LU05b - Die Symmetrische Verschlüsselung

Lernziele

- Den Begriff **Symmetrische Verschlüsselung** in eigenen Worten erklären können.
- Die **vier grundlegenden Varianten** von symmetrischen Verschlüsselungen nennen und mit konkreten Beispielen ergänzen können.
- Einfache Begriffe mit Hilfe der Vigenère Verschlüsselung ohne technische Hilfsmitteln ver- und und entschlüsseln können.
- Die Enigma-Verschlüsselung und deren Komponenten nennen und Gründe nennen können, warum dieses Verfahren erfolgreich war.
- Anzahl von Schlüsselpaaren zu einer gegebenen Anzahl von Usern berechnen können.

1. Symmetrische Verschlüsselung

Symmetrische Verschlüsselungsverfahren zeichnen sich dadurch aus, dass zum Verschlüsseln und zum Entschlüsseln der gleiche Schlüssel verwendet wird.

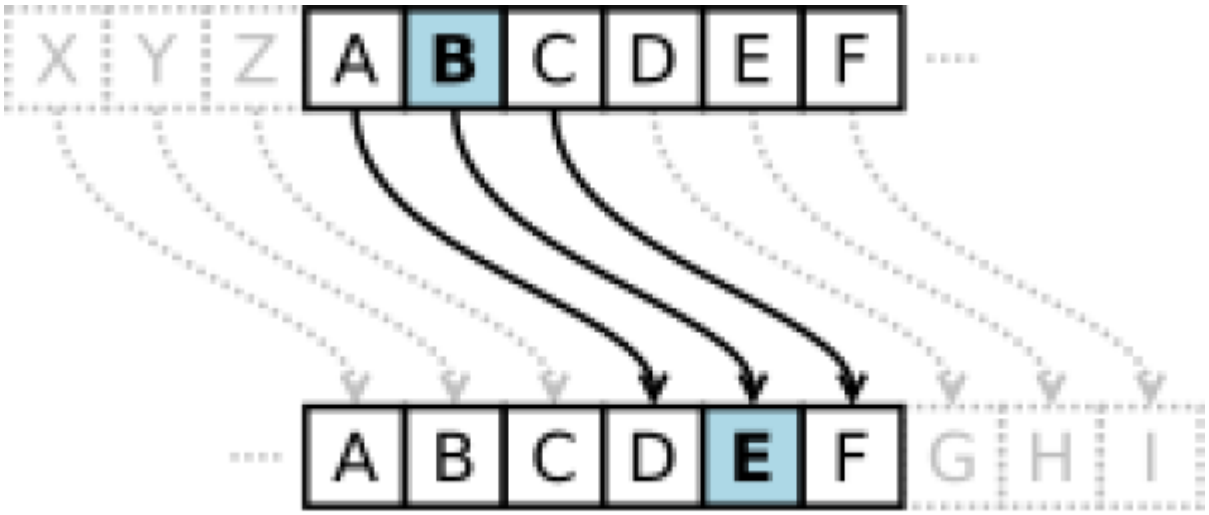


Abbildung 1: Der Ablauf einer symmetrischen Verschlüsselung

Monoalphabetische Verfahren gehören zu den ältesten bekannten Verschlüsselungen. Schon Cäsar setzte sie bei seinen Feldzügen ein.



Sie beruhen darauf, dass in einem Text jedem Buchstaben fix ein anderer Buchstabe zugeordnet ist. Die Definition dieser Zuordnung bildet den Schlüssel. Einfache monoalphabetische Verfahren addieren zu jedem Buchstaben einen fixen Betrag, wobei nach Z wieder A folgt.



1.1 Monoalphabetische Verfahren

Volkan Demir

From:
https://wiki.bzz.ch/ - **BZZ - Modulwiki**

Permanent link:
https://wiki.bzz.ch/modul/m183/learningunits/lu05/02?rev=1755007897

Last update: **2025/08/12 16:11**