Chiffrier-Ring

written by ps



Einsatzgebiet

- Informatik: Themengebiet Codierung und Verschlüsselung
- Mathematik

Einleitung

Mit Hilfe dieses Chiffrier-Rings können geheime Botschaften verschlüsselt bzw. entschlüsselt werden. Der Chiffrier-Ring kann bei unterschiedlichen Verschlüsselungsverfahren eingesetzt werden. Am besten man wählt dabei die folgende Reihenfolge:

1. Caesar-Verschlüsselung
2. Alberti-Verschlüsselung
3. Vigenère-Verschlüsselung

Funktionsweise für die Caesar-Verschlüsselung:

Sender und Empfänger der Nachricht benötigen einen Chiffrier-Ring. Um die Nachricht zu verschlüsseln, muss ein Buchstabe als Schlüssel ausgewählt werden (monoalphabetisches Verschlüsselungsverfahren).

- Auf dem oberen Ring befindet sich das Alphabet zur Darstellung des Klartextes
- Auf dem unteren Ring befindet sich das Alphabet zur Darstellung des Geheimtextes
- Man dreht den unteren Ring so, dass sich der Buchstabe “A” des oberen Rings oberhalb des gewählten Schlüsselbuchstabens (z.B. “D”) des unteren Rings befindet (z.B. “A” steht über “D”)
- Nun steht unter jedem Buchstaben des Klartextes auf dem oberen Ring der entsprechende verschlüsselte Buchstabe auf dem unteren Ring.

Jetzt darf der Ring nicht weitergedreht werden und der verschlüsselte Text kann von “oben” nach “unten” abgelesen werden.

Beispiel:

Schlüssel=D: aus „A“ wird „D“, aus „B“ wird „E“, etc.

Klartext: CAESAR –> verschlüsselter Text: FDHVDU

Zur Entschlüsselung muss man nur von “unten” nach “oben” lesen.

Die Verfahren von Alberti und Vigenère bauen auf die Caesar-Verschlüsselung auf. Hier gibt es jedoch für jeden Klartextbuchstaben einen eigenen Schlüssel (polyalphabetisches Verschlüsselungsverfahren).