2. Transposition

Während bei sehr kurzen Mitteilungen (z. B. „hey“) nur eine geringe Anzahl von Anordnungsmöglichkeiten existieren (ehy, eyh, hey, hye, yeh, yhe), gibt es bereits bei Sätzen wie „Lieber krank feiern als gesund arbeiten“ knapp 300 Millionen Millionen Millionen Millionen Millionen Millionen verschiedene Möglichkeiten, die 34 Buchstaben des Satzes umzuordnen. Könnte ein Mensch eine Anordnung pro Sekunde prüfen, und arbeiteten alle Menschen der Erde Tag und Nacht, dann würde immer noch die hundertmilliardenfache Lebensspanne des Universums nötig sein, um alle Möglichkeiten durchzuprüfen.

Eine Zufallstransposition von Buchstaben bietet also ein sehr hohes Maß an Sicherheit. Doch die Sache hat einen Haken: Der eigentliche Empfänger kann ebenso wenig wie der gegnerische Abhörer die Nachricht entschlüsseln. Die Umstellung muss also nach einem handhabbaren System erfolgen. Zwei dieser Systeme wollen wir uns ein bisschen genauer anschauen.

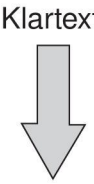
Die „Gartenzaun“-Transposition

Bei der „Gartenzaun“-Transposition werden die Buchstaben des Textes abwechselnd auf zwei Zeilen geschrieben und anschließend wird die zweite Zeile an die erste angehängt:

LIEBERTUGENDHAFTALSJUGENDHAFT

L E E T G N H F A S U E D A T
I B R U E D A T L J G N H F

LEETGNHFASUEDATIBRUEDATLJGNHF



Der Name kommt daher, dass die versetzte Anordnung der Buchstaben auf zwei Zeilen mit etwas Fantasie an einen Gartenzaun erinnert.

1 Du willst einer Freundin folgende traurige Nachricht schicken:

HABEAMSONNTAGKEINEZEITMUSSLERNENSORRY

Verschlüssle den Satz mit der „Gartenzaun“-Transposition.

2 Du hast einen Zettel gefunden, auf dem nur die folgende, ziemlich sinnlos aussehende, Botschaft steht:

LEEMTEOAEENLMTITROLNIBRIVRNKGLASIDEEBHE

Welche Lebensweisheit wollte der Sender dem Empfänger damit wohl mitteilen?

3 Am Vertretungsplan hat ein Witzbold einen Zettel aufgehängt, auf dem steht:

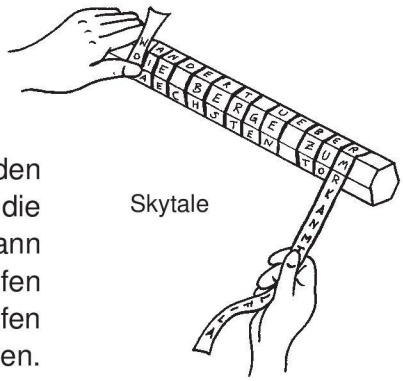
Wichtige Info:
AMTWCFLEDERTNWITNEASMITOHALNIESEZESUDNU

Entschlüssle die Nachricht.

1 *Programmieraufgabe*

Schreibe ein Programm, das einen Klartext mit der „Gartenzaun"-Transposition verschlüsseln kann und zudem einen mit der „Gartenzaun"-Transposition verschlüsselten Geheimtext entschlüsseln kann.

Die Skytale


Skytale

Bei der Skytale (sprich: *Skütale*) handelt es sich um einen Holzstab, um den ein Streifen Leder oder Pergament gewickelt wird. Der Sender schreibt die Nachricht der Länge des Stabes nach auf den Streifen und wickelt ihn dann ab. Liest man die Buchstaben in der Reihenfolge, in der sie auf dem Streifen stehen, ergibt sich nur Kauderwelsch. Der Empfänger wickelt den Streifen um eine Skytale mit demselben Durchmesser und kann die Nachricht lesen.

Dieses Verfahren lässt sich relativ einfach mit einem STABILO-Stift und einem Streifen Papier (ca. 30 cm lang und 5 mm breit) nachvollziehen. Der STABILO-Stift dient dabei als (sechsseitige) Skytale, der Papierstreifen ist unser Pergament (Ende mit Tesafilm festkleben). Zwar funktioniert die Transposition auch mit einem runden Stift, aber mit einem eckigen geht es wesentlich einfacher.

Tipp: Wer es lieber größer mag, kann sich auch mit einer Rolle Klopapier an einem Pfosten versuchen, allerdings reißt das Klopapier relativ schnell ab.

4 Verschlüssle die unten stehende Nachricht mit der STABILO-Skytale. Wechsle dabei nach jeweils 5 Buchstaben auf die nächste STABILO-Seite und achte darauf, dass das erste A ganz oben auf dem Papierstreifen steht.

ALLESGUTEZUMGEBURTSTAGANNEGRET

5

Ein gegnerischer Spion hat bei einer heimlichen Hausdurchsuchung bei dir auf dem Schreibtisch ein Pack STABILOs entdeckt. STABILOs auf dem Schreibtisch sind zwar relativ unauffällig, aber es wäre trotzdem denkbar, dass der Gegner die Verschlüsselung mittels STABILO-Skytale durchschaut hat – als Spion muss man extrem vorsichtig und misstrauisch sein. Du hast deshalb beschlossen, deine geheimen Botschaften ab sofort mit einer achtseitigen Skytale-Codierung zu schützen und dich sicherheitshalber nach Dänemark abzusetzen. Verschlüssle die folgende Botschaft an deinen Kontaktmann und überlege dir vorher, nach wie vielen Buchstaben du auf die nächste Seite der Skytale wechseln musst.

TARNUNGAUFGEFLOGENSTOPBINENTDECKTSTOPFLUCHTNACHDAENEMARK

6

Du sitzt mäßig interessiert im Unterricht und beginnst gerade, dich zu langweilen, als dich ein Papierstreifen mit der folgenden Nachricht erreicht:

KUITKSOHTZEPMETUTIMUAMBESTGBALTEMALEDMISLN

Der Freund, der die Nachricht geschrieben hat, zeigt, als er deinen ratlosen Blick sieht, auf einen STABILO-Stift. Wie lautet die entschlüsselte Botschaft?

7

Es ist dir unter großem Aufwand gelungen, den folgenden Funkspruch abzuhören:

SHLNWRIHIÜATAAENNHTERKDEDNTLDTELDEWLEORLIRIERRSEEPERTWCR

Du vermutest (zu Recht!), die Botschaft könnte mit einer Skytale verschlüsselt worden sein. Leider gibt es aber keinerlei Anhaltspunkte über die Anzahl der Seiten. Es bleibt dir also nichts anderes übrig, als verschiedene Möglichkeiten durchzuprobieren – schließlich könnte die Nachricht die Lösungen der nächsten Mathearbeit enthalten! Doch in diesem Fall hat sich der Sender wohl eher einen Scherz erlaubt. Wie lautet die entschlüsselte Nachricht?

2 *Programmieraufgabe*

Schreibe ein Programm, das einen Klartext mittels einer Skytale verschlüsseln kann (bzw. dies simuliert) und zudem einen mit der Skytale verschlüsselten Geheimtext entschlüsseln kann.

Tipp: Die Skytale-Verschlüsselung ist natürlich davon abhängig, wie viele Buchstaben auf den Streifen passen, wenn dieser genau einmal um den Holzstab gewickelt wird (geht man nicht von einem runden, sondern einem eckigen Stock aus, entspricht diese Zahl der Anzahl der Seiten des Stocks). Da diese Anzahl sowohl für das Ver- als auch für das Entschlüsseln von entscheidender Bedeutung ist, sollte man sie an irgendeiner Stelle im Programm eingeben und auch ändern können. So kann man beim Entschlüsseln quasi verschiedene „Stöcke“ durchprobieren, bis der entschlüsselte Text Sinn macht (und damit die richtige „Stockgröße“ gefunden wurde).