Einfache Blockchiffreverfahren

Sie haben im Zusammenhang mit der Vigenère-Verschlüsselung den Begriff Konfusion kennengelernt:

In der Kryptologie spricht man von **KONFUSION**, wenn sich statistische Auffälligkeiten des Klartextes nicht auf den Geheimtext übertragen.

Manchmal ist bei der Verschlüsselung eine vollständige Konfusion nicht möglich. Gründe können beispielsweise zu kurze Schlüssellängen, statistische Auffälligkeiten im Schlüssel oder Ähnliches sein. Deswegen versucht man in einem Verschlüsselungsverfahren zusätzlich zur Konfusion für Diffusion zu sorgen:

In der Kryptologie spricht man von **DIFFUSION**[1], wenn Änderungen eines einzelnen Zeichens des Klartextes möglichst viele Änderungen des Geheimtextes bewirken. Im Idealfall hängt sogar jedes Bit des Geheimtextes von jedem Bit des Klartextes und des Schlüssels ab.

Aufgabe: Begründen Sie kurz, warum das Vigenère-Verfahren nicht für Diffusion sorgt.

Beispiel: Ein einfaches Blockchiffreverfahren mittels Permutationen

Bei einem Blockchiffreverfahren wird der Geheimtext in Blöcke aufgeteilt und diese Blöcke jeweils einzeln verschlüsselt. Bei modernen Verfahren sind die Blöcke sehr groß und bestehen beispielsweise aus 128 Bits oder sogar noch mehr. Wir betrachten dagegen jetzt erst einmal ein deutlich einfacheres Beispiel mit Blöcken der Länge 6. Das im Folgenden beschriebene Verfahren ist willkürlich ausgedacht und soll nur die prinzipielle Vorgehensweise verdeutlichen. Auf existierende moderne Blockchiffreverfahren gehen wir später ein.

Als Beispiel wollen wir den folgenden Text verschlüsseln: DERSCHATZLIEGTUNTERDERBANK. Wir hatten als Blocklänge (willkürlich) 6 festgelegt, teilen den Klartext jetzt also in Blöcke der Länge 6 auf:

DERSCH ATZLIE GTUNTE RDERBA NK

Da der letzte Block nur aus zwei Buchstaben besteht, füllen wir ihn willkürlich auf:

DERSCH ATZLIE GTUNTE RDERBA NKOCQH.

Jetzt verschlüsseln wir jeden Block einzeln. Als Schlüssel wählen wir eine sogenannte Permutation (Vertauschung). Dabei legen wir fest, welche Stelle des Klartextes an welche Stelle des Geheimtextes getauscht wird. In der Mathematik stellt man eine Permutation häufig durch eine Matrix mit zwei Zeilen dar. In der oberen Zeile stehen die Zahlen 1 bis n (in unserem Fall 1 bis 6). In der unteren Zeile stehen die Stellen, an die die Werte getauscht werden. So bedeutet die Matrix

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 5 & 3 & 2 \end{pmatrix}$, dass der Wert der ersten Stelle an die vierte Stelle wandert, der Wert der zweiten Stelle an die erste, usw.

[1] In der Literatur findet man unterschiedliche Definitionen von Konfusion und Diffusion, auch hinsichtlich der Stärkegrade. Die hier verwendete Definition von Diffusion wird auch als Lawineneffekt bezeichnet.

Aus dem Block DERSCH wird damit EHCDSR. Als Hilfe schreibt man sich dazu beispielsweise die „alten“ Stellen über den Klartext und die „neuen“ Stellen im Geheimtext darunter:

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ D & E & R & S & C & H \\ 4 & 1 & 6 & 5 & 3 & 2 \end{matrix}.$$

Analog erhält man als Verschlüsselung des zweiten Blocks $\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ A & T & Z & L & I & E \\ 4 & 1 & 6 & 5 & 3 & 2 \end{matrix}$, dass ATZLIE zu TEIALZ wird.

Aufgaben:

1) Verschlüsseln Sie auch die restlichen Blöcke GTUNTE RDERBA NKOCQH mit dem Schlüssel $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 5 & 3 & 2 \end{pmatrix}$.

2) Entscheiden Sie, ob es sich bei dem Verfahren um ein Substitutions- oder Transpositionsverfahren handelt.

3) Verschlüsseln Sie nach dem gleichen Verfahren den Text TREFFENBEIDEREICHE mit dem Schlüssel $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \end{pmatrix}$.

   Entschlüsseln Sie außerdem den ebenfalls mit dem Schlüssel $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \end{pmatrix}$ verschlüsselten Text UGETDIEE.

4) Entscheiden Sie, ob dieses Beispielverfahren für Diffusion sorgt.

5) Knacken Sie den folgenden Geheimtext, der mittels des beschriebenen Blockchiffreverfahrens mit einem Schlüssel der Länge 3 verschlüsselt wurde:

IBE EDI MSE RVE HFA NRE TIS EDI NLÄ DGE BER CLÖ EKE SNT ECH EID FND DÜR SIE HIC HER TEI

6) Es soll ein zufälliger Schlüssel für Blöcke der Länge 32 erzeugt werden. Implementieren Sie eine Methode, die einen geeigneten Schlüssel erzeugt.