

Untersuchung eines Transpositionsverfahrens

Bei dem Transpositionsverfahren, das hier untersucht werden soll, wird der Klartext zeilenweise in eine Tabelle geschrieben. Der Schlüssel legt die Anzahl der Spalten fest. Freie Plätze in der letzten Zeile werden mit zufälligen Buchstaben aufgefüllt. Der Geheimtext wird spaltenweise von links nach rechts ausgelesen.

Beispiel: Der Klartext TREFFEN AUF DEM MARKT wird mit dem Schlüssel 5 zu dem Geheimtext TEDRRNEKEAMTFUMEFFAP verschlüsselt.

T	R	E	F	F
E	N	A	U	F
D	E	M	M	A
R	K	T	E	P

Aufgabe 1:

- Verschlüsseln Sie den Klartext SONNTAGMORGEN mit dem Schlüssel 3.
- Entschlüsseln Sie den Geheimtext LESDCEEREHLILRNASETSEG mit dem Schlüssel 4.
- Versuchen Sie den Geheimtext DFIRCEAHDGERENEZPIEY ohne Kenntnis des Schlüssels zu Knacken. Welche Angriffsmöglichkeiten gibt es hier?
- Anstatt die freien Plätze mit zufälligen Buchstaben aufzufüllen, könnte man sie auch alle mit dem Buchstaben X auffüllen oder frei lassen. Untersuchen Sie welche Auswirkung diese Änderungen jeweils auf die Sicherheit des Verfahrens hätten.

Aufgabe 2*: Implementieren Sie das hier vorgestellte Transpositionsverfahren: Erstellen Sie ein Programm, das die Eingabe eines Klartextes und eines Schlüssels als Zahl erlaubt und den entsprechenden Geheimtext ausgibt. Entscheiden Sie selbst, wie Sie dabei mit freien Plätzen in der Tabelle umgehen. Ergänzen Sie auch die Möglichkeit der Entschlüsselung.

Tipp: Es bietet sich an eine zweidimensionale Reihung vom Typ Zeichen zu erstellen. Dabei gibt der Schlüssel die eine Dimension vor, die andere muss aus der Länge des Textes und des Schlüssels berechnet werden. In die Reihung muss der Klartext dann zunächst wie in der Tabelle dargestellt eingetragen und anschließend geeignet ausgelesen werden.

Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](#). Von der Lizenz ausgenommen ist das InfSII-Logo.

* Aufgabe zur Verknüpfung von Kryptologie und Algorithmik