

Aufgabe 3

Alice und Bob verwenden zum Verschlüsseln ihrer Botschaften die folgende Tabelle. Zur Verschlüsselung bestimmen sie eine mögliche Position des jeweiligen Buchstabens in der Tabelle, z.B. kann „HALLO“ durch 74 88 55 67 14 verschlüsselt werden.

	0	1	2	3	4	5	6	7	8	9
0	N	H	E	D	N	E	R	O	I	E
1	E	M	C	S	O	E	B	S	G	N
2	T	R	A	E	T	H	I	E	S	T
3	A	E	G	D	W	R	N	D	N	U
4	L	U	I	K	E	D	C	Z	M	S
5	N	S	D	N	T	L	J	I	Q	N
6	R	E	B	P	I	N	O	L	I	V
7	E	G	E	S	H	Y	E	F	S	A
8	I	N	F	R	U	R	X	R	A	H
9	T	E	C	M	A	E	E	T	E	I

- a) Entschlüsseln Sie das folgende Chifftrat:
74 05 41 29 31 88 62 91 65 52 41 93 47 15 89 81 84 04 97 23 83 03 96 35 62 35 84 15 12 43 44
Diskutieren Sie die Vorteile dieses Verfahrens gegenüber einer Verschlüsselung nach dem Cäsar-Verfahren.
- b) Zur Umsetzung dieses Verschlüsselungsverfahrens in einem Programm soll eine Operation `suche` verwendet werden, die zu einem zu chiffrierenden Buchstaben eine passende Position findet und diese als Zeichenkette aus zwei Zeichen zurückgibt. In dieser Operation wird solange eine Stelle zufällig in der Tabelle bestimmt, bis man den zu chiffrierenden Buchstaben gefunden hat. Implementieren Sie diese Operation unter Verwendung der Vorgaben im Material.
- c) In der Kryptoanalyse wird neben der Buchstabenhäufigkeit auch die Häufigkeit von Buchstabenpaaren (Bigrammen) untersucht. In deutschsprachigen Texten treten z.B. die Bigramme EN, ER, CH, TE, DE, ND, EI, IE, IN und ES besonders häufig auf.
Erstellen Sie einen Algorithmus in schriftlich verbalisierter Form, mit dem die zehn häufigsten Bigramme eines Textes bestimmt werden können.

Zentralabitur 2010	Informatik	Schülermaterial
Aufgabe II	gA	Bearbeitungszeit: 220 min

Material

Zu Aufgabe 3b)

in Java:

```
char [][] tabelle = {{'N','H','E','D','N','E','R','O','I','E'},
                    {'E','M','C','S','O','E','B','S','G','N'},
                    {'T','R','A','E','T','H','I','E','S','T'},
                    {'A','E','G','D','W','R','N','D','N','U'},
                    {'L','U','I','K','E','D','C','Z','M','S'},
                    {'N','S','D','N','T','L','J','I','Q','N'},
                    {'R','E','B','P','I','N','O','L','I','V'},
                    {'E','G','E','S','H','Y','E','F','S','A'},
                    {'I','N','F','R','U','R','X','R','A','H'},
                    {'T','E','C','M','A','E','E','T','E','I'}}
```

in Pascal / Delphi:

```
var tabelle : ARRAY[0..9,0..9] of CHAR =
    (('N','H','E','D','N','E','R','O','I','E'),
     ('E','M','C','S','O','E','B','S','G','N'),
     ('T','R','A','E','T','H','I','E','S','T'),
     ('A','E','G','D','W','R','N','D','N','U'),
     ('L','U','I','K','E','D','C','Z','M','S'),
     ('N','S','D','N','T','L','J','I','Q','N'),
     ('R','E','B','P','I','N','O','L','I','V'),
     ('E','G','E','S','H','Y','E','F','S','A'),
     ('I','N','F','R','U','R','X','R','A','H'),
     ('T','E','C','M','A','E','E','T','E','I'))
```

Für die zufällige Bestimmung einer Stelle in der Tabelle können Sie eine Operation zur Erzeugung einer Zufallszahl voraussetzen, die eine ganzzahlige Zufallszahl zwischen 0 und $n - 1$ (einschließlich der Grenzen) liefert:

in Java: `public int zufallszahl(int n)`

in Pascal / Delphi: `function zufallszahl(n:integer):integer`