Aufgabe 3

Der Engländer Sir Charles Wheatstone veröffentlichte 1854 ein Chiffrierverfahren, das unter dem Namen seines Freundes Lyon Playfair bekannt wurde. Es wurde z. B. von der britischen Armee im 1. Weltkrieg verwendet und in einer Variante von der deutschen Wehrmacht noch im 2. Weltkrieg benutzt.

Die grundlegende Idee bei der Playfair-Verschlüsselung besteht darin, dass jedes Buchstabenpaar im Klartext durch ein anderes Buchstabenpaar ersetzt wird.

Zunächst vereinbaren Sender und Empfänger ein Schlüsselwort. Dieses Schlüsselwort wird in ein 5 x 5-Quadrat geschrieben, wobei mehrfach vorkommende Buchstaben beim zweiten, dritten, ... Auftreten gestrichen werden. Die restlichen Felder des Quadrats werden mit den übrigen Buchstaben des Alphabets aufgefüllt. Außerdem werden die Buchstaben I und J zum Buchstaben I zusammengefasst.

Der Klartext wird zur Verschlüsselung in Buchstabenpaare aufgeteilt. Bei der Verschlüsselung sind drei Fälle zu unterscheiden:

1. Die Buchstaben stehen in derselben Zeile: Sie werden ersetzt durch die unmittelbar rechts stehenden Buchstaben (ggf. wird die Zeile zyklisch fortgesetzt).
2. Die Buchstaben stehen in derselben Spalte: Sie werden ersetzt durch die unmittelbar darunter stehenden Buchstaben (ebenfalls ggf. mit zyklischer Fortsetzung der Spalte).
3. Anderenfalls bilden die Buchstaben ein Rechteck: Dann werden die Buchstaben ersetzt durch diejenigen Buchstaben, die in den anderen Ecken des Rechtecks stehen. Dabei ist der erste Chiffre-Buchstabe derjenige, der in derselben Zeile wie der erste Klartext-Buchstabe steht.

Falls zwei gleiche Buchstaben im Klartext aufeinander folgen, wird ein X dazwischen gesetzt. Ein X wird an den Klartext angehängt, falls die Anzahl der Buchstaben ungerade ist.

Beispiel:
Das Schlüsselwort ist WEINHEIM.

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

Beispiele zur Verschlüsselung von Buchstabenpaaren:

LG $\rightarrow$ OK

TZ $\rightarrow$ ZH

PC $\rightarrow$ SM

a) Verschlüsseln Sie das Wort PLAYFAIR. Das Schlüsselwort sei MANCHESTER.
Entschlüsseln Sie den folgenden Text. Das Schlüsselwort sei wiederum MANCHESTER.

NCITKGWGESFRPANTTMHOGINCPN

b) Vergleichen Sie das Playfair-Verfahren mit anderen klassischen Chiffrierverfahren und beurteilen Sie die Sicherheit des Playfair-Verfahrens.
Manchmal werden zwei Verschlüsselungsverfahren nacheinander auf dieselbe Nachricht angewendet (so genannte Überschlüsselung). Erläutern Sie, wie eine zusätzliche Verschlüsselung nach dem Verfahren von Vigenère die Sicherheit verändern würde.

c) Der Algorithmus zum Verschlüsseln kann in Schritte unterteilt werden:

Vorbereiten des Klartextes (X einfügen bzw. mit X auffüllen)
Die eigentliche Verschlüsselung:
Für jedes Buchstabenpaar des modifizierten Klartextes wiederhole:
(i) Bestimme die Positionen des ersten und des zweiten Buchstabens in dem Playfair-Quadrat.
(ii) Bestimme die Buchstaben des zugehörigen Geheimtextpaares.
(iii) Hänge das soeben ermittelte Paar an den bereits ermittelten Geheimtext an.

Schreiben Sie für Teil (ii) in Java bzw. Pascal / Delphi eine Operation

```
String ermittlePaar(int x1, int y1, int x2, int y2)
```

bzw.

```
function ermittlePaar(x1, y1, x2, y2: integer): String;
```

die aus den Positionen (x1 | y1) und (x2 | y2) der Buchstaben des Klartextpaares im Playfair-Quadrat das Buchstabenpaar des Geheimtextes ermittelt.
Das Playfair-Quadrat wird in der globalen Variablen

```
char[][] quadrat = new char[5][5];
```

bzw.

```
quadrat: array[0..4,0..4] of char;
```

gespeichert.