5. Die ADFGVX-Chiffrierung

Schon Polybius soll das folgende Verschlüsselungsverfahren benutzt haben: Man identifiziert J mit I, schreibt die verbleibenden 25 Buchstaben A,...,Z in ein 5×5-Quadrat, eventuell unter Benutzung eines Kennworts, und nummeriert Zeilen und Spalten. (So etwas nennt man auch ein Polybius-Quadrat.) Ein Buchstabe entspricht dann also einem Zahlenpaar. Beispielsweise erhält man mit 'SEMESTERFERIEN' das Quadrat

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

und das Wort 'MATHEMATIK' wird zu '13 24 14 34 12 13 24 14 22 35'. Eine verschlüsselte Nachricht wird immer aus einer geraden Anzahl der Ziffern 1,2,3,4,5 bestehen, eine Häufigkeitsanalyse von Ziffernpaaren hilft beim Entschlüsseln.

Ersetzen wir die Ziffern 1,2,3,4,5 durch die Buchstaben A,D,F,G,X, so erhalten wir ein Verfahren, das im 1. Weltkrieg auf deutscher Seite ab März 1918 benutzt wurde.

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

Allerdings wurde dann im entstehenden Text noch eine Buchstabenvertauschung durchgeführt. Ab Juni 1918 wurde dann noch der Buchstabe V hinzugenommen. Die Buchstaben A,D,F,G,V,X lassen sich beim Funken unter Verwendung des Morse-Alphabets gut unterscheiden:

$$\mathrm{A} = \cdot - \quad \mathrm{D} = - \cdot \cdot \quad \mathrm{F} = \cdot \cdot - \cdot \quad \mathrm{G} = - - \cdot \quad \mathrm{V} = \cdot \cdot \cdot - \quad \mathrm{X} = - \cdot \cdot -$$

Das ADFGVX-Verschlüsselungsverfahren:

(1) Das Klartextalphabet besteht aus 36 Zeichen, den Buchstaben A,...,Z und den Ziffern 0,1,...,9. Das Chiffretextalphabet aus den Zeichen A,D,F,G,V,X.

(2) Als ersten Teil eines Schlüssels stellt man eine 6×6-Matrix auf, die die 36 Zeichen a,...,z,0,...,9 enthält. Die Zeilen und Spalten werden mit den Buchstaben A, D, F, G, V, X bezeichnet. Ein Beispiel ist

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

(3) Eine aus den Zeichen A,...,Z,0,...,9 bestehende Zeichenfolge wird jetzt in eine aus A,D,F,G,V,X bestehende Zeichenfolge umgewandelt, indem ein Zeichen mit Hilfe obiges Quadratrs durch das entsprechende Paar (Zeilenindex,Spaltenindex) ersetzt wird. Beispielsweise wird aus '14TAGE' dann 'VDAXXGDGXXXA'.

(4) Als zweiten Teil eines Schlüssels wählt man eine natürliche Zahl n und eine Permutation π der Zahlen von 1 bis n. Wir schreiben die Zeichenfolge jetzt zeilenweise in eine Matrix mit n Spalten, erhalten also eine Matrix a_{ij} mit $j = 1, \ldots, n$. Nun werden die Spalten mit obiger Permutation vertauscht:

$$b_{i,j} = a_{i,\pi(j)}.$$

Schreibt man die Matrix $b_{i,j}$ jetzt spaltenweise aus, so erhält man die chiffrierte Zeichenfolge:

$$b_{1,1}, b_{2,1}, b_{3,1}, \ldots, b_{1,2}, b_{2,2}, b_{3,2}, \ldots\ldots b_{1,n}, b_{2,n}, b_{3,n}, \ldots$$

Beispiel: Wir wollen '14TAGE' verschlüsseln mit obigem 6×6-Quadrat. Aus '14TAGE' erhalten wir zunächst die Buchstabenfolge 'VDAXXGDGXXXA'. Für den nächsten Schritt wählen wir als Zeilenlänge $n = 4$ und die Permutation

i	1	2	3	4
$\pi(i)$	3	1	4	2

Wir ordnen den Text jetzt als Matrix mit 4 Spalten an

VDAX		AVXD
XGDG	und vertauschen die Spalten:	DXGG
XXXA		XXAX

Der Chiffretext ist dann 'ADXVXXXGADGX'.

Ein historisches Beispiel Am 3. Juni 1918 fingen die Franzosen den folgenden chiffrierten Funkspruch auf. (D. Kahn, The Codebreakers, S.346)

```
FGAXA XAXFF FAFFA AVDFA GAXFX FAAAG DXGGX AGXFD XGAGX GAXGX
AGXVF VXXAG XFDAX GDAAF DGGAF FXGGX XDFAX GXAXV AGXGG DFAGD
GXVAX XFXGV FFGGA XDGAX ADVGG A
```

Wir wollen ihn entschlüsseln unter der Annahme, dass er mit obigem 6×6-Quadrat, der Zeilenlänge $n = 21$ und der Permutation π

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$\pi(i)$	12	6	18	15	4	1	3	16	10	8	19	14	11	7	9	2	5	21	17	20	13

verschlüsselt wurde. Der Text hat 126 Zeichen. Wir schreiben ihn spaltenweise in eine 6×21-Matrix:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
F	A	F	F	X	D	G	A	G	F	X	D	G	G	X	A	F	V	G	A	A
G	X	F	A	F	X	X	G	X	V	F	A	A	X	G	G	A	A	V	X	D
A	F	A	G	A	G	F	X	A	X	D	A	F	X	X	X	G	X	F	D	V
X	F	A	A	A	G	D	G	G	X	A	F	F	D	A	G	D	X	F	G	G
A	F	V	X	A	X	X	A	X	A	X	D	X	F	X	G	G	F	G	A	G
X	A	D	F	G	A	G	X	V	G	G	G	G	A	V	D	X	X	G	X	A

Mit der inversen Permutation π^{-1}

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$\pi^{-1}(i)$	6	16	7	5	17	2	14	10	15	9	13	1	21	12	4	8	19	3	11	20	18

vertauschen wir jetzt die Spalten:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
D	A	G	X	F	A	G	F	X	G	G	F	A	D	F	A	G	F	X	A	V
X	G	X	F	A	X	X	V	G	X	A	G	D	A	A	G	V	F	F	X	A
G	X	F	A	G	F	X	X	X	A	F	A	V	A	G	X	F	A	D	D	X
G	G	D	A	D	F	D	X	A	G	F	X	G	F	A	G	F	A	A	G	X
X	G	X	A	G	F	F	A	X	X	X	A	G	D	X	A	G	V	X	A	F
A	D	G	G	X	A	A	G	V	V	G	X	A	G	F	X	G	D	G	X	X

Jetzt schreiben wir den Text zeilenweise ab und fassen je zwei Buchstaben zusammen:

```
DA GX FA GF XG GF AD FA GF XA VX GX FA XX VG XA GD AA GV FF XA GX FA GF XX
XA FA VA GX FA DD XG GD AD FD XA GF XG FA GF AA GX XG XA GF FA XX XA GD XA
GV XA FA DG GX AA GV VG XA GF XG DG XX
```

Wenden wir jetzt die 6×6-Matrix darauf an, so erhalten wir

MUNITIONIERUNGBESCHLEUNIGENPUNKTSOWEITNICUTEINGESEHENAUCHBEITAG,

also ‘MUNITIONIERUNG BESCHLEUNIGEN PUNKT SOWEIT NICUT EINGESEHEN AUCH BEI TAG’, wobei ‘NICUT’ wohl ein Schreibfehler war und ‘NICHT’ bedeuten soll (H↔GV, U↔GX).

Die deutsche ADFGVX-Chiffrierung wurde allerdings von französischer Seite schnell entschlüsselt, durch den Kryptologen Georges Painvin. (Painvin bekam am 1. Juni 1918 die erste mit ADFGVX chiffrierte Nachricht, am Abend des 2. Juni hatte er sie bereits entschlüsselt.)