2. Die Playfair-Chiffre

PLAYFAIR-Verschlüsselung:

(1) Als Alphabet liegen die 25, von J verschiedenen Großbuchstaben zugrunde. Kommt der Buchstabe J in einem Text vor, ersetzt man ihn durch I.

(2) Ein Code-Wort wird Buchstabe für Buchstabe in eine 5×5-Matrix $M = (a_{i,j})_{0\leq i,j\leq 4}$geschrieben. Steht ein Buchstabe bereits in der Matrix, wird er übergangen. Der Rest der Matrix wird mit den restlichen Buchstaben des Alphabets in alphabetischer Reihenfolge aufgefüllt. (Die Matrix enthält dann alle 25, von J verschiedenen Großbuchstaben.) Beispielsweise liefert das Code-Wort 'KRYPTOGRAPHIE' die Matrix

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

(3) Der Ausgangstext wird in Blöcke der Länge 2 unterteilt, eventuell der Buchstabe X eingefügt oder angehängt, damit alle Blöcke aus zwei verschiedenen Zeichen bestehen. Der Text 'WASSER' wird also zu 'WA SX SE RX'.

(4) Ist jetzt ein Block gegeben, so schreibt man diesen als a_{i_1,j_1}, a_{i_2,j_2}, d.h. das erste Zeichen hat Zeilenindex i_1 und Spaltenindex j_1, das zweite entsprechend i_2 und j_2. Man unterscheidet nun 3 Fälle:
- Ist $i_1 = i_2$, so wird der Block zu $a_{i_1,j_1+1}, a_{i_2,j_2+1}$ verschlüsselt, wobei die Indizes modulo 5 zu betrachten sind.
- Ist $j_1 = j_2$, so wird der Block zu $a_{i_1+1,j_1}, a_{i_2+1,j_2}$ verschlüsselt, wobei die Indizes modulo 5 zu betrachten sind.
- Ist $i_1 \neq i_2$, $j_1 \neq j_2$, so wird der Block zu a_{i_1,j_2}, a_{i_2,j_1} verschlüsselt.

'WA SX SE RX' wird mit obigem Code-Wort also zu 'YC QZ LF PV'.

(5) Entschlüsselung: Man erstellt aus dem Code-Wort wie zuvor eine 5×5-Matrix. Einen Block des verschlüsselten Texts schreibt man als a_{i_1,j_1}, a_{i_2,j_2}, d.h. das erste Zeichen hat Zeilenindex i_1 und Spaltenindex j_1, das zweite entsprechend i_2 und j_2. Man unterscheidet nun 3 Fälle:
- Ist $i_1 = i_2$, so wird der Block zu $a_{i_1,j_1-1}, a_{i_2,j_2-1}$ entschlüsselt, wobei die Indizes modulo 5 zu betrachten sind.
- Ist $j_1 = j_2$, so wird der Block zu $a_{i_1-1,j_1}, a_{i_2-1,j_2}$ entschlüsselt, wobei die Indizes modulo 5 zu betrachten sind.
- Ist $i_1 \neq i_2$, $j_1 \neq j_2$, so wird der Block zu a_{i_1,j_2}, a_{i_2,j_1} entschlüsselt.

Beispiel: Wir wollen 'Die klassische Aufgabe der Kryptographie ist es, eine Nachricht oder Aufzeichnung für den Unbefugten unverständlich zu machen' mit dem Passwort KRYPTOGRAPHIE Playfair-chiffrieren. Im ersten Schritt unterteilen wir den Text in Bigramme und fügen eventuell ein X ein:

```
DI EK LA SX SI SC HE AU FG AB ED ER KR YP TO GR AP HI EI ST ES EI NE NA CH RI CH TO
DE RA UF ZE IC HN UN GF UE RD EN UN BE FU GT EN UN VE RS TA EN DL IC HZ UM AC HE NX
```

Mit dem Playfair-Quadrat von oben (zum Passwort KRYPTOGRAPHIE) verschlüsseln wir nun:

```
FH LO NO QZ ZF NF OD OW BI GC BF BK RY PT KI BG HY IO FO ZI FL FO LC WC DA TG DA KI
FB YG ZE UF AF AQ WL IB KL PB CL WL CB EZ IR CL WL UB TM YI CL EQ AF IX VL CN OD QW
```

Ein historisches Beispiel: Im 2. Weltkrieg sandte der spätere US-Präsident John F. Kennedy folgende mit dem Kennwort ‘ROYAL NEW ZEALAND NAVY’ Playfair-verschlüsselte Nachricht ab [David Kahn. The Codebreakers. S.592]:

```
KXIEY UREBE ZWEHE WRYTU HEYFS
KREHE GOYFI WTTTU OLKSY CAIPO
BOTEI ZONTX BYBWT GONEY CUZWR
GDSON SXBOU YWRHE BAAHY USEDQ
```

Lässt man das Digramm ‘TT’ in der zweiten Zeile einfach stehen, da es als Playfair-Verschlüsselung nicht auftreten kann, so erhält man mit dem zum Passwort gehörigen Quadrat

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

die Entschlüsselung:

```
PTBOA TONEO WENIN ELOST INACT
IONIN BLACK ETTST RAITT WOMIL
ESSWM ERESU COCEX CREWO FTWEL
VEXRE QUEST ANYIN FORMA TIONX
```

und etwas umgeschrieben:

```
PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO MILES SW MERESU COCE X
CREW OF TWELVE X REQUEST ANY INFORMATION X
```

(Statt ‘MERESU COCE’ muss es wohl ‘MERESU COVE’ heißen, also sollte an entsprechender Stelle im verschlüsselten Text ‘BN’ statt ‘BW’ stehen.)