# Einführung in Kryptologie

## Kryptologie IL (Vorlesungsteil)

Andreas Unterweger

Studiengang ITS
FH Salzburg

Sommersemester 2023

# Überblick

- Kryptologie umfasst **Kryptografie** und Kryptoanalyse (später)
- Was ist Kryptografie?
  - Definition laut Wörterbuch[1]: „Geheimschrift“ *(vom Griechischen kryptós mit der Bedeutung „versteckt“ oder „geheim“, und gráphein mit der Bedeutung „schreiben“)*
  - Modern (breitere Definition): „Wissenschaft bzw. Technik der Verschlüsselung und Entschlüsselung von Daten”
- Ziele
  - Historisch: Geheime Kommunikation (Chiffren entwickeln und brechen)
  - Authentifizierung (z.B. digitale Signaturen)
  - Geheimnis-/Schlüsselverwaltung
  - Beweise von Sicherheit

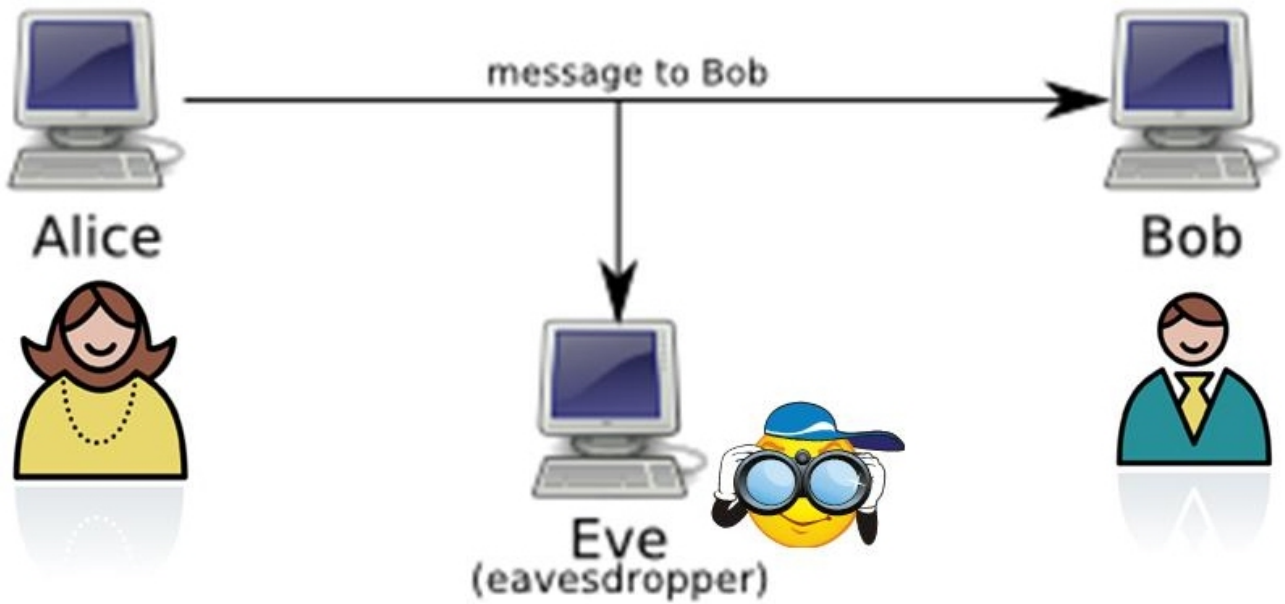
...

[1] Landesinstitut für Schule und Medien Berlin-Brandenburg: Kryptologie - Unterrichtsmaterial. `https://bildungsserver.berlin-brandenburg.de/kryptologie` (Zugriff am 6.12.2022), 2022.

[1] `https://www.dwds.de/wb/Kryptographie` (Zugriff am 6.12.2022)

# Akteure in der klassischen Kryptologie

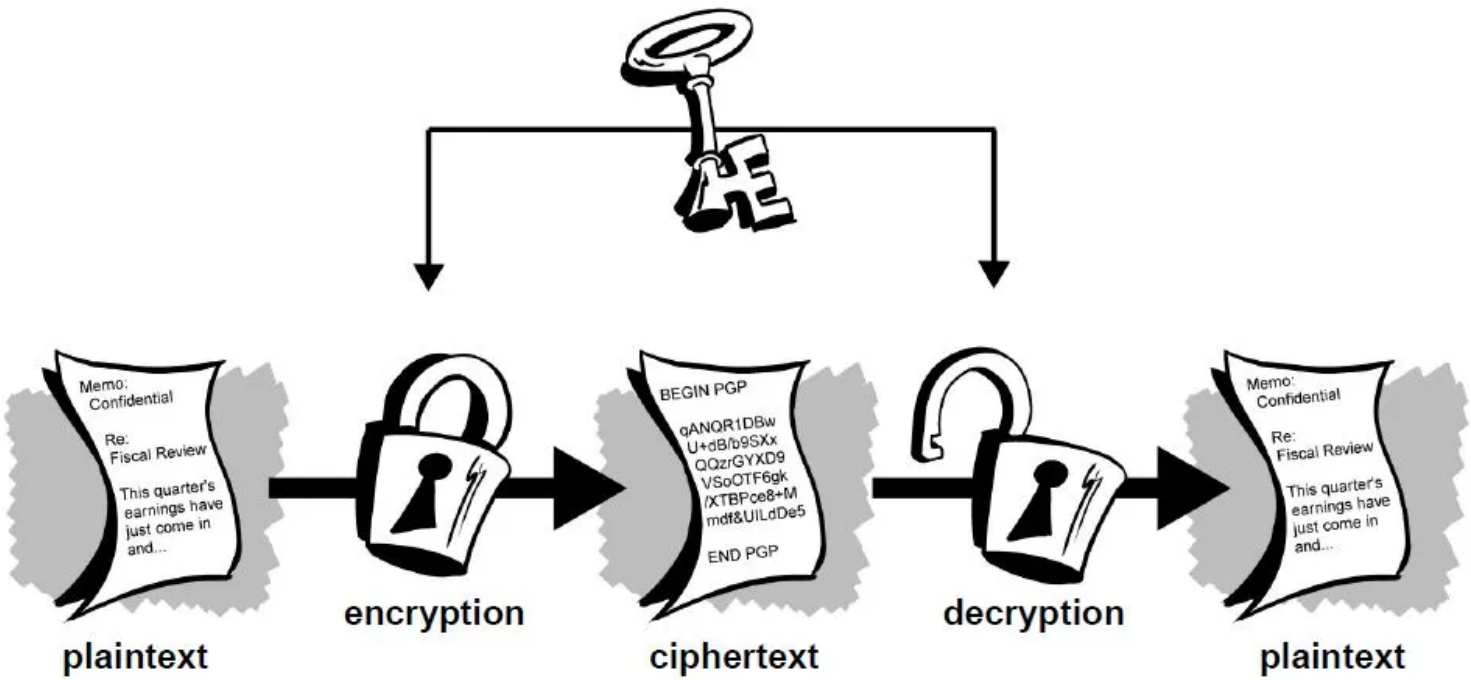
- Situation: Geheime Kommunikation
- Traditionelle Benennung von Akteuren
  - Alice: Absender der Nachricht/des Geheimnisses
  - Bob: Empfänger der Nachricht/des Geheimnisses
  - Eve (Lauscher, von engl. eavesdropper) möchte zuhören/abfangen




Quelle: CS110 staff: Encryption and Security.
`https://cs.wellesley.edu/~cs110/reading/cryptography-files/handoutPrint.html` (Zugriff am 16.8.2022), 2014.

# Begriffe in der klassischen Kryptologie I

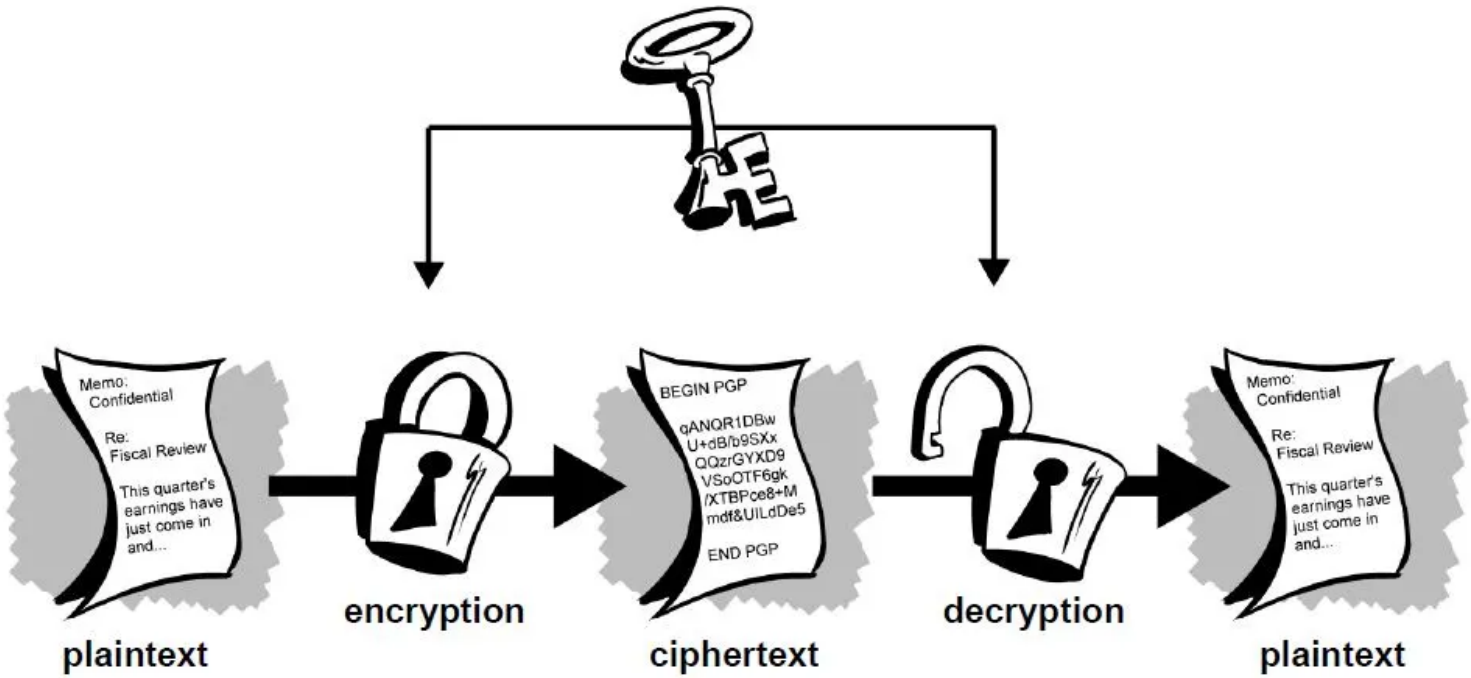
- Klartext (engl. plaintext) $m$: Originalnachricht (engl. message)
- Chiffretext (engl. ciphertext) $c$: Verschlüsselte Nachricht
- Schlüssel $k$: Geheime Information




Quelle: Pacia, C.: Beginners' Guide To Off-the-Record Messaging. `https://www.bitcoinnotbombs.com/beginners-guide-to-off-the-record-messaging/` (Zugriff am 16.8.2022), 2014.

# Begriffe in der klassischen Kryptologie II

- Verschlüsselung(-sfunktion) $E(k, m)$: Wandelt eine Klartextnachricht in einen Chiffretext um, d.h., $c := E(k, m)$
- Entschlüsselung(-sfunktion) $D(k, c)$: Wandelt einen Chiffretext zurück in seinen Klartext um, d.h., $D(k, c) \stackrel{!}{=} m$




Quelle: Pacia, C.: Beginners' Guide To Off-the-Record Messaging. `https://www.bitcoinnotbombs.com/beginners-guide-to-off-the-record-messaging/` (Zugriff am 16.8.2022), 2014.

# Arten von Chiffren

- Schlüsselsymmetrie
  - Symmetrische Kryptografie (engl. secret key cryptography): Verwendet denselben Schlüssel zur Ver- und Entschlüsselung
  - Asymmetrische Kryptografie (engl. public key cryptography): Verwendet verschiedene Schlüssel zur Ver- und Entschlüsselung
- Eingabe/Ausgabe
  - Blockchiffre: Verarbeitet Daten in Blöcken von z.B. mehreren Bytes
  - Stromchiffre: Verarbeitet Daten zeichenweise (oder Bit für Bit)
- Zusätzliche Kategorisierung, z.B. Substitutionschiffren (ersetzen umkehrbar Zeichen durch andere Zeichen)
  - Monoalphabetisch: Zeichen werden mittels eines einzigen Alphabets ersetzt
  - Polyalphabetisch: Zeichen werden mittels mehrerer Alphebete ersetzt

[2] Robshaw, M. J. B.: Stream Ciphers – RSA Laboratories Technical Report TR-701. `http://www.networkdls.com/Articles/tr-701.pdf` (Zugriff am 18.8.2022), 1995.

# Sicherheitsannahmen

- Perfekte Sicherheit gibt es in der Praxis nicht
  - Manche Personen benötigen Zugriff (inhärentes Risiko)
  - Menschlicher Faktor ist Risiko zusätzlich zu technischen Aspekten
  - Jedes System ist nur so stark wie sein schwächstes Glied
  - Bedrohungsmodell: Sicherheit nur gegen bestimmte Angriffe $\rightarrow$ Wie mächtig ist der Angreifer (angenommenerweise)?
- Prinzipien moderner Kryptografie
  - Präzise (formalisierte) Sicherheitsdefinition
  - Wenn eine Annahme (z.B. eine bestimmte Operation ist schwierig) nicht bewiesen werden kann, muss sie angegeben, gut untersucht und so minimal wie möglich sein
  - Gründliche Beweise (außerhalb des Umfangs dieser Lehrveranstaltung): Die Sicherheit einer Chiffre oder eines kryptografischen Systems auf eine wahr geglaubte Annahme reduzieren

# Kerckhoffsches Prinzip

- Die Sicherheit einer Chiffre
  - hängt nur von der Geheimhaltung des Schlüssels ab
  - darf **nicht** darauf basieren, dass die Chiffre/der Algorithmus geheim ist
- Argumentation
  - (Kurze) Schlüssel sind leichter geheim zu halten als (komplexe) Algorithmen
  - Exponierte Schlüssel sind leichter zu ersetzen als gebrochene Chiffren
  - es ist einfacher, verschiedene Personen verschiedene Schlüssel benutzen zu lassen als verschiedene Chiffren
- Konsequenz: Moderne Chiffren/Algorithmen sind öffentlich
  - Vereinfachte Standardisierung
  - Experten können Schwachstellen bewerten

  $\rightarrow$ Stärkeres Vertrauen und wahrscheinlichere Meldung von Schwachstellen

# Die Vernam-Chiffre I

- Auch engl. one-time pad (OTP) genannt
- Liest Binärstrings konstanter Länge ein/gibt diese aus
- $E(k, m) := k \oplus m$, wobei $\oplus$ bitweises Exklusiv-Oder bezeichnet
- $D(k, c) := k \oplus c$ (gleich wie Verschlüsselung)

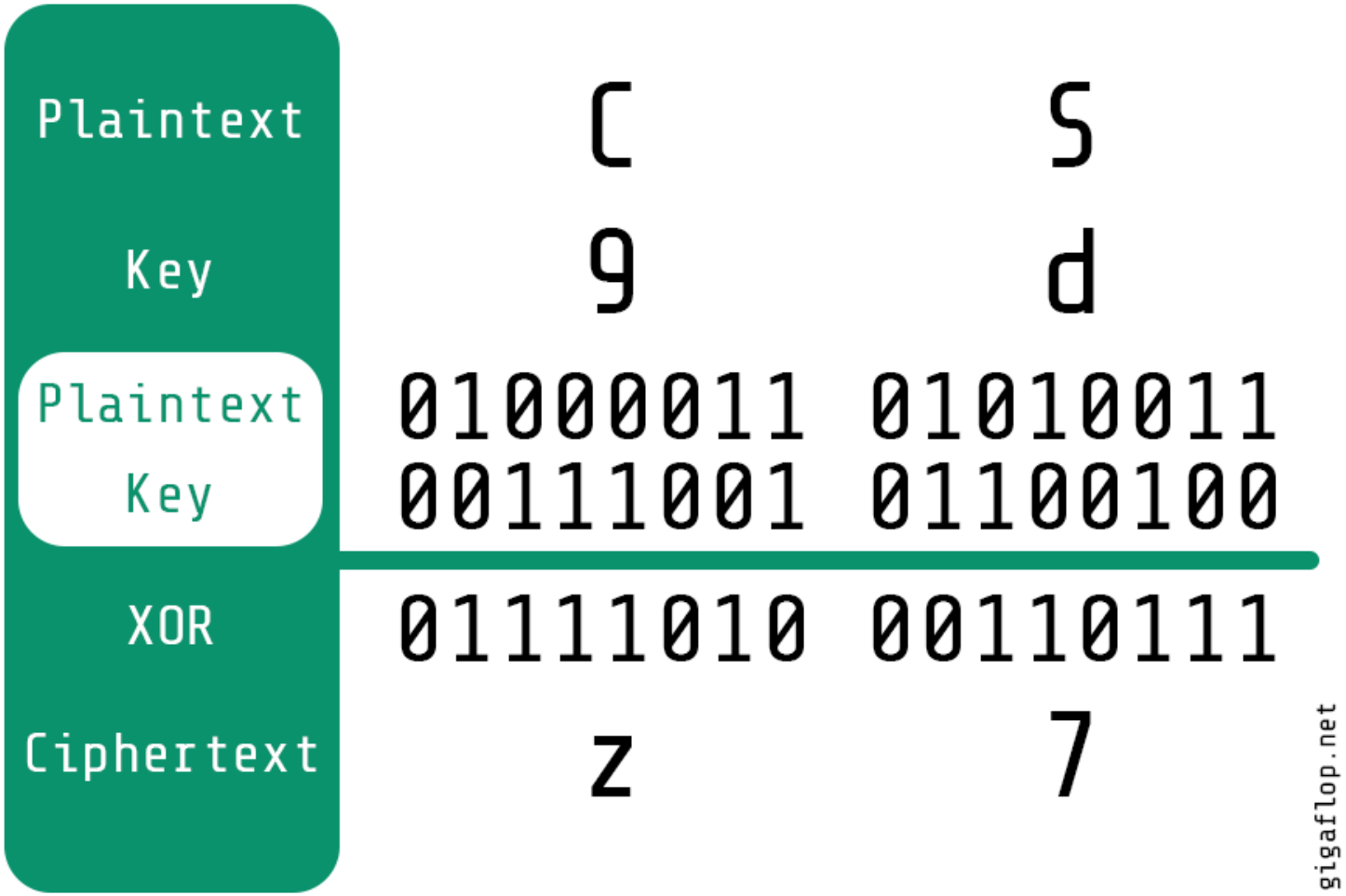
$\rightarrow D(k, E(k, m)) = k \oplus (k \oplus m) = (k \oplus k) \oplus m = 0 \oplus m \stackrel{!}{=} m$

- Beweisbar sicher, wenn
  - Nachricht $m$ und Schlüssel $k$ **genau** die gleiche Länge haben
  - ein Schlüssel **nie** wiederverwendet wird
  - der Schlüsselbitstring gleichverteilt ist (praktische Einschränkungen liegen außerhalb des Umfangs dieser Lehrveranstaltung)

$\rightarrow$ ansonsten kann ein Angreifer die perfekte Geheimhaltung brechen

- Chiffretext verrät nichts über den Klartext, da alle Klartexte bei einem zufälligen Schlüssel gleich wahrscheinlich sind; formaler Beweis in der Literatur

# Die Vernam-Chiffre II




Quelle: Gigaflop: Encryption. https://gigaflop.net/chapter/data-representation/encryption/ (Zugriff am 16.8.2022), 2022.

# Überblick über klassische Chiffren

- Klassische kryptografische Chiffren
  - In der Vergangenheit für geheime Kommunikation verwendet
  - Anfällig für verschiedene Arten von Angriffen

  $\rightarrow$ Nicht mehr sicher (nicht verwenden)
- Beispiele für klassische Chiffren
  - Caesar-Chiffre
  - Vigenère-Chiffre
  - Enigma
- Vereinfachtes (Nachrichten)-Alphabet
  - Zeichensatz: `A..Z` (nur Großbuchstaben, keine Kleinbuchstaben, keine Ziffern, keine Sonderzeichen)
  - Für Berechnungen: `A` entspricht 0, `B` entspricht 1, ..., `Z` entspricht 25

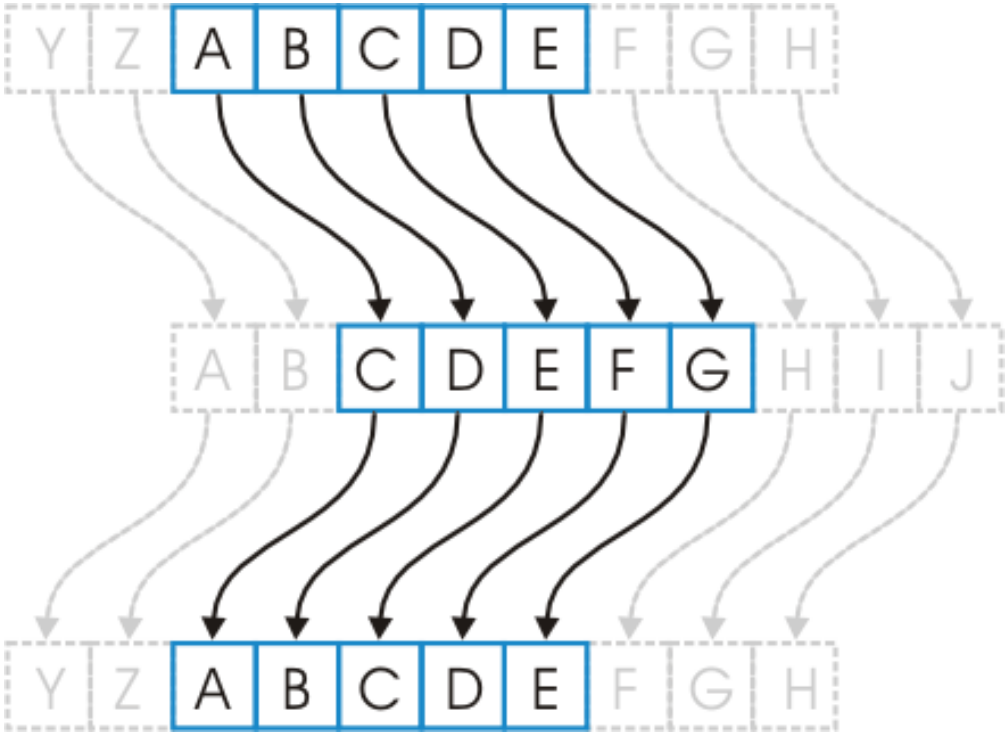
# Die Caesar-Chiffre I

- Idee: Alphabet um konstanten Versatz verschieben (mit Überlauf)

→ Verschlüsselung: Jedes Zeichen um den Versatz, z.B. 2, verschieben

→ Entschlüsselung: Jedes Zeichen um denselben Versatz zurückverschieben, z.B. $-2$

- Versatz ist der Schlüssel, z.B. $k = 2$ (C)




Quelle: Smith, J.: A functional implementation of the Caesar cipher in Swift. `https://github.com/ijoshsmith/swift-caesar-cipher` (Zugriff am 16.8.2022), 2015.

# Die Caesar-Chiffre II

- $E(k,m) := (m+k) \mod 26$
- $D(k,c) := (c-k) \mod 26$
- Zwei Beispiele mit $k = 2 \stackrel{\wedge}{=} \mathtt{C}$
- Beispiel 1 (kein Überlauf):
  - $m = 1 \stackrel{\wedge}{=} \mathtt{B}$
  - $c := E(k,m) = (m+k) \mod 26 = (1+2) \mod 26 = 3 \stackrel{\wedge}{=} \mathtt{D}$
  - $m \stackrel{!}{=} D(k,c) = (c-k) \mod 26 = (3-2) \mod 26 = 1 \stackrel{\wedge}{=} \mathtt{B}$
- Beispiel 2 (Überlauf):
  - $m = 25 \stackrel{\wedge}{=} \mathtt{Z}$
  - $c := E(k=2, m=25) = (25+2) \mod 26 = 27 \mod 26 = 1 \stackrel{\wedge}{=} \mathtt{B}$
  - $m \stackrel{!}{=} D(k=2, c=1) = (1-2) \mod 26 = -1 \mod 26 = 25 \stackrel{\wedge}{=} \mathtt{Z}$

# Die Caesar-Chiffre III

- Monoalphabetische Substitutionschiffre (Zeichen für Zeichen)
- Ver- und Entschlüsselung von Nachrichten mit mehreren Zeichen $m_i$:
  - $c_i := E(k, m_i) := (m_i + k) \mod 26$ für alle $i$
  - $m_i \stackrel{!}{=} D(k, c_i) = (c_i - k) \mod 26$ für alle $i$
- Beispiel: Verschlüsseln der Nachricht ZOO mit $k = 2 \stackrel{\wedge}{=} \mathtt{C}$
  - $m_0 = 25 \stackrel{\wedge}{=} \mathtt{Z}$
  - $m_1 = m_2 = 14 \stackrel{\wedge}{=} \mathtt{O}$
  - $c_0 := E(k = 2, m_0 = 25) = (25 + 2) \mod 26 = 27 \mod 26 = 1 \stackrel{\wedge}{=} \mathtt{B}$
  - $c_1 = c_2 := E(k = 2, m_2 = 14) = (14 + 2) \mod 26 = 16 \stackrel{\wedge}{=} \mathtt{Q}$

  $\rightarrow$ Verschlüsselte Nachricht (Chiffretext) BQQ

# Die Vigènere-Chiffre I

- Idee: Alphabet um positionsabhängigen Versatz verschieben (mit Überlauf), wiederholt in regelmäßigen Intervallen, sofern notwendig
- Für Einzelzeichen: Caesar-Chiffre mit positionsabhängigem Schlüssel

$\rightarrow$ Polyalphabetische Substitutionschiffre

- Schlüssellänge bestimmt, wie viele mögliche Verschiebungen/ positionsabhängige Schlüssel es gibt; Beispielcodetabelle für $k \triangleq$ `CODE`:

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **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 |
| **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 |
| **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** | 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 |

Quelle: Ibmathsresources.com: Crypto Analysis to Crack Vigenere Ciphers. `https://schoolcodebreaking.com/2015/06/18/crypto-analysis-to-crack-vigenere-ciphers/` (Zugriff am 16.8.2022), 2015.

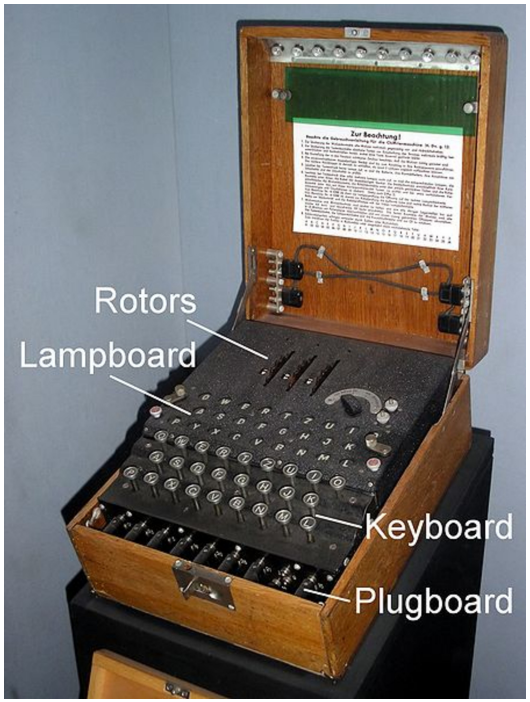
# Die Vigènere-Chiffre II

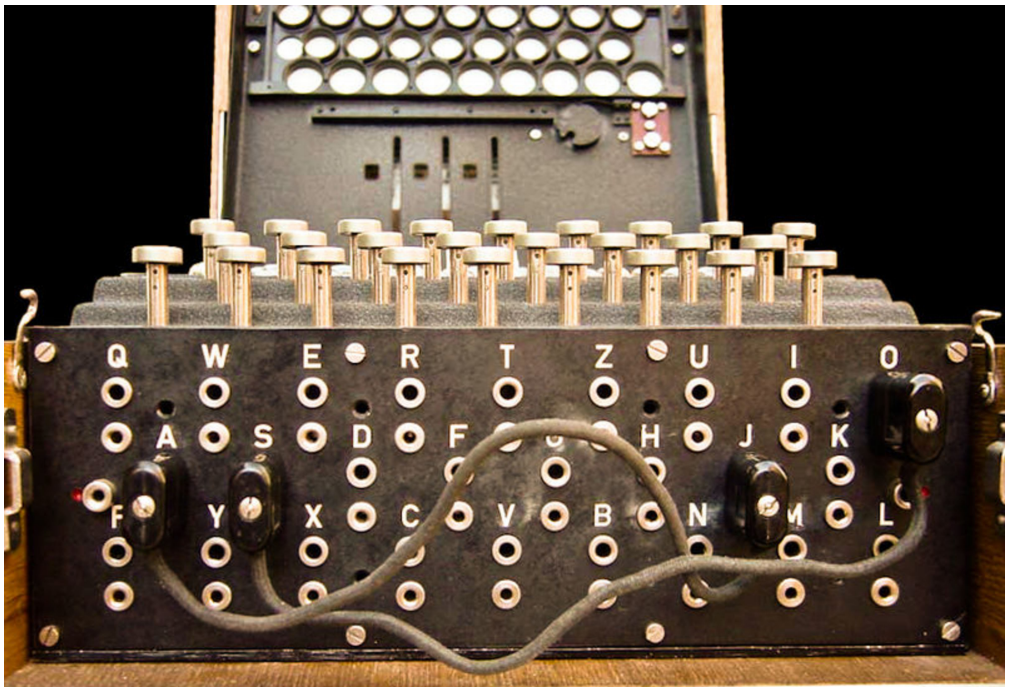
- $Vigenere(k, m_i) = Caesar(k_{i \bmod ||k||}, m_i)$, wobei $||\cdot||$ Länge bezeichnet
- $c_i := (m_i + k_{i \bmod ||k||}) \bmod 26$
- $m_i \stackrel{!}{=} (c_i - k_{i \bmod ||k||}) \bmod 26$
- Beispiel: Verschlüsseln der Nachricht TESTING mit $k \stackrel{\wedge}{=} \texttt{CODE}$
  - $m_0 \stackrel{\wedge}{=} \texttt{T}$ , $k_{0 \bmod 4} = \texttt{CODE}_0 \stackrel{\wedge}{=} \texttt{C} \rightarrow c_0 \stackrel{\wedge}{=} \texttt{V}$
  - $m_1 \stackrel{\wedge}{=} \texttt{E}$ , $k_{1 \bmod 4} = \texttt{CODE}_1 \stackrel{\wedge}{=} \texttt{O} \rightarrow c_1 \stackrel{\wedge}{=} \texttt{S}$
  - $m_2 \stackrel{\wedge}{=} \texttt{S}$ , $k_{2 \bmod 4} = \texttt{CODE}_2 \stackrel{\wedge}{=} \texttt{D} \rightarrow c_2 \stackrel{\wedge}{=} \texttt{V}$
  - $m_3 \stackrel{\wedge}{=} \texttt{T}$ , $k_{3 \bmod 4} = \texttt{CODE}_3 \stackrel{\wedge}{=} \texttt{E} \rightarrow c_3 \stackrel{\wedge}{=} \texttt{X}$
  - $m_4 \stackrel{\wedge}{=} \texttt{I}$ , $k_{4 \bmod 4} = \texttt{CODE}_0 \stackrel{\wedge}{=} \texttt{C} \rightarrow c_4 \stackrel{\wedge}{=} \texttt{K}$
  - $m_5 \stackrel{\wedge}{=} \texttt{N}$ , $k_{5 \bmod 4} = \texttt{CODE}_1 \stackrel{\wedge}{=} \texttt{O} \rightarrow c_5 \stackrel{\wedge}{=} \texttt{B}$
  - $m_6 \stackrel{\wedge}{=} \texttt{G}$ , $k_{6 \bmod 4} = \texttt{CODE}_2 \stackrel{\wedge}{=} \texttt{D} \rightarrow c_6 \stackrel{\wedge}{=} \texttt{J}$

$\rightarrow$ Chiffretext $c \stackrel{\wedge}{=} \texttt{VSVXKBJ}$

# Enigma I

- Komplexe Substitutionschiffre mit mehreren Varianten
- Maschinell unterstützte Ver- und Entschlüsselung mit Codebüchern




Quellen: Moore, K. et al.: Enigma Machine. `https://brilliant.org/wiki/enigma-machine/` (Zugriff am 16.8.2022), 2022.

[3] Moore, K. et al.: Enigma Machine. `https://brilliant.org/wiki/enigma-machine/` (Zugriff am 16.8.2022), 2022.

# Enigma II

- Vereinfachter Verschlüsselungsvorgang:

1. Buchstabenvertauschung: Eingesteckte Buchstaben werden vor der eigentlichen Verschlüsselung vertauscht (z.B. `A` zu `J` und umgekehrt)
   - Täglich gewechselt basierend auf Codebuch
   - Fatale Schwachstelle: Buchstaben können im Chiffretext nie auf sich selbst abgebildet werden $\rightarrow$ Nachrichtenrückgewinnung durch (Zeichen-)Ausschluss
2. Sequenzielle Mehr-Walzen-Substitution: Jede von drei Walzen (wählbar aus insgesamt fünf) führt eine andere Substitution durch
   - Walzenreihenfolge kann gewählt werden
   - Startposition jeder Walze kann festgelegt werden

- Entschlüsselung erfordert identische Maschineneinstellung (Brett zum Vertauschen, Walzenreihenfolge, Walzenstartpositionen) wie bei der Verschlüsselung

[3] Moore, K. et al.: Enigma Machine. `https://brilliant.org/wiki/enigma-machine/` (Zugriff am 16.8.2022), 2022.

# Überblick über Kryptoanalyse

- Definition laut Wörterbuch[2]: „Methoden und Techniken, um Informationen aus verschlüsselten Texten zu gewinnen“
- Altes Bedrohungsmodell: Die Chiffre/der Algorithmus ist unbekannt (z.B. Enigma)

→ Eventuell muss zuerst Entschlüsselungsalgorithmus gefunden werden

- Modernes Bedrohungsmodell: Die Chiffre ist bekannt (Kerckhoffsches Prinzip)
- Kurzwiederholung: Sicherheit nur gegen bestimmte Angriffe → Wie mächtig ist der Angreifer?
- Verschiedene Angriffsszenarien
- Beispiele für einfache Kryptoanalyse
  - Häufigkeitsanalyse
  - Angriffe auf die Vigenère-Chiffre

[2] `https://www.fremdwort.de/suchen/bedeutung/kryptoanalyse` (Zugriff am 6.12.2022)

# Angriffsszenarien I

- Unterschiedliche mögliche Ziele eines Angreifers
  - Klartext aus einem bestimmten Chiffretext rückgewinnen/entschlüsseln
  - Schlüssel rückgewinnen, um Klartexte aus beliebigen Chiffretexten rückgewinnen zu können (stärkerer Angreifer, der bei Erfolg alle vergangenen und zukünftigen Nachrichten lesen kann)

- **Einfache Angriffe**
- Erschöpfender/**Brute-force-Suchangriff**
- Timing-Angriffe
- Seitenkanalangriffe

...

# Angriffsszenarien II

Vier einfache Angriffe (von schwach bis stark, für die Chiffre):

- Ciphertext-only-Angriff: Einzelne Nachricht nur basierend auf dem Chiffretext entschlüsseln (keine anderen Fähigkeiten)
- Known-Plaintext-Angriff: Zusammengehörige Klartext/Chiffretext-Paare vom selben Schlüssel sammeln und Schlüssel zum Entschlüsseln anderer Chiffretexte ableiten
- Chosen-Plaintext-Angriff: Klartext auswählen/beeinflussen, der in Chiffretext verschlüsselt wird und versuchen, Klartexte aus anderen Chiffretexten zu rekonstruieren
- Chosen-Ciphertext-Angriff: Beliebige Chiffretexte in Klartexte entschlüsseln und versuchen Schlüssel abzuleiten, um andere Chiffretexte zu entschlüsseln

# Angriffsszenarien III

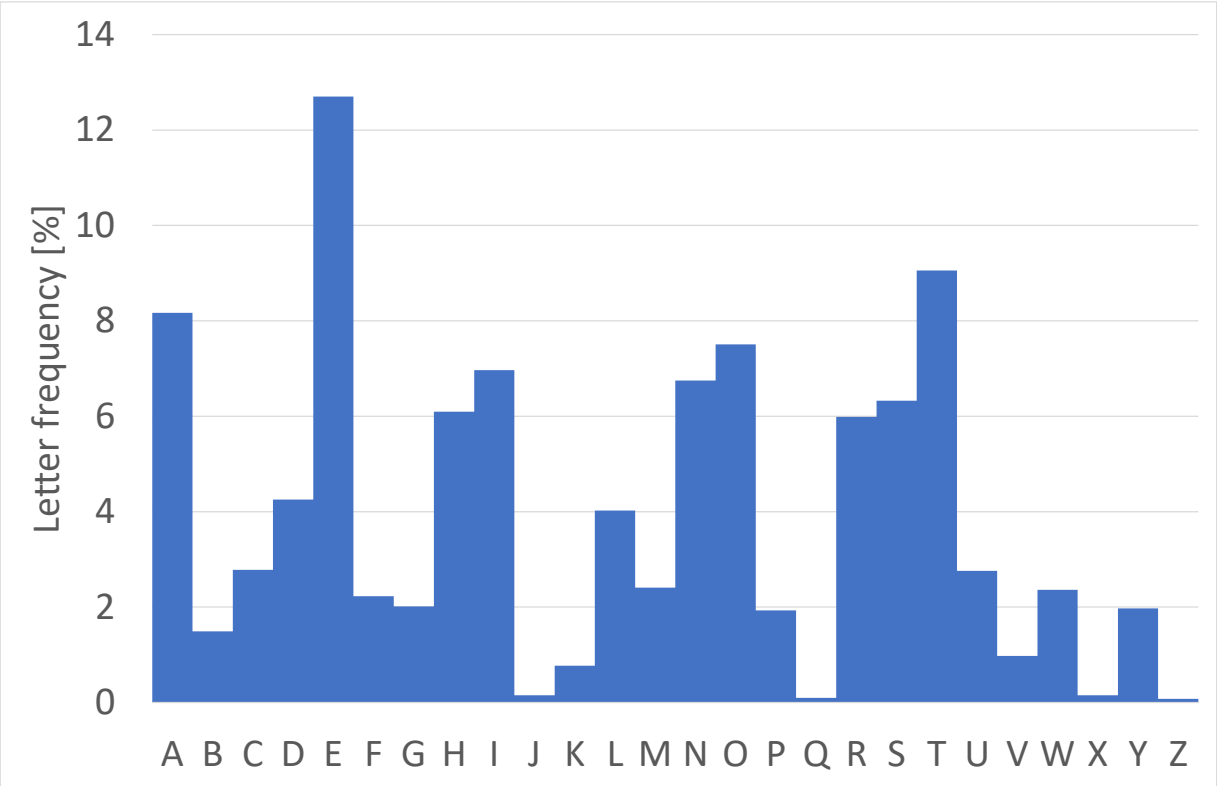
- Brute-force-Suchangriff
  - Alle möglichen Schlüssel ausprobieren bis der richtige gefunden ist
  - $\rightarrow$ Arbeits-/rechenintensiver bei längeren Schlüsseln
  - Schlüsselraum: Menge aller möglichen Schlüssel

- Beispiele für Schlüsselraumgrößen:
  - Caesar-Chiffre: $26 \approx 10^1$ Schlüssel (S.)
  - Vigenère-Chiffre mit 3-stelligem Schlüssel: $26^3 = 17,576 \approx 10^4$ S.
  - Vernam-Chiffre mit 10-Bit-Schlüssel/-Nachricht: $2^{10} = 1,024 \approx 10^3$ S.
  - Vernam-Chiffre mit $n$-Bit-Schlüssel: $2^n \approx 10^{\frac{n}{3}}$ Entschlüsselungen

- Praktisches Ziel: Unzumutbare Schlüsselraumgrößen für Angreifer (z.B. 256 Bit)

# Einfaches Kryptoanalysebeispiel: Häufigkeitsanalyse I

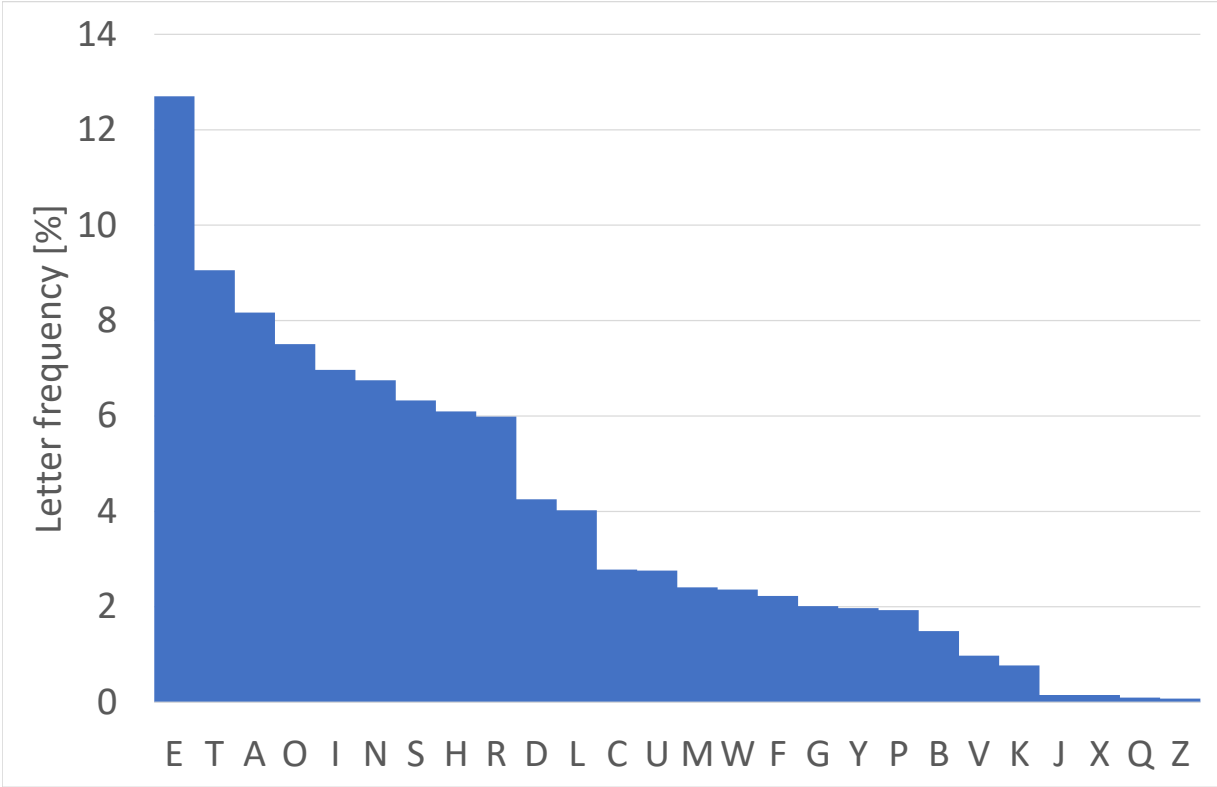
- Annahme: Klartext ist Nachricht in natürlicher Sprache, z.B. Englisch
- Buchstabenhäufigkeiten in natürlichsprachlichen Texten sind bekannt




Datenquelle: Neckář, J.: Letter frequency (English). `http://en.algoritmy.net/article/40379/Letter-frequency-English` (Zugriff am 16.8.2022), 2016.

# Einfaches Kryptoanalysebeispiel: Häufigkeitsanalyse II

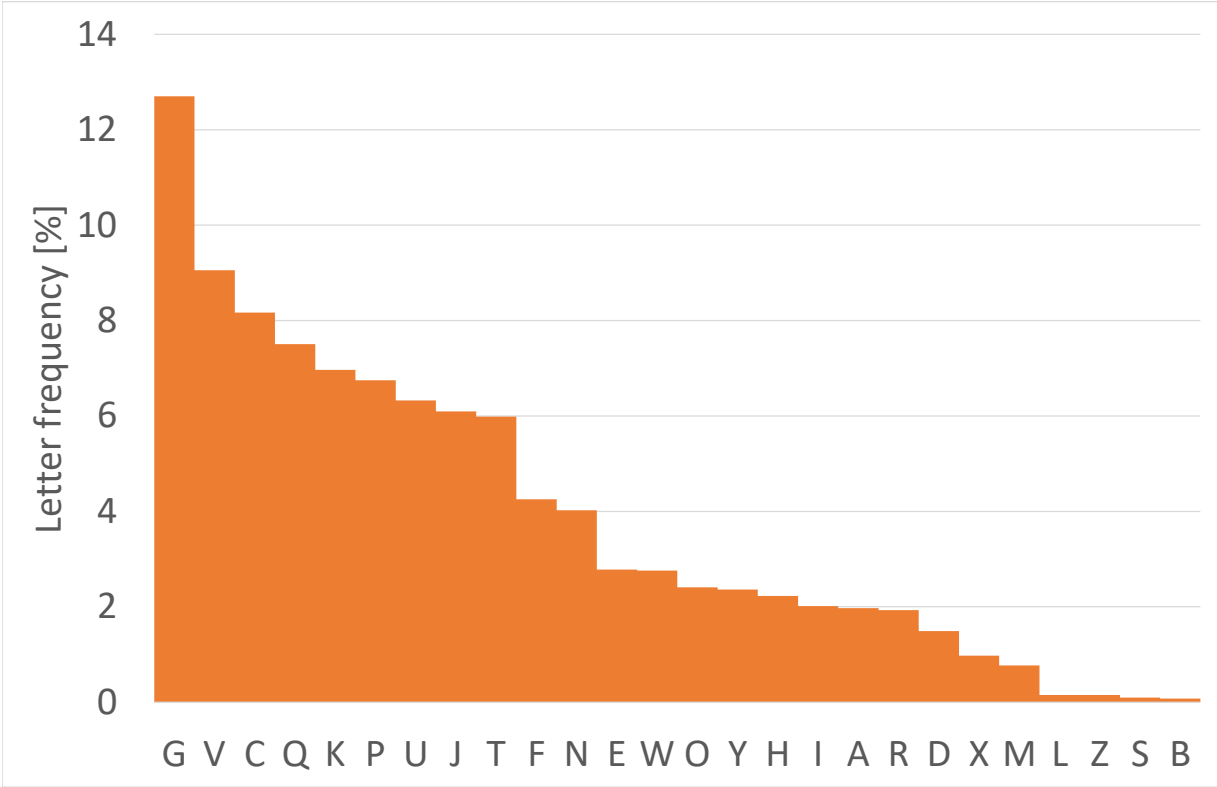
- Häufige Zeichen in der englischen Sprache sind E, T, A, ...




Datenquelle: Neckář, J.: Letter frequency (English). `http://en.algoritmy.net/article/40379/Letter-frequency-English` (Zugriff am 16.8.2022), 2016.

# Einfaches Kryptoanalysebeispiel: Häufigkeitsanalyse III

- Häufigkeitsanalyse von Chiffretext zeigt Chiffretextzeichenhäufigkeit




Originaldatenquelle: Neckář, J.: Letter frequency (English).
`http://en.algoritmy.net/article/40379/Letter-frequency-English` (Zugriff am 16.8.2022), 2016.

# Einfaches Kryptoanalysebeispiel: Häufigkeitsanalyse IV

- Bei monoalphabetischen Substitutionschiffren (z.B. Caesar) ähnliche Häufigkeiten zu erwarten, mit entsprechend verschobenen Buchstaben
- Einheitliche Verschiebung (im Alphabet) zwischen ähnlich häufigen Zeichen erlaubt Versatz-/Schlüsselrückgewinnung (etwas Fehlertoleranz ist sinnvoll!)

- (Ideal-)Beispiel:
  - Häufigster Buchstabe (`G` vs. `E`) $\rightarrow$ Unterschied von $+2$ (`C`)
  - Zweithäufigster Buchstabe (`V` vs. `T`) $\rightarrow$ Unterschied von $+2$ (`C`)

  ...

  $\rightarrow$ Schlüssel ist `C`

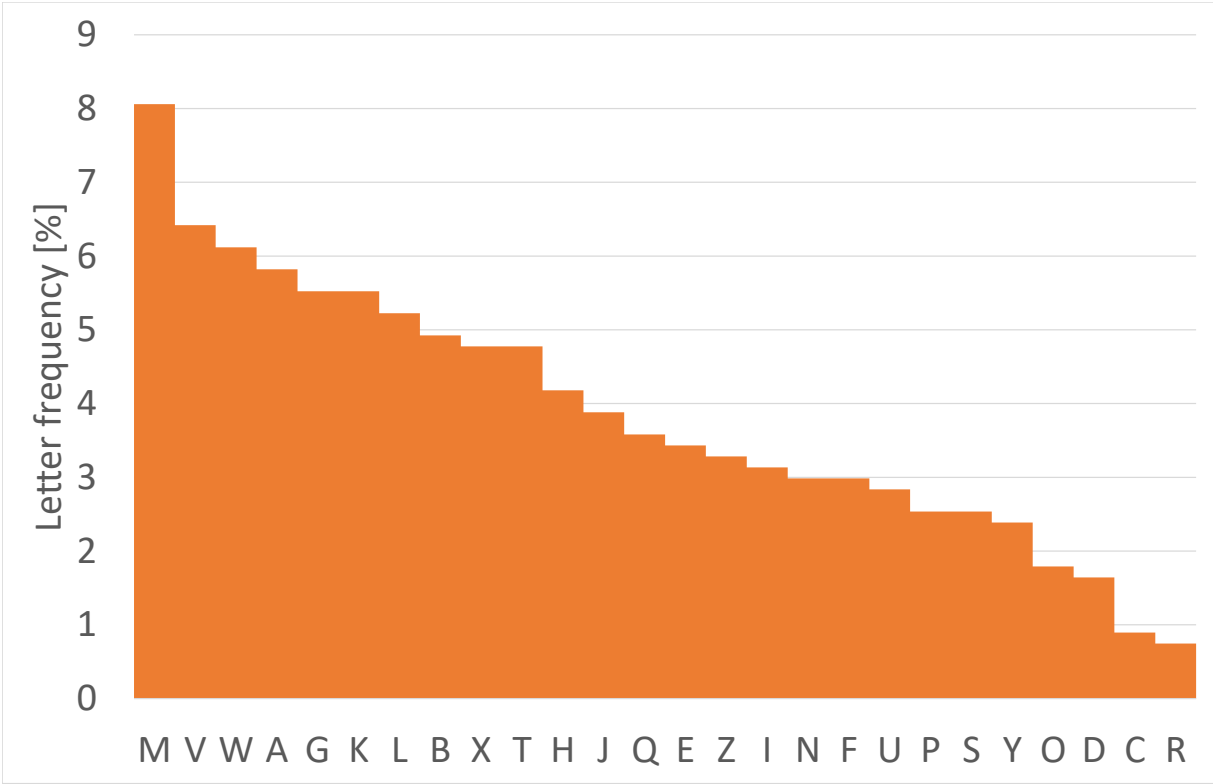
- Vorbehalt: Langer Text benötigt
  - Zeichenhäufigkeiten nähern sich nur in längeren, sprachtypischen Texten an $\rightarrow$ je länger der Text, umso besser; Fremdwörter schaden

  $\rightarrow$ Kurze Texte können unzureichend für Häufigkeitsanalyse sein

# Angriffe auf die Vigenère-Chiffre: Versuchte H.-analyse

- Für polyalphabetische Substitutionschiffren wie Vigènere funktioniert Häufigkeitsanalyse auf dem gesamten Chiffretext nicht
  - Selber Klartextbuchstabe $m_i$ verschiedenen $c_i$ an verschiedenen Stellen zugeordnet

  $\rightarrow$ Zeichenhäufigkeiten sind „verschmiert“ (mehr bei längeren Schlüsseln)



# Angriffe auf die Vigenère-Chiffre: Modifizierte H.-analyse

- Zur Erinnerung
  - Vigenère-Chiffre ist Caesar-Chiffre mit positionsabhängigem Schlüssel
    $\rightarrow$ Folie 15
  - $\rightarrow$ Schlüssel wiederholt sich alle $||k||$ Stellen:
    $Vigenere(k, m_i) = Caesar(k_{i \mod ||k||}, m_i)$ $\rightarrow$ Folie 16
  - $\rightarrow$ Ein Vigenère-Chiffretext ist eine Verschmelzung von $||k||$ Caesar-Chiffretexten: $C_0 = \{c_i : i \mod ||k|| = 0\}$,
    $C_1 = \{c_i : i \mod ||k|| = 1\}$,
    $\dots$,
    $C_{||k||-1} = \{c_i : i \mod ||k|| = ||k|| - 1\}$
- **Wenn** die Schlüssellänge $||k||$ bekannt ist
  - Häufigkeitsanalyse von jedem Caesar-Chiffretext $C_n$ einzeln
  - Verschiebung/Schlüssel von jedem Caesar-Chiffretext bestimmen
  - $\rightarrow$ Schlüssel von Caesar-Chiffretexten zu Vigènere-Schlüssel zusammenfügen
- Wie die Schlüssellänge herausfinden?
  - Kasiski-Test
  - Autokorrelation

# Angriffe auf die Vigenère-Chiffre: Kasiski-Test I

- Zur Erinnerung: Schlüssel wiederholt sich alle $||k||$ Stellen

$\rightarrow$ Selbe Wörter im Klartext ergeben selbe Wörter im Chiffretext, wenn sie ein ganzzahliges Vielfaches von $||k||$ voneinander entfernt sind

```
K QRQG BR QQFH XQ ADOG MRY NOXKJ: HKMPUV RQK, WLCH EICF D AGWJLVM
DRF O VITWRYU PUSY, GDH, JWJL, CBG AQFNMPU, IYNZ RJ UHDXG OQH
YCH, WWQK RQPOI UQHRGG DW FFDA VVH IAS WS HZRA, YS QSY DUIUSQX.
VVRWG HKEV QDR RWWC, JSUI OOB, MH HKIA HKMPY LX YSOP, NSW JCZO E
VSDV; VVH WWPMIEH ZMNZ GIUSUZG WW. WWQK EU ULZG HKIKF PSPSB SWH
RJ JCSI VVHC OOB FGZLIXS, PEA VHVG TLRF HUYVV WSQ. HKSUS WLCH
FSOS WS USH SPZB E UVRA QF WAQ, OQH UC DKTSH XJS SPCM PEA DDWU,
WI XJSB FG GWMNZ DRF KLPNWQK, K'ZO YPRHVVONI OOB WGS DACM WLGWU
WJWOPKBJ VKQKPA WQ XYC VLQFW LQIUW. QBOC VVHC VVDX ECPI VC KICF D
QGFUC DOZHA DOEA, O QSKGH SH HDVISWW, QF WS USH E HSOPQK LR C
ZRRI ARXNSB GQOW KWOUHGR ZMVV BINZRA, YWOP DS GIESLZGR; IST,
UHRVZH LGOUITG, NRQK, WS TOQO QIU GJCVIP HUYVV ZMVV VYEV D WJCZ
[..]
```

# Angriffe auf die Vigenère-Chiffre: Kasiski-Test II

- Zur Erinnerung: Schlüssel wiederholt sich alle $||k||$ Stellen

$\rightarrow$ Selbe Wörter im Klartext ergeben selbe Wörter im Chiffretext, wenn sie ein ganzzahliges Vielfaches von $||k||$ voneinander entfernt sind

```
K QRQG BR QQFH XQ ADOG MRY NOXKJ: HKMPUV RQK, WLCH EICF D AGWJLVM
DRF O VITWRYU PUSY, GDH, JWJL, CBG AQFNMPU, IYNZ RJ UHDXG OQH
YCH, WWQK RQPOI UQHRGG DW FFDA VVH IAS WS HZRA, YS QSY DUIUSQX.
VVRWG HKEV QDR RWWC, JSUI OOB, MH HKIA HKMPY LX YSOP, NSW JCZO E
VSDV; VVH WWPMIEH ZMNZ GIUSUZG WW. WWQK EU ULZG HKIKF PSPSB SWH
RJ JCSI VVHC OOB FGZLIXS, PEA VHVG TLRF HUYVV WSQ. HKSUS WLCH
FSOS WS USH SPZB E UVRA QF WAQ, OQH UC DKTSH XJS SPCM PEA DDWU,
WI XJSB FG GWMNZ DRF KLPNWQK, K'ZO YPRHVVONI OOB WGS DACM WLGWU
WJWOPKBJ VKQKPA WQ XYC VLQFW LQIUW. QBOC VVHC VVDX ECPI VC KICF D
QGFUC DOZHA DOEA, O QSKGH SH HDVISWW, QF WS USH E HSOPQK LR C
ZRRI ARXNSB GQOW KWOUHGR ZMVV BINZRA, YWOP DS GIESLZGR; IST,
UHRVZH LGOUITG, NRQK, WS TOQO QIU GJCVIP HUYVV ZMVV VYEV D WJCZ
[..]
```

# Angriffe auf die Vigenère-Chiffre: Kasiski-Test III

- Terminologie:
  - N-Gramm[3]: „beliebig lange Folge von Buchstaben [..], wobei N für die jeweilige Anzahl steht“
  - Bigramm (zwei Buchstaben) → Folie 29
  - Trigramm (drei Buchstaben) → Folie 30
- In langen Texten tauchen Bigramme/Trigramme/etc. an Stellen auf, die ein ganzzahliges Vielfaches von $||k||$ sind

→ Positionsdifferenzen sind sehr wahrscheinlich Vielfache der Schlüssellänge

→ Größter gemeinsamer Teiler ($ggT$) der Positionsdifferenzen ist sehr wahrscheinlich die Schlüssellänge oder ein Vielfaches davon

[3] `https://www.wortbedeutung.info/N-Gramm/` (Zugriff am 9.12.2022)

# Angriffe auf die Vigenère-Chiffre: Kasiski-Test IV

- `WS`-Bigramm aus Beispiel (→ Folie 29):
  - An Stellen 126, 294, 470 und 550

  → Positionsdifferenzen 168, 80 und 80
- `OQH`-Trigramm aus Beispiel (→ Folie 30):
  - An Stellen 93 und 313

  → Positionsdifferenz 220
- $ggT(168, 80, 80, 220) = 4$

→ Schlüssellänge ist wahrscheinlich 4 oder ein Vielfaches von 4

- Alternativer Ansatz: Häufigkeitsanalyse von den Faktoren der Positionsdifferenzen (z.B. von allen Bigrammen)

→ Häufigere/Häufigste Faktoren sind sehr wahrscheinlich Faktoren der Schlüssellänge

# Angriffe auf die Vigenère-Chiffre: Autokorrelation I

- Zur Erinnerung: Schlüssel wiederholt sich alle $||k||$ Stellen

$\rightarrow$ Chiffretextzeichen, die ein ganzzahliges Vielfaches der Schlüssellänge voneinander entfernt sind, sind wahrscheinlicher gleich

$\rightarrow$ Inzidenz identischer Zeichen (Koinzidenz) an Chiffretextstellen $i + l$ für alle Chiffretextzeichen $c_i$ mit jeder plausiblen Schlüssellänge $l$ berechnen

$\rightarrow$ Inzidenz $I_l$ für alle plausiblen Schlüsellängen $l \in \mathbb{N}^+$ berechnen

$\rightarrow$ Schlüssellänge $\arg\max_l I_l$ mit höchster Inzidenz ist sehr wahrscheinlich die Schlüssellänge oder ein Vielfaches davon

# Angriffe auf die Vigenère-Chiffre: Autokorrelation II

- Illustration von Zeichenkoinzidenz (Referenz: R an Stelle 2):

K QRQG BR QQFH XQ ADOG MRY NOXKJ: HKMPUV RQK, WLCH EICF D AGWJLVM DRF O VITWRYU PUSY, [..]

- Schlüssellänge von $l = 4$ (korrekt) angenommen

$\rightarrow$ 3 von 15 Übereinstimmungen (20%)

K QRQG BR QQFH XQ ADOG MRY NOXKJ: HKMPUV RQK, WLCH EICF D AGWJLVM DRF O VITWRYU PUSY, [..]

- Schlüssellänge von $l = 3$ (fälschlicherweise) angenommen

$\rightarrow$ 0 von 20 Übereinstimmungen (0%)

- Erwartete Koinzidenz: $\frac{1}{26} \approx 4\%$ (in längeren Texten)

# Danke für die Aufmerksamkeit!

Fragen?