Die ADFGVX-Chiffrierung[1]

Polybius-Verschlüsselung: 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.) Jeder Buchstaben z hat dann einen Zeilenindex i und einen Spaltenindex j. Beim Verschlüsseln wird z durch das Zahlenpaar ij ersetzt.

Beispiel: Wir bilden mit dem Schlüsselwort „SEMESTERFERIEN“ das Polybius-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

Das Wort „MATHEMATIK“ wird zu „13 24 14 34 12 13 24 14 22 35“ verschlüsselt.

[1] Version: 9.1.2025

Bemerkung: Die Polybius-Verschlüsselung ist einfach eine Substitutionschiffrierung mit Klartextalphabet

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

und Geheimtextalphabet
11,12,13,14,15,21,22,23,24,25,31,32,33,34,35,41,42,43,44,45,51,52,53,54,55

Ersetzt man im Polybius-Quadrat die Ziffern 1,2,3,4,5 durch die Buchstaben A,D,F,G,X, so erhält man 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. Damit erhält man ein 6×6-Schlüsselquadrat, man hat also 36 Zeichen für den Klartext zur Verfügung, beispielsweise die 26 Großbuchstaben A,...,Z und die 10 Ziffern 0,...,9.
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:

- 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.
- Die Verschlüsselung geschieht in zwei Schritten, einer Polybius-Verschlüsselung und einer TRANSSPA-Verschlüsselung (Spaltentransposition).
- 1. Verschlüsselungsschritt (Polybius-Verschlüsselung):
  - Der erste Schlüssel besteht aus einer 6×6-Matrix, die die Buchstaben A,...,Z und die Ziffern 0,...,9 enthält, deren Zeilen und Spalten mit A,D,F,G,V,X bezeichnet sind.
    - Man kann die Matrix auch durch ein Schlüsselwort s_1 erzeugen, bei dem nur Großbuchstaben A,...,Z und Ziffern 0,...,9 berücksichtigt werden: Man hängt an s_1 die Zeichen ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 an und streicht dann (von links nach rechts) alle Zeichen heraus, die schon vorkamen. Dann schreibt man s_1 zeilenweise in die Schlüsselmatrix.
  - Im Klartext a wird nun jedes Zeichen das zugehörige Buchstabenpaar (Zeilenindex,Spaltenindex) ersetzt. Man erhält dann eine Zeichenkette b, die nur die Buchstaben A,D,F,G,V,X enthält.

- 2. Verschlüsselungsschritt (TRANSSPA-Verschlüsselung):
  - Dies ist einfach eine TRANSSPA-Verschlüsselung, eine Spaltentransposition. Den Schlüssel kann man durch ein Schlüsselwort s_2 oder eine Liste von Zahlen angeben, aus der ersichtlich wird, in welcher Reihenfolge die Spalten auszulesen sind. Die (aus A,D,F,G,V,X bestehende) Zeichenkette b wird mit dem Schlüssel s_2 zu c TRANSSPA-Verschlüsselt.
  - c ist der Chiffretext der ADFGVX-Verschlüsselung von a.
- **Entschlüsselung:**
  - Zunächst wird mit dem Schlüssel s_2 der Chiffretext c zu b TRANSSPA-entschlüsselt.
  - Mit dem Schlüssel s_1 wird dann die Polybius-Verschlüsselung rückgängig gemacht und man erhält aus b den Klartext a.

Beispiel: Wir wollen „101 IST EINE PRIMZAHL“ verschlüsseln, wobei als erstes Schlüsselwort „JANUAR 2025“ und als zweites Schlüsselwort „EISREGEN“ verwendet werden soll. Wir stellen zunächst die Schlüsselmatrix zu „JANUAR 2025“ auf:

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

Aus „101 IST EINE PRIMZAHL“ wird nun

```
VX DA VX FG GV GX DX FG AF DX GF AV FG GA VV AD FF FX
```

Für die TRANSSPA-Verschlüsselung legen wir eine Tabelle an und bezeichnen die Spalten mit E,I,S,R,E,G,E,N, wobei wir darunter gleich die Reihenfolge schreiben, in der die Spalten später ausgelesen werden:

```
E I S R E G E N
1 5 8 7 2 4 3 6
- - - - - - - -
```

Nun tragen wir
`VX DA VX FG GV GX DX FG AF DX GF AV FG GA VV AD FF FX`
zeilenweise in die Matrix ein:

```
E I S R E G E N
1 5 8 7 2 4 3 6
- - - - - - - -
V X D A V X F G
G V G X D X F G
A F D X G F A V
F G G A V V A D
F F F X
```

Nun wird der Text spaltenweise ausgelesen, wobei die Reihenfolge der Spalten durch das Schlüsselwort bestimmt wird:

`VGAFF VDGV FFAA XXFV XVFGF GGVD AXXAX DGDGF`

oder in 5-er Blöcken geschrieben:

`VGAFF VDGVF FAAXX FVXVF GFGGV DAXXA XDGDG F`

(Dies ist der Chiffretext.)

Ein historisches Beispiel Am 3. Juni 1918 fingen die Franzosen den folgenden chiffrierten Funkspruch auf. (D. Kahn. The Codebreakers. 1996. 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 dem Schlüsselquadrat

	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

und der Spaltenreihenfolge

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

verschlüsselt wurde. Der Chiffretext hat 126 Zeichen, es gibt 21 Spalten, wegen $126 = 6 \cdot 21$ enthält jede Spalte 6 Zeichen. Wir legen eine Tabelle mit 21 Zeichen an, füllen die Tabelle dann spaltenweise auf, wobei die Spaltenreihenfolge durch die darüber stehenden Zahlen gegeben ist:

6	16	7	5	17	2	14	10	15	9	13	1	21	12	4	8	19	3	11	20	18
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 lesen wir den Text zeilenweise aus 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
```

Entschlüsseln wir dies mit der 6×6-Schlüsselmatrix, 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$\leftrightarrow$GV, U$\leftrightarrow$GX).

Bemerkungen:

- Die deutsche ADFGVX-Chiffrierung wurde allerdings von französischer Seite schnell entschlüsselt, und zwar durch Georges Painvin. Er bekam am 1. Juni 1918 die erste mit ADFGVX chiffrierte Nachricht, am Abend des 2. Juni hatte er sie bereits entschlüsselt. (R. Kippenhahn. Verschlüsselte Botschaften. 2012. S.215)
- Mir ist nicht klar, wie die Schlüssel angegeben wurden. Die Schlüsselmatrix

	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

lässt sich zwar durch

`CO8XF4 MK3AZ9 NWL0JD 5SIYHU P1VB6R EQ7T2G`

beschreiben, was aber nicht viel bringt.
Den Schlüssel für die TRANSSPA-Verschlüsselung (Spaltentransposition) kann man wie oben durch

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

angeben, oder auch durch „FPGEQBNJOIMAULDHSCKTR“ oder durch „EKEDKBJGJFIANHCELBGMK“.