



## openHPI – Sicherheit im Internet Klassische Verschlüsselungsverfahren

Prof. Dr. Christoph Meinel  
Hasso-Plattner-Institut, Potsdam

### Verschlüsselung mit monoalphabetischer Substitution (1/2)

Bei Verschlüsselung durch **monoalphabetische Substitution** wird Klartext buchstabenweise substituiert – **verschlüsselt** –, wobei Klartext- und Geheimtextalphabet gleich sind

- Substitutionsschemata zur Verschlüsselung können beliebig gewählt werden, müssen aber allen Kommunikationsteilnehmern bekannt gegeben werden, z.B.
  - Umkehr der Reihenfolge im Alphabet ( $A \Leftrightarrow Z$ ,  $B \Leftrightarrow Y$ ,...)
  - Verschiebung im Alphabet um bestimmte Position
  - Verschlüsselung mit Startwort
  - ...

## Verschlüsselung mit monoalphabetischer Substitution (2/2)

### Verschlüsselung mit Startwort

- Teilnehmer wählen Startwort aus
- An das Startwort wird Alphabet angehängt
- Dann werden alle Mehrfachvorkommen von Buchstaben gestrichen
- **Beispiel:**
  - Teilnehmer wählen Startwort „Internetsicherheit“ aus
  - Hängen an Internetsicherheit das Alphabet an und streichen alle Mehrfachvorkommen von Buchstaben: Es ergibt sich „INTERSCH“ gefolgt vom ausgedünnten Alphabet



## Verschlüsselung mit Verschiebechiffre (1/2)

**Substitutionschiffre**, bei der jeder Buchstabe durch den im Alphabet um  $X$  Positionen (Verschlüsselungsschlüssel) nachfolgenden Buchstaben ersetzt wird

### Beispiel:

- Sender und Empfänger wählen (lateinisches) Alphabet und einigen sich auf Schlüssel (Verschiebungszahl)  $X = 12$ 
  - Klartext: „INTERNETSICHERHEIT“



- Chiffrierter Text: „UZFQDZQFEUOTQDTQUF“
- **Achtung:** Ist  $X$  Vielfaches der Größe des Alphabets, dann ist chiffrierter Text = Klartext

### Aufwand zum Knacken des Schlüssels X:

- Ist bekannt, dass es sich um Verschiebechiffre handelt, braucht Angreifer maximal  $\# \{ \text{Alphabet} \}$  viele Versuche, in unserem Beispiel also maximal 26 Versuche
  - Angreifer verschiebt alle Buchstaben zunächst um  $X=1$ , dann um 2, 3, 4, usw. und testet jeweils, ob Ergebnis einen sinnvollen Text ergibt ...
- **Cäsar-Chiffre:**
  - Ist Spezialfall einer Verschiebechiffre mit  $X=3$ , bei dem „A“ in ein „D“ übersetzt wird ...

## Verschlüsselung mit polyalphabetischer Chiffren

Bei **polyalphabetischen Chiffren** werden mehrere Geheimtextalphabete verwendet

- Gleiche Zeichen im Klartext können so in unterschiedliche Buchstaben im Geheimtext überführt werden und umgekehrt
- **Beispiel:**
  - Die Anzahl der Verschiebungen wird für jedes Zeichen in Abhängigkeit von der Position im Wort gewählt, z.B.
  - Position bestimmt Verschiebung: z.B. „Internetsicherheit“:
    - „I“ an Position 1 wird um 1 verschoben → „J“
    - „N“ an Position 2 wird um 2 verschoben → „P“
    - ...
    - „T“ an Position 18 wird um 18 verschoben → „L“
- „INTERNETSICHERHEIT“ → „JPWIWTLBBSNTRFWUZL“

## Verschlüsselung mit Vigenère Verschlüsselung (1/2)

... von Blaise de Vigenère im 16. Jahrhundert entwickelt

- Wahl eines Schlüsselwortes, z.B. „sicher“  
(im Folgenden werden die Positionen der Buchstaben im Alphabet verwendet: A=0, B=1, ...)
- Danach Verschiebechiffre um entsprechend viele Positionen

|                |    |   |   |   |   |    |    |   |   |   |   |    |    |   |   |   |   |    |
|----------------|----|---|---|---|---|----|----|---|---|---|---|----|----|---|---|---|---|----|
| Klartext       | I  | N | T | E | R | N  | E  | T | S | I | C | H  | E  | R | H | E | I | T  |
| Schlüsseltext  | S  | I | C | H | E | R  | S  | I | C | H | E | R  | S  | I | C | H | E | R  |
| Verschiebungen | 18 | 8 | 2 | 7 | 4 | 17 | 18 | 8 | 2 | 7 | 4 | 17 | 18 | 8 | 2 | 7 | 4 | 17 |
| Chiffre        | A  | V | V | L | V | E  | W  | B | U | P | G | Y  | W  | Z | J | L | M | K  |

- Falls Länge des Texts kein Vielfaches der Schlüssellänge ist, wird dieser am Ende abgeschnitten ...

## Verschlüsselung mit Vigenère Verschlüsselung (2/2)

### Vigenère Chiffre kann man knacken:

- Wenn Text ausreichend lang, kann Angreifer Schlüssellänge (n) ermitteln: Jedes n-te Zeichen ist mit gleicher Verschiebechiffre kodiert, die durch Häufigkeitsanalyse dekodiert werden kann ...

### Vigenère-Variante mit Autokey:

- Schlüsseltext besteht aus Schlüsselwort gefolgt vom Klartext

|               |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Klartext      | I | N | T | E | R | N | E | T | S | I | C | H | E | R | H | E | I | T |
| Schlüsseltext | S | I | C | H | E | R | I | N | T | E | R | N | E | T | S | I | C | H |
| Chiffre       | A | V | V | L | V | E | M | G | L | M | T | U | I | K | Z | M | L | A |

- Empfänger kann die ersten Zeichen mit Schlüsselwort entschlüsseln und die dann folgende Zeichen können mit bereits entschlüsseltem Text dekodiert werden

**Kryptoanalyse** – wie kann Verschlüsselung geknackt werden?

### Das Kerckhoff Prinzip:

- Sicherheit eines Verschlüsselungsverfahrens soll **allein** auf Geheimhaltung des Schlüssels basieren und **nicht** auf Geheimhaltung des Verfahrens

Kerckhoff empfiehlt, Verschlüsselungsverfahren öffentlich bekannt zu geben, um vielen Experten eine Analyse zu ermöglichen und so möglichst schnell eventuelle Schwächen zu erkennen

### Angriffsmöglichkeiten:

- **Brute Force:**
  - Systematisches Durchprobieren aller möglichen Schlüssel
- **Wörterbuchangriffe:**
  - Systematisches Durchprobieren von häufig verwendeten oder bekannten Schlüsselwörtern
- **Statistische Analysen:**
  - Möglich auf Basis von sprachwissenschaftlichen Beobachtungen, z.B. Buchstabenhäufigkeiten in Wörtern einer Sprache
- **Chosen-Plaintext:**
  - Analyse der Verschlüsselung eines bekannten Textes
- ...