

LU05.A08 - Skytale -Verschlüsselung programmieren - TBD

Lernziele

- Ich kann den Skytale-Algorithmus mittels einer Programmiersprache umsetzen.

Rahmenbedingungen

- **Zeitbudget:** 40 Minuten
- **Sozialform:** Einzelarbeit
- **Hilfsmittel:**
 - Programmierumgebung
 - Codeeditor Ihrer Wahl
 - Programmiersprachen: JS, Python, BASH, SHELL, ...
 - **Keine AI oder Google-Suchen → Sie haben genug Programmierkenntnisse, um den Algorithmus selbst zu programmieren.**
- **Erwartetes Ergebnis:** Script, das eine Cäsar-Verschlüsselung realisiert. In beide Richtungen: Klartext → Chiffretext, Chiffretext → Klartext.

Ausgangslage

Die Skytale-Verschlüsselung gehört zu den ältesten Systemen der Welt. Im Kern wird ein Papierband um ein Stab gewickelt und die Nachricht der Länge nach auf das Band geschrieben.

Der Key dabei ist der Durchmesser des Stabes.

Arbeitsauftrag

Schreiben Sie ein Script bzw. Programm, das eine Nachricht mit Hilfe der Skytale-Verschlüsselung verschlüsselt und entschlüsselt.

Idee Die Skytale ist eine Transpositionschiffre: Die Buchstaben bleiben gleich, nur ihre Reihenfolge ändert sich.

Physikalisch wickelt man einen Lederstreifen um einen Stab und schreibt längs der Stabachse. Abgewickelt steht der Text in verwürfelter Reihenfolge auf dem Streifen. Der Stabdurchmesser ist der Schlüssel.

Modell im Code

Der Stab entspricht einer Matrix mit k Spalten, wobei k = Anzahl Buchstaben, die um den Umfang passen.

Verschlüsseln: Klartext zeilenweise einfüllen, spaltenweise auslesen
Entschlüsseln: genau umgekehrt

Beispiel mit HALLOWELT und $k = 3$:

```
H A L      Zeilenweise füllen
L O W
E L T
```

Spaltenweise gelesen: **HLE AOL LWT** → **HLEAOLLWT**

Anforderungen:

1. Das Programm soll
 - vom Benutzer eine Nachricht (Text) einlesen.
 - vom Benutzer einen ganzzahligen Schlüssel (Anzahl Zeilen der Speichermatrix) einlesen.
 - `verschluesseln(text, shift)` → gibt den verschlüsselten Text zurück
 - `entschluesseln(text, shift)` → gibt den entschlüsselten Text zurück
2. Das Programm soll den verschlüsselten Text ausgeben, dann den entschlüsselten Text, um zu zeigen, dass die ursprüngliche Nachricht wiederhergestellt wird

**** Beispiel:****

```
Eingabe:  Hallo Welt
Shift:    3
Verschlüsselt:  Kdoor Zhou
Entschlüsselt:  Hallo Welt
```

Hinweis

- Den Shift bekommen Sie hin, wenn Sie mit den Ordinalzahlen (Codewerte der Zeichen arbeiten).
- Codiert wird einfach, indem der Ordinalzahl ein Shift addiert wird.
- Bei Dekodieren wird einfach der Ordinalzahl der Shift abgezogen.

Solution

Lösung

 Volkan Demir

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

Permanent link:
<https://wiki.bzz.ch/modul/m183/learningunits/lu05/aufgaben/08?rev=1788335959>

Last update: **2026/09/02 09:59**

