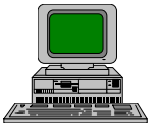

Die ADFGVX-Verschüsselung
(auch Polybios-Verschlüsselung)

Im Jahr 1900 erfand der deutschen Physiker Karl Ferdinand Braun die drahtlose Telegrafie. Damit war es möglich auch ohne Kabelverbindung Morsezeichen mittels Funkwellen von einem Sender zu einem Empfänger zu übertragen. Braun erhielt für seine Erfindung 1909 den Nobelpreis für Physik. Diese Technik wurde in Militärkreisen sehr schnell als wichtig erkannt, da sie zum Beispiel die Verbindung zu Marineeinheiten auf hoher See oder gar transatlantische Funksprüche (in Form von Morsezeichen) ermöglichte.

Selbstverständlich konnen derartige Funksprüche sehr leicht abgehört werden. Deshalb war es von höchster militärischer Priorität die Funksprüche so zu verschlüsseln, dass die Gegenseite ihren Inhalt trotz Abhören nicht entschlüsseln konnte.

Der deutsche Nachrichtenoffizier Oberst Fritz Nebel (1891-1967) entwickelte ein Verschlüsselungsverfahren, das am 1. März 1918 erstmals verwendet wurde: die ADFGX-Verschlüsselung. In der Folge wurde dieses Verfahren ausgebaut und es entstand die ADFGVX-Verschlüsselung, welche ab dem 1. Juni 1918 von den Deutschen eingesetzt wurde.

Das ADFGX- und auch das ADFGVX-Verfahren sind zweistufig aufgebaut und bestehen zuerst aus einer monoalphabetischen Verschlüsselung (sog. Substitution) und anschliessend aus einer Vertauschung der Zeichen (sog. Transposition). Der Mechanismus wird weiter unten an einem konkreten Beispiel erläutert.


Georges Painvin

Das Knacken der ADFGX-Verschlüsselung gelang dem französischen Artillerie-Offizier Captain Georges Painvin noch im April 1918 (und dadurch auch das spätere Knacken der ADFGVX-Verschlüsselung, das nach dem gleichen Prinzip funktioniert).

Die wesentliche Schwäche des Verfahrens ist die einfache monoalphabetische Substitution in der ersten Stufe. Insofern besteht die kryptographische Sicherheit des ADFGX-Verfahrens (und auch des ADFGVX-Verfahrens) hauptsächlich im Zerreissen des Textes mit Hilfe der Transposition. Das Verfahren ist daher im Grunde nur einstufig. Gelingt es, die Transposition zu knacken, kann der Klartext leicht rekonstruiert werden.

Beispiel einer ADFGVX-Verschlüsselung

Klartext: `neuen bereitschaftsraum in planquadrat x24`

Schlüsselwort für Substitution: `hinterhalt`

Schlüsselwort für Transposition: `beobachtungsposten`

Für den ersten Teil der Verschlüsselung (Substitution) wird ein Polybios-Qudrat (vgl. Abbildung auf der nächsten Seite) erstellt. Dazu werden die Buchstaben A, D, F, G, V, X[1] sowohl waagrecht wie auch senkrecht als Beschriftung hingeschieben. Auf diese Weise entsteht ein Quadrat mit 36 Plätzen. In die 36 Plätze werden nun die 26 Buchstaben und die Ziffern 0-9 eingefügt. Begonnen wird mit den Buchstaben des Schlüsselwortes für die Substitution, wobei doppelt vorkommende Buchstaben (hier `h` und `t`) nur einmal genommen. Aus `hinterhalt` wird somit `hinteral`. Die restli-

[1] Die Buchstaben ADFGVX wurden ausgewählt, weil sie sich im Morsealphabet gut unterscheiden lassen.

chen Plätze werden mit den noch nicht verwendeten Buchstaben und Zahlen aufgefüllt (vgl. Abbildung).

	A	D	F	G	V	X
A	h	i	n	t	e	r
D	a	l	b	c	d	f
F	g	j	k	m	o	p
G	q	s	u	v	w	x
V	y	z	0	1	2	3
X	4	5	6	7	8	9

Polybios-Quadrat

Als nächstes wird jeder Klartextbuchstabe durch ein Buchstabenpaar, bestehend aus Zeilen- und Spaltenbuchstabe, ersetzt. Aus `n` wird somit `AF`, aus `e` wird `AV` und so weiter.

Es ergibt sich also folgender Zwischentext:

```
n  e  u  e  n  b  e  r  e  i  t  s  c  h  a  f  t  s  r  a  u
AF AV GF AV AF DF AV AX AV AD AG GD DG AA DA DX AG GD AX DA GF

m  i  n  p  l  a  n  q  u  a  d  r  a  t  x  2  4
FG AD AF FX DD DA AF GY GF DA DV AX DA AG GX VV XA
```

Als Vorbereitung für die Transposition wird nun das Schlüsselwort für die Transposition (hier `beobachtungsposten`) hingeschrieben. Es sollte eine Wortlänge von üblicherweise 15-22 Buchstaben haben. Die Buchstaben des Schlüsselwortes werden alphabetisch nummeriert, wobei gleiche Buchstaben nacheinander verschiedene Nummern bekommen. Dann wird der Zwischentext Zeile für Zeile unter dem Schlüsselwort (und der Nummerierung) hingeschrieben.

```
b  e  o  b  a  c  h  t  u  n  g  s  p  o  s  t  e  n
2  5  11 3  1  4  8  16 18 9  7  14 13 12 15 17 6  10
A  F  A  V  G  F  A  V  A  F  D  F  A  V  A  X  A  V
A  D  A  G  G  D  D  G  D  G  A  A  D  A  D  X  A  G
G  D  A  X  D  A  G  F  F  G  A  D  A  F  F  X  D  D
D  A  A  F  G  Y  G  F  D  A  D  V  A  X  D  A  A  G
G  X  V  V  X  A
```

Der Geheimtext ist nun das Aneinanderreihen der Spalten, in der Reihenfolge der Nummerierung der Schlüsselwortbuchstaben. Zuerst also die Spalte unter dem Buchstaben `a` nämlich `GGDGX`, gefolgt von der Spalte unter dem ersten `b`, also `AAGDG`. Der gesamte Geheimtext lautet also wie folgt, wobei die Buchstaben der besseren Lesbarkeit wegen in 5er-Gruppen aufgeteilt wurden:

```
GGDGX AAGDG VGXFV FDAYA FDDAX AADAD AADAD
GGFGG AVGDG AAAAV VAFXA DAAFA DVADF DVGFF
XXXAA DFD
```

Welche Schlüsselwörter?
Um das Verfahren noch sicherer zu machen, wurden die Schlüsselwörter täglich gewechselt. Die Wörter waren in sogenannten Codebüchern verzeichnet. Aus Sicherheitsgründen mussten auch die Codebücher gelegentlich ausgewechselt werden, was eine ziemliche logistische Leistung bedeutet.

Für die Entschlüsselung des Geheimtextes ist in Umgekehrter Reihenfolge vorzugehen. Zuerst werden die 5er-Gruppen in die entsprechenden Spalten gesetzt. Dabei ist durch die Gesamtzahl der Buchstaben auszurechnen, wieviele Buchstaben pro Spalte notwendig sind. Anschliessend kann die monoalphabetische Verschlüsselung mit Hilfe des Polybios-Quadrats entschlüsselt werden.

Weiterführende Links (15.12.06)

http://de.wikipedia.org/wiki/ADFGVX
http://www.apprendre-en-ligne.net/crypto/subst/adfgvx.html