
| unverschlüsselt: | meet me after the toga party |
| verschlüsselt: | PHHW PH DIWHU WKH WRJD SDUWB |

Cäsar-Chiffre - historische Verwendung

Die Transformation kann wie folgt ausgedrückt werden:

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| 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 |
| 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 |

Mathematisch, wenn wir jedem Buchstaben einen Wert zuweisen:

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| 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 |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Der Algorithmus zur Verschlüsselung ist dann (p ist der Wert des zu verschlüsselnden Buchstabens):

$$Y = E(3, p) = (p + 3) \bmod 26$$

Verallgemeinerter Cäsar-Chiffre-Algorithmus

Eine Verschiebung kann beliebig groß sein (k), so dass der allgemeine Caesar-Algorithmus lautet:

$$Y = E(k, p) = (p + k) \bmod 26$$

Wobei k einen Wert im Bereich von 1 bis 25 annimmt; der Entschlüsselungsalgorithmus ist einfach:

$$p = D(k, C) = (Y - k) \bmod 26$$

Brute-Force-Kryptoanalyse der Caesar-Chiffre

| Key | PHHW | PH | DIWHU | WKH | WRJD | SDUWB |
|-----|------|-----|-------|-----|------|-------|
| 1 | OGGV | OG | CHVGT | VJG | VQIC | RCTVA |
| 2 | NFFU | NF | BGUFS | UIF | UPHB | QBSUZ |
| 3 | MEET | ME | AFTER | THE | TOGA | PARTY |
| 4 | LDDS | LD | ZESDQ | SGD | SNFZ | OZQSX |
| 5 | KCCR | KC | YDRCP | RFC | RMEY | NYPRW |
| 6 | JBBQ | JB | XCQBO | QEB | QLDX | MXOQV |
| 7 | IAAP | IA | WBPAN | PDA | PKCW | LWNPU |
| 8 | HZZO | HZ | VAOZM | OCZ | OJBV | KVMOT |
| 9 | GYYN | GY | UZNYL | NBY | NIAU | JULNS |
| 10 | FXXM | FX | TYMXK | MAX | MHZT | ITKMR |
| 11 | EWWL | EW | SXLWJ | LZW | LGYS | HSJLQ |
| 12 | DVVK | DV | RWKVI | KYV | KFXR | GRIKP |
| 13 | CUUJ | CU | QVJUH | JXU | JEWQ | FQHJO |
| ... | ... | ... | ... | ... | ... | ... |
| 25 | QIIX | QI | EJXIV | XLI | XSKE | TEVXC |

Brute-Force-Kryptoanalyse (z. B. der Caesar-Chiffre)

Die Entschlüsselung ist komplizierter, wenn der Klartext bereits eine sehr hohe Entropie aufweist, wie z. B. im Falle einer komprimierten ZIP Datei:

| | | | | | | | | | |
|-----------|------|------|------|------|------|------|------|------|--------------------|
| 00000000: | 504b | 0304 | 1400 | 0000 | 0800 | afb1 | 4257 | 1da9 | PK.....BW.. |
| 00000010: | b0b9 | 4b00 | 0000 | 4f04 | 0000 | 0800 | 1c00 | 6465 | ..K...O.....de |
| 00000020: | 6d6f | 2e74 | 7874 | 5554 | 0900 | 036a | 241b | 65a4 | mo.txtUT...j\$.e. |
| 00000030: | a9c0 | 6575 | 780b | 0001 | 04f8 | 0100 | 0004 | 1400 | ..eux..... |
| 00000040: | 0000 | edcc | db09 | 8030 | 0c05 | d07f | a7c8 | 049d |0..... |
| 00000050: | a28b | c4f6 | 6203 | e983 | 18d0 | 6e2f | ee91 | ffc3 |b.....n/.... |
| 00000060: | c928 | b697 | cb1c | 2437 | f569 | a032 | fb52 | 29ec | . (....\$7.i.2.R). |
| 00000070: | a8f4 | 340c | f206 | 5aca | 321c | afff | 8cd5 | c075 | ..4...Z.2.....u |
| 00000080: | d3c5 | 762a | d291 | 2389 | 2492 | 48d2 | 0750 | 4b01 | ..v*...#\$.H..PK. |
| 00000090: | 021e | 0314 | 0000 | 0008 | 00af | b142 | 571d | a9b0 |BW... |
| 000000a0: | b94b | 0000 | 004f | 0400 | 0008 | 0018 | 0000 | 0000 | .K...O..... |
| 000000b0: | 0001 | 0000 | 00ff | 8100 | 0000 | 0064 | 656d | 6f2e |demo. |
| 000000c0: | 7478 | 7455 | 5405 | 0003 | 6a24 | 1b65 | 7578 | 0b00 | txtUT...j\$.eux.. |
| 000000d0: | 0104 | f801 | 0000 | 0414 | 0000 | 0050 | 4b05 | 0600 |PK... |
| 000000e0: | 0000 | 0001 | 0001 | 004e | 0000 | 008d | 0000 | 0000 |N..... |
| 000000f0: | 00 | | | | | | | | |

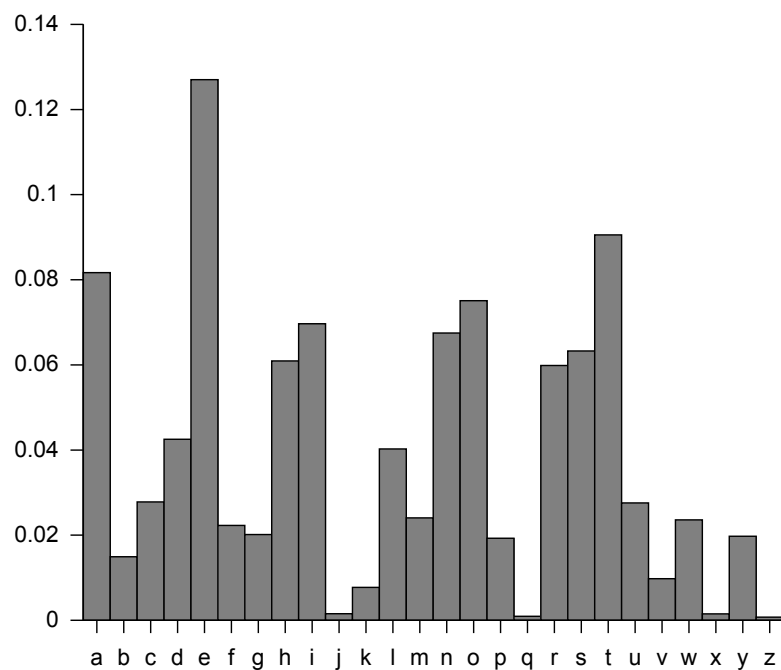
? Frage

Wie kann man - wenn man weiss, dass es sich um eine ZIP Datei handelt - die Caesar-Chiffre knacken?

Monoalphabetische Chiffren

- Eine Permutation einer endlichen Menge von Elementen S ist eine geordnete Folge aller Elemente von S , wobei jedes Element genau einmal vorkommt.
- Wenn die „Chiffre“-Zeile (siehe Cäsar-Chiffre) eine beliebige Permutation der 26 alphabetischen Zeichen sein kann, dann gibt es $26!$ oder mehr als 4×10^{26} mögliche Schlüssel.
 - Dies ist um 10 Größenordnungen größer als der Schlüsselraum für DES!
 - Der Ansatz wird als monoalphabetische Substitutions-Chiffre bezeichnet, da pro Nachricht ein einziges Chiffre-Alphabet verwendet wird.

Häufigkeit der englischen Buchstaben [1]



[1] Analyse des Concise Oxford Dictionary (9th edition, 1995) — <https://www.nd.edu>

Angriffe auf Monoalphabetische Chiffren

Sie sind leicht zu knacken, da sie die Häufigkeitsdaten des ursprünglichen Alphabets widerspiegeln.

Die Gegenmaßnahme besteht darin, mehrere Substitute (Homophone) für einen einzigen Buchstaben anzubieten.

Playfair Cipher

Erfunden vom britischen Wissenschaftler Sir Charles Wheatstone im Jahr 1854.

- Bekannteste Chiffrierung mit mehreren Buchstaben.
- Behandelt Digramme im Klartext als einzelne Einheiten und übersetzt diese Einheiten in Digramme des Geheimtextes.
- Basiert auf der Verwendung einer 5 x 5 Buchstabenmatrix, die mit Hilfe eines Schlüsselworts konstruiert wird.
- Wurde von der britischen Armee im Ersten Weltkrieg und von der US-Armee und anderen alliierten Streitkräften im zweiten Weltkrieg als Standardfeldsystem verwendet.

Bemerkung

Digram

- Zwei-Buchstaben-Kombination
- am häufigsten im Englischen: "th"

Trigram

- Drei-Buchstaben-Kombination
- am häufigsten im Englischen: "the"

Playfair Key Matrix

Füllen Sie die Buchstaben des Schlüsselworts (abzüglich der Duplikate) von links nach rechts und von oben nach unten aus, dann füllen Sie den Rest der Matrix mit den restlichen Buchstaben in alphabetischer Reihenfolge aus. Die Buchstaben I und J zählen als ein Buchstabe.

Sei das Schlüsselwort MONARCHY:

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

Playfair Verschlüsselung

Die Verschlüsselung wird für jedes Buchstabenpaar des Klartextes durchgeführt.

1. Wenn beide Buchstaben gleich sind (oder nur ein Buchstabe übrig ist), fügen Sie ein "X" hinter dem ersten Buchstaben ein.
Verschlüsseln Sie das neue Paar und fahren Sie fort. (Z. B. würde statt "ballon" "ba lx lo nX" verschlüsselt werden.)
2. Wenn die Buchstaben in der gleichen Zeile stehen, ersetzen Sie sie durch die Buchstaben unmittelbar rechts davon (ggf. umbrechen).
(Z. B. wird *ar* als *RM* verschlüsselt.)
3. Tauchen die Buchstaben in derselben Spalte auf, so sind sie durch die unmittelbar darunter liegenden Buchstaben zu ersetzen (ggf. umbrechen). (Z. B. wird "mu" als "CM" verschlüsselt.)
4. Befinden sich die Buchstaben nicht in derselben Zeile oder Spalte, so werden sie durch die Buchstaben in derselben Zeile bzw. in dem anderen Paar von Ecken des durch das ursprüngliche Paar definierten Rechtecks ersetzt. (Z. B. wird *hs* als *BP* und *ea* als *IM* verschlüsselt.)

Bemerkung

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

Hill Chiffre

Entwickelt von dem Mathematiker Lester Hill im Jahr 1929.

- Die Stärke ist, dass die Häufigkeit von einzelnen Buchstaben vollständig ausgeblendet wird.
 - Durch die Verwendung einer größeren Matrix werden mehr Frequenzinformationen verborgen.
 - Eine 3 x 3 Hill-Chiffre verbirgt nicht nur die Häufigkeiten einzelner Buchstaben sondern auch von Digrammen.
- Stark gegen einen Angriff auf den Geheimtext, aber leicht zu brechen sobald ein Klartext vorliegt (*known plaintext attack*).

Polyalphabetische Chiffren

Polyalphabetische Substitutions-Chiffren verbessern einfache monoalphabetische Chiffren, indem sie verschiedene monoalphabetische Substitutionen verwenden, während man die Klartextnachricht verschlüsselt.

Bemerkung

Alle diese Techniken haben die folgenden Merkmale gemeinsam:

- Es wird ein Satz verwandter monoalphabetischer Substitutionsregeln verwendet.
- Ein Schlüssel bestimmt, welche bestimmte Regel für eine bestimmte Umwandlung gewählt wird.

Vigenère Chiffre

- Die bekannteste und eine der einfachsten polyalphabetischen Substitutions-Chiffren.
- In diesem Schema besteht die Menge der verwandten monoalphabetischen Substitutionsregeln aus den 26 Caesar-Chiffren mit Verschiebungen von 0 bis 25.
- Jede Chiffre wird durch einen Schlüsselbuchstaben identifiziert, der den Klartextbuchstaben durch den Chiffretextbuchstaben ersetzt.

Aufbau des Vigenère-Tableaus

- Kopfzeile: Klartextbuchstabe
- 1. Spalte: Schlüsselbuchstabe
- Tableau: Verschlüsselter Buchstabe

Beispiel

Nehmen wir an, der Schlüssel ist "D" und der Klartextbuchstabe sei "b". Dann ist der Chiffretextbuchstabe "E".

| / | 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 |

Beispiel einer Vigenère-Verschlüsselung

- Um eine Nachricht zu verschlüsseln, wird ein Schlüssel benötigt, der so lang ist wie die Nachricht.
- In der Regel ist der Schlüssel ein sich wiederholendes Schlüsselwort.

Beispiel

Wenn das Schlüsselwort `deceptive` ist, wird die Nachricht „Wir wurden entdeckt, rette dich“ wie folgt verschlüsselt:

Schlüssel: `DECEPTIVEDECEPTIVEDECEPTIVE`
Klartext: `wearediscoveredsaveyourself`
Geheimtext: `ZICVTWQNGRZGVTWAVZHCQYGLMGJ`

Vigenère *Autokey* System

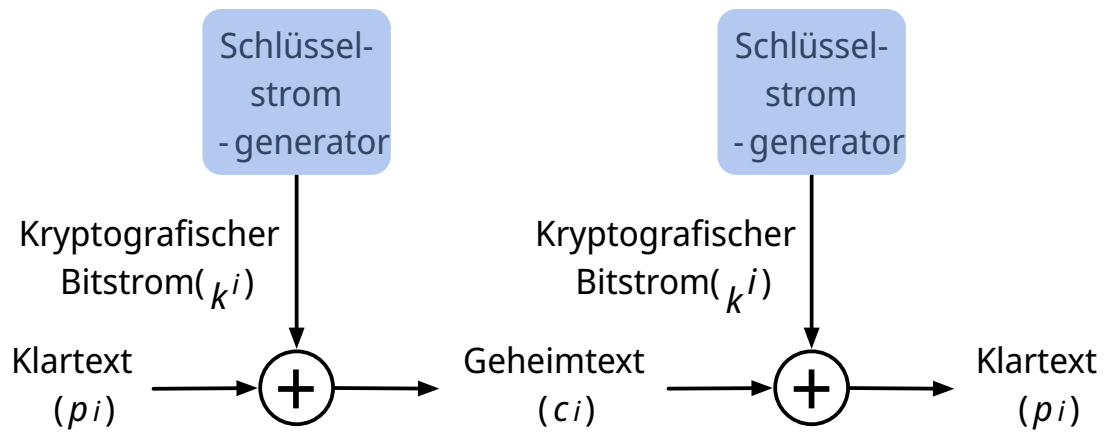
Ein Schlüsselwort wird mit dem Klartext selbst verkettet, um einen laufenden Schlüssel zu erhalten.

Beispiel

| | |
|-------------------|-----------------------------|
| Schlüssel | DECEPTIVEwearediscoveredsav |
| Klartext | wearediscoveredsaveyourself |
| Geheimtext | ZICVTWQNGKZEIIGASXSTSLVVWLA |

Auch dieses Verfahren ist anfällig für eine Kryptoanalyse, da der Schlüssel und der Klartext die gleiche Häufigkeitsverteilung der Buchstaben aufweisen und eine statistische Technik angewendet werden kann.

Vernam Chiffre



One-Time Pad

- Verbesserung der Vernam-Chiffre, vorgeschlagen von dem Offizier Joseph Mauborgne des Army Signal Corp.
- Verwendung eines Zufallsschlüssels, der so lang wie die Nachricht ist, so dass der Schlüssel nicht wiederholt werden muss.
- Der Schlüssel wird zum Ver- und Entschlüsseln einer einzigen Nachricht verwendet und dann verworfen.
- Jede neue Nachricht erfordert einen neuen Schlüssel mit der gleichen Länge wie die neue Nachricht.
- Das Schema ist nachweislich nicht zu knacken.
 - Erzeugt eine zufällige Ausgabe, die in keinem statistischen Zusammenhang mit dem Klartext steht.
 - Da der Chiffriertext keinerlei Informationen über den Klartext enthält, gibt es keine Möglichkeit, den Code zu knacken.

Schwierigkeiten von One-Time-Pads

- Das One-Time-Pad bietet vollständige Sicherheit, hat aber in der Praxis zwei grundlegende Schwierigkeiten:
 1. Es gibt das praktische Problem der Herstellung großer Mengen von Zufallsschlüsseln.
Jedes stark genutzte System könnte regelmäßig Millionen von zufälligen Zeichen benötigen.
 2. Ein „gigantisches“ Schlüsselverteilungsproblem
Für jede zu übermittelnde Nachricht benötigen Sender und Empfänger einen gleich langen Schlüssel.
- Aufgrund dieser Schwierigkeiten ist das One-Time-Pad nur von begrenztem Nutzen; es eignet sich vor allem für Kanäle mit geringer Bandbreite, die eine sehr hohe Sicherheit erfordern.
- Das One-Time-Pad ist das einzige Kryptosystem, das eine perfekte Geheimhaltung bietet.

Rail Fence Chiffre

- Einfachste Transpositions-Chiffre (d. h. Chiffre basierend auf *Vertauschung*).
- Der Klartext wird als eine Folge von Diagonalen aufgeschrieben und dann als eine Folge von Zeilen abgelesen.

Beispiel

Um die Nachricht: „Meet me after the Toga-Party“ mit einer Rail Fence Chiffre der Tiefe 2 (Schlüssel) zu verschlüsseln, würden wir schreiben:

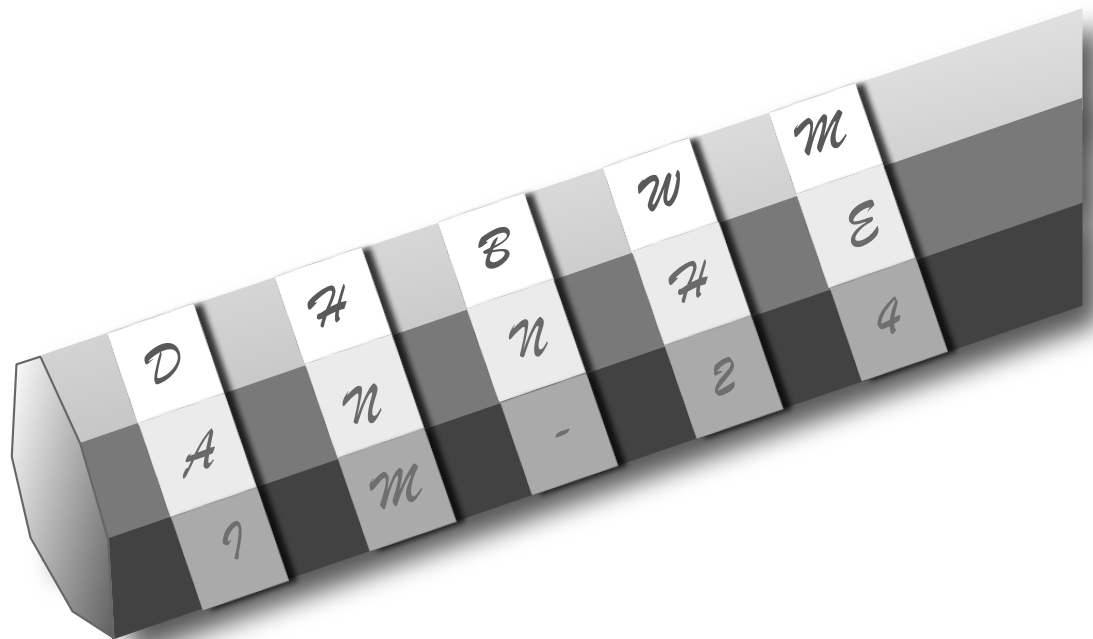
```
m e m a t r h t g p r y  
e t e f e t e o a a t
```

Die verschlüsselte Nachricht ist: MEMATRHTGPRYETEFETEOAAT

Um die Nachricht zu entschlüsseln, wird die Nachricht in K Zeilen geschrieben und dann in einer Diagonalen abgelesen. Die Länge einer Zeile ergibt sich aus der Länge der Nachricht (L) und der Tiefe der Chiffre (K): $\lfloor L/K \rfloor$. Wobei die ersten $L \bmod K$ Zeilen um eins länger sind als die anderen.

Skytale

- Ältestes bekannte (militärische) Verschlüsselungsverfahren.
- Vor mehr als 2500 Jahren (vermutlich) von den Spartanern entwickelt.
- Die Verschlüsselung erfolgte mit einem (Holz-)Stab mit einem bestimmten Durchmesser („Schlüssel“) (Skytale).



Zeilenverschiebungs-Chiffre

- Ist eine komplexere Transposition.
- Schreiben Sie die Nachricht zeilenweise in ein Rechteck mit wohldefinierter Breite und lesen Sie die Nachricht spaltenweise ab, aber vertauschen Sie die Reihenfolge der Spalten.
- Die Reihenfolge der Spalten ist dann der Schlüssel.

Beispiel

Verschlüsselung von *attack postpone until two am*

Schlüssel: 4312567

Klartext: attackp
ostpone
duntilt
woamxyz

Geheimtext: TTNA APTM TSUO AODW COIX KNLY PETZ
(Spalte: 3--- 4--- 2--- 1--- 5--- 6--- 7---)

Zeilenverschiebungs-Chiffre $\hat{=}$ 🇬🇧 *Row Transposition Cipher*

Wenn der Schlüssel 4312567 ist, dann wird:

- die erste Spalte wird als die *vierte* (4),
- die zweite Spalte als die *dritte* (3),
- die dritte Spalte als die *erste* (1),
- ...

geschrieben

Beim Entschlüsseln ergibt sich die Anzahl der Reihen trivial aus der Länge der Nachricht (28 Zeichen) und der Länge des Schlüssels (7 Zeichen); $28/7 = 4$.

Steganografie - Beispiel

Dear Friend ; We know you are interested in receiving cutting-edge announcement . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail . This mail is being sent in compliance with Senate bill 1626 ; Title 4 , Section 305 . This is a legitimate business proposal ! Why work for somebody else when you can become rich in 96 months . Have you ever noticed nobody is getting any younger & nobody is getting any younger . Well, now is your chance to capitalize on this ! We will help you decrease perceived waiting time by 170% and use credit cards on your website ! You are guaranteed to succeed because we take all the risk ! But don't believe us . Mrs Anderson of Indiana tried us and says "I was skeptical but it worked for me" . We assure you that we operate within all applicable laws . You will blame yourself forever if you don't order now . Sign up a friend and you'll get a discount of 10% ! Thank-you for your serious consideration of our offer !

Mit Spammimic <https://www.spammimic.com/>, kann die Nachricht extrahiert werden.

Auswahl anderer Steganographie-Techniken

■ **Zeichenmarkierung**

Ausgewählte Buchstaben eines gedruckten oder maschinengeschriebenen Textes werden mit Bleistift überstrichen. Die Markierungen sind nur sichtbar, wenn das Papier schräg in helles Licht gehalten wird.

■ **Unsichtbare Tinte**

Es gibt eine Reihe von Substanzen, die zum Schreiben verwendet werden können, aber keine sichtbaren Spuren hinterlassen, solange das Papier nicht erhitzt oder mit einer chemischen Substanz behandelt wird.

■ **Nadelstiche**

Kleine Nadelstiche auf ausgewählten Buchstaben sind normalerweise nicht sichtbar, es sei denn, das Papier wird vor ein Licht gehalten.

■ **Sehr helle Tinte**

Druckerhersteller drucken winzige Punktmuster in sehr hellen Farben auf die Seiten. Dies erlaubt es Dokumente zu dem Drucker zurückzuverfolgen, auf dem sie gedruckt wurden.

Steganographie vs. Verschlüsselung

- Steganografie hat eine Reihe von *Nachteilen* im Vergleich zur Verschlüsselung:
 - ! Es erfordert einen hohen Overhead, um relativ wenige Bits an Informationen zu verbergen.
 - ! Sobald das System entdeckt wird, wird es praktisch wertlos.
- Der *Vorteil* der Steganografie:
 - ✓ Sie kann von Parteien eingesetzt werden, die etwas zu verlieren haben, wenn die Tatsache ihrer geheimen Kommunikation (nicht unbedingt der Inhalt) entdeckt wird.
 - ✓ Verschlüsselung kennzeichnet den Verkehr als wichtig oder geheim oder kann den Sender oder Empfänger als jemanden identifizieren, der etwas zu verbergen hat.

Übung

0.1. Playfair Chiffre

Entschlüsseln Sie: XGAWMGAZ. Das Passwort ist MONARCHY (wie auf den Folien.)

0.2. Vigenère Chiffre

Sie haben das folgende Klartext-Chiffretext-Paar:

P: `secret`

C: `HSFGSW`

1. Wie ist der Schlüssel?
2. Welche Art von Angriff haben Sie durchgeführt?

Übung

0.3. Rail-fence Chiffre

Entschlüsseln Sie: ggettueietmsr

0.4. Rail-fence Chiffre

Verschlüsseln Sie "i love crypto" mit dem Schlüssel/der Tiefe 3.

Übung

0.5. Zeilenverschiebungs-Chiffre

Sie haben die folgende Nachricht erhalten:

YSFRITTUNCOSPJU

Außerdem konnten Sie den Schlüssel bis auf einen Wert ermitteln: 4153.

- Wie viele Entschlüsselungsmöglichkeiten gibt es (noch)?
- Bestimmen Sie den richtigen Schlüssel und entschlüsseln Sie den Text?

0.6. Eigenschaften von Chiffren

1. Wie unterscheiden sich Transpositions- und Substitutions-Chiffren?
2. Handelt es sich bei Monoalphabetischen Chiffren um Transpositions- oder Substitutions-Chiffren?
3. Kann man Transpositions- und Substitutions-Chiffren kombinieren?