

Stuchsabenbuppe

Schon im alten Rom verstanden die Kriegsherren, dass es wichtig ist, Informationen zu verschlüsseln. Ein bekanntes Verfahren geht auf Julius Caesar zurück. Beim sogenannten Caesar Verfahren wird jeder Buchstabe im Klartext durch den um drei Stellen im Alphabet folgenden Buchstaben ersetzt. Aus einem A wird ein D, aus einem P ein S usw. Das Wort INFORMATIK wird demnach zum Geheimtext LQIRUPDWLN.

Zur Vereinfachung betrachten wir ausschließlich Großbuchstaben.

Aufgaben:

- a) Verschlüssele das Wort GEHEIM mit diesem Verfahren. 1 Punkt
- b) Der Buchstabe X wird bei dieser Verschlüsselung zum Buchstaben A. Begründe, dass das sinnvoll ist. 2 Punkte

Man kann nicht nur um drei Stellen verschieben, sondern auch um beliebig viele Stellen. Die Information, um wie viele Stellen verschoben wird, nennt man Schlüssel.

- c) Nach einer Verschlüsselung mit dem Schlüssel 17 erhielt man das Wort CVSVEJNVIK. Gib das unverschlüsselte Wort an. 1 Punkt
- d) Ein Wort wurde mit dem Schlüssel 25 verschlüsselt. Du musst das Wort entschlüsseln. Jeden Buchstaben um 25 Stellen „rückwärts“ zu verschieben ist sehr aufwändig. Beschreibe eine schnellere Möglichkeit der Entschlüsselung. 1 Punkt

In Tabellenkalkulationsprogrammen gibt die Funktion `code()` eine Zahl zu einem Zeichen zurück, die Funktion `zeichen()` das Zeichen zu einer Zahl. Solche Funktionen gibt es auch in den meisten Programmiersprachen.

- e) Gib unter Benutzung dieser Funktionen die Zahlen für die Zeichen B und Z und die Zeichen zu den Zahlen 83 und 64 an. 2 Punkte
- f) Beschreibe, wie diese beiden Funktionen dazu eingesetzt werden können, einen Buchstaben um einen vorgegebenen Schlüssel zu „verschieben“. 2 Punkte

Für die nächsten Aufgaben können auch folgende Funktionen der Tabellenkalkulation nützlich sein: `max()`, `suchen()`, `summe()`, `wenn()`, `zählenwenn()`, `rest()`.

- g) Bogdan hat nach diesem Verfahren das Wort INFORMATIX verschlüsselt. Dabei ist der Zettel unten entstanden. Setze dieses Verfahren in eine Computerlösung um, die einen einzugebenden Text verschlüsseln kann. 6 Punkte

Klartext	I	N	F	O	R	M	A	T	I	X
Klartextcode	73	78	70	79	82	77	65	84	73	88
Schlüssel	3									
Geheimtextcode	76	81	73	82	85	80	68	87	76	65
Geheimtext	L	Q	I	R	U	P	D	W	L	A

Im alten Rom konnte es kriegsentscheidend sein, eine verschlüsselte Nachricht entschlüsseln zu können, auch wenn man den Schlüssel nicht kannte.

- h) In Aufgabe c) hast du einen Geheimtext entschlüsselt. Der häufigste Buchstabe im Geheimtext ist V. In der deutschen Sprache tritt der Buchstabe E am häufigsten auf. Beschreibe, wie man mit diesen Informationen den Schlüssel 17 ermitteln kann. 1 Punkt
- i) Erstelle eine Computerlösung, die zu einem Text ermittelt, wie häufig jeder Buchstabe vorkommt. 3 Punkte
- j) Stelle die Daten aus Aufgabe i) grafisch dar. 2 Punkte
- k) Beschreibe ein Verfahren, um einen verschlüsselten Text automatisch zu entschlüsseln, wenn man den Schlüssel nicht kennt. 4 Punkte
- l) Erstelle eine Computerlösung, die zu einem verschlüsselten Text den Schlüssel findet und den Text automatisch entschlüsselt. Zum Testen kannst Du folgenden Geheimtext verwenden:

RVA RUEYVPURE RFRY RURYVPUG RVAR RVASNRYGVTR RHYR

5 Punkte