Alles durcheinander – Transpositionschiffren

Skytale

Vor über 2500 Jahren nutzten die Spartaner Skytalen zur Übermittlung von geheimen Nachrichten. Sender und Empfänger besaßen je einen dieser Zylinder. Der Sender wickelte ein schmales Band aus Leder spiralförmig um seine Skytale und schrieb dann der Länge nach die Nachricht auf das Band. War das Band abgewickelt, konnte die Nachricht nur von einer Person gelesen werden, die eine Skytale mit genau denselben Radius hatte.

1) Baue aus einem Bleistift eine Skytale. Kommuniziere verschlüsselt mit einem Partner.

2) Ermittle die Skytale, mit der der gegebene Geheimtext entschlüsseln werden kann.
3) Erläutere eine Strategie, um den Geheimtext auch ohne Skytale zu knacken.
4) Bewerte die Sicherheit des Verfahrens.

Arbeitsauftrag Informatik

Name: **Vorname:** **Klasse:**

Muster und Raster

Hinweis: Unabhängig von Verschlüsselungsverfahren sollten zur besseren Lesbarkeit von Klar- und Geheimtexten diese in Buchstabengruppen gegliedert werden. Die Leerzeichen sind also beim Entschlüsseln zu ignorieren.

Neben dem Verstecken von Texten in Bilden und Zeichnungen wurden gern auch Klartexte in vereinbarte Muster/Quadrate oder Raster geschrieben. Diese Techniken waren bis in die 1950er Jahre beliebte Variante der Verschlüsselung.

5) Bei der 6x6-Quadrat-Matrixverschlüsselung wird der Klartext zeilenweise eingetragen und spaltenweise als Geheimtext entnommen. Beschreibe das Prinzip der Entschlüsselung. Entschlüssle den Geheimtext `MLSBR LAACE UETEH NNSRN RUTEI GENEN XSIDR X`.

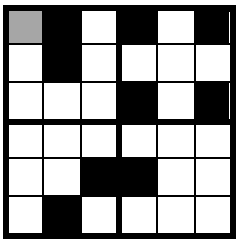
6) Der Geheimtext `ZCTMC EUIAK NSIDS HAGAN CZNNI HETEJ EZKEC UNR` entstand durch Anwendung der Methode $^{Z}\mathrm{I}_{\mathrm{C}_{\mathrm{K}}}\mathrm{Z}\mathrm{A}^{\mathrm{C}}\mathrm{K}$. Was schreibt er?

7) Wie könnte man das Zick-Zack-Methode variabler gestalten? Wird dadurch die Sicherheit des Verfahrens erhöht?

Arbeitsauftrag Informatik

Name: **Vorname:** **Klasse:**

Schablonen (FLEIßNERsche Schablone)



JULES VERNE verwendet in seinem Roman *Mathias Sandorf* die Kunst der Ver- und Entschlüsselung mit Hilfe einer FLEIßNERschen Schablone. Der österreichische Oberst EDUARD FLEIßNER VON WOSTROWITZ entwickelte 1881 eine 6x6-Matrix-Schablone, an der sich befinden an bestimmten Stellen (hier schwarz markiert) Löcher. Die Schablone wird so auf ein Blatt gelegt, dass sich die grauen Ecke oben links befindet. In die Löcher trägt man von rechts oben beginnend zeilenweise die Buchstaben des Klartextes ein. Dann wird die Schablone um ihren Mittelpunkt um neunzig Grad nach rechts gedreht (damit ist das graue Kästchen rechts oben) und die weiteren Buchstaben wieder rechts oben beginnend zeilenweise eingetragen usw.

8) Verschlüssele `HABKE NNWOR TINAL TENBA UMGEL EGTAG ENTOO X.`

9) `CSHCEH LLSAMO SRTUAE RGMEBN ENSSIQ TEBCUA`

   Was schreibt der Absender?

10) Wovon hängt sich Sicherheit des Verfahrens ab?