Knack den Code

Auf einem Bildschirm erscheint eine Folge von Buchstaben, die in Blöcke eingeteilt, auf den ersten Blick aber nicht lesbar sind. Es handelt sich um die codierte (chiffrierte oder „verschlüsselte“) Form eines zunächst unbekannten Textes („Klartext“). Anders ausgedrückt: zu sehen ist nicht der „Klartext“, sondern ein verschlüsselter oder chiffrierter Text, der „Geheimtext“. Die Aufgabe der so genannten Decodierung besteht darin, den Geheimtext in den zugehörigen Klartext zurückzuübersetzen (zu dechiffrieren, d.h. zu übersetzen). Dazu muss der Code „geknackt“ werden, mit dem der Klartext codiert, also verschlüsselt, worden ist.

Die Geheimtexte, die auf dem Bildschirm im ERLEBNISLAND MATHEMATIK erscheinen, wurden nach einem monoalphabetischen Code verschlüsselt. Dieser Code ordnet jedem Buchstaben des Alphabetes genau einen Buchstaben des Geheimtext-Alphabets zu. Ein solcher Code ist seit über 2000 Jahren als die so genannte Cäsar-Verschlüsselung bekannt und berühmt. Sie trägt den Namen des römischen Feldherrn und Imperators, Gajus Julius Cäsar (100 - 44 v.Chr.), der auf diese Weise die Korrespondenz mit seinen Truppen „verschlüsselte“. Das Alphabet des Geheimtextes entsteht einfach dadurch, dass die Reihenfolge der Buchstaben im Alphabet des Klartextes um eine bestimmte Anzahl von Stellen verschoben wird (Translation). Bei einer Verschiebung um vier Stellen wird aus den Buchstaben des Klartext-Alphabets das folgende Geheimtext-Alphabet:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

Will man zum Beispiel ein „geheimes“ Treffen im ERLEBNISLAND MATHEMATIK mit der Freundin oder dem Freund verabreden, würde der Treffpunkt in der Geheimschrift lauten:

I V P I F R M W P E R H Q E X L I Q E X M O.

In der Regel werden bei einem monoalphabetischen Code die Buchstaben des Klartext-Alphabets jedoch nicht gleichmäßig „verschoben“, sondern permutiert, das heißt durcheinander gewürfelt. Ein Beispiel dafür ist die folgende Codierung:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D F G K I J H L M E O P R Q S B U V N X Y A Z T C W

Das ERLEBNISLAND MATHEMATIK hieße in der Geheimschrift nun

I B P I F Q M P D Q K R D X L I R D X M O.

Der Code ist dabei eine (umkehrbar) eindeutige Zuordnung jeweils eines Buchstaben des Klartext-Alphabetes zu einem Buchstaben des Geheimtext-Alphabets. Dafür gibt es $26! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 26 = 403291461126605635584000000$ Möglichkeiten!

Trotz dieser Schwindel erregenden Zahl besteht die Chance, einen solchen Code in überschaubarer Zeit zu knacken. Dazu bedient man sich der sog. Häufigkeitsanalyse. Dabei werden zunächst die Häufigkeiten der einzelnen Buchstaben im Geheimtext festgestellt, und mit den allgemeinen Häufigkeiten der Buchstaben in der Sprache des (unbekannten) Klartextes verglichen. Anschließend werden die Buchstaben im Geheimtext durch die Buchstaben gleicher Häufigkeit in der Sprache ersetzt. Man beginnt mit den häufigsten Buchstaben. Bei den deutschen Klartexten sind das „E“ und „N“. Diese Methode, die an unserem Exponat ausprobiert werden kann (indem man zunächst versucht, das „E“ im Klartext zu finden, dann das „N“, usw.), ist natürlich um so zuverlässiger, je länger der zu dechiffrierende Text ist. Die folgende Tabelle zeigt für deutschsprachige Texte, welche relativen Häufigkeiten die einzelnen Buchstaben des Alphabets hinsichtlich ihres Auftretens besitzen:

Buchstabe	Platz	relative Häufigkeit
E	1.	17,40%
N	2.	9,78 %
I	3.	7,55 %
S	4.	7,27 %
R	5.	7,00 %
A	6.	6,51 %
T	7.	6,15 %
D	8.	5,08 %
H	9.	4,76 %
U	10.	4,35 %
L	11.	3,44 %
C	12.	3,06 %
G	13.	3,01 %
M	14.	2,53 %
O	15.	2,51 %
B	16.	1,89 %
W	17.	1,89 %
F	18.	1,66 %
K	19.	1,21 %
Z	20.	1,13 %
P	21.	0,79 %
V	22.	0,67 %
ß	23.	0,31 %
J	24.	0,27 %
Y	25.	0,04 %
X	26.	0,03 %
Q	27.	0,02 %

Zum Vergleich: Bei einer Gleichverteilung der 27 Buchstaben (einschließlich „ß“) betrüge die Häufigkeit jeweils 3,704 %.

Literatur

[1] Bauer, F.L.: *Entzifferte Geheimnisse. Codes und Chiffren und wie sie gebrochen werden,* Berlin / Heidelberg 1995

[2] Beutelspacher, A. u.a.: *mathematik zum anfassen,* Mathematikum, Gießen 2005

[3] Beutelspacher, A.: *Kryptologie,* 7.Auflage, Wiesbaden 2005

[4] Singh, S.: *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet.* 7.Auflage, München 2006