Teil 2.2 Die Vigenere-Verschlüsselung

➔ **Video:**

- http://perm.ly/kryptologie-vigenere-verfahren

Die Schwäche des Caesar-Verfahrens, und allen übrigen monoalphabetischen Verfahren, beruht darauf, dass die Häufigkeit der Buchstaben erhalten bleibt: Ein und derselbe Buchstabe wird immer durch denselben Buchstaben ersetzt. Solche Verfahren sind relativ leicht zu attackieren (siehe Kryptoanalyse - Häufigkeitsanalyse). Eine bessere Verschlüsselung würde also ein Verfahren bieten, das ein und demselben Buchstaben aus einem Klartext unterschiedliche Buchstaben im Geheimtext zuordnet. Diese Verfahren sind sogenannte polyalphabetische Verfahren. Der Name polyalphabetisch leitet sich daraus ab, dass bei der Verschlüsselung jeweils unterschiedliche Alphabete zum Verschlüsseln verwendet werden. Dies muss natürlich so geschehen, dass der Empfänger den Geheimtext leicht entschlüsseln kann.

Diese Idee wurde im 16. Jahrhundert von dem Franzosen Blaise de Vigenère (1523-1585) umgesetzt: Bei dem sogenannten Vigenère-Verfahren werden die einzelnen Klartextbuchstaben durch verschiedene Alphabete verschlüsselt. Man verwendet wechselnde Alphabete, wobei der Wechsel der Alphabete durch ein Schlüsselwort gesteuert wird.
Stellen wir uns vor, das Schlüsselwort heißt GYMBO. Dann wird der erste Buchstabe des Klartextes mit dem Caesar-Alphabet verschlüsselt, dass mit G beginnt, der zweite mit dem
Alphabet, das mit Y beginnt, der dritte mit dem Alphabet, das mit M beginnt, usw.
Das folgende Beispiel verdeutlicht das Verfahren. Zunächst werden alle 26 Caesar-Alphabete
untereinander aufgeschrieben. Dieses Schema heißt Vigenère-Quadrat (Seite 2).
Wir schreiben nun den Klartext auf und darüber so oft wie nötig das Schlüsselwort.

Schlüsselwort:	G	Y	M	B	O	G	Y	M	B	O	G	Y	M	B	O	G
Klartext:		D	E	R	T	E	X	T	I	S	T	S	I	C	H	E	R

Nun geht man wie folgt vor: Um den ersten Buchstaben zu verschlüsseln, muss man im Vigenère-Quadrat den Buchstaben in der Zeile G und der Spalte D suchen, das ist J. Um den zweiten Buchstaben zu verschlüsseln, bestimmt man in der Zeile Y den Buchstaben der Spalte E, das ist C. Für den dritten Geheimtextbuchstaben sucht man den Buchstaben in der Zeile M und der Spalte R und erhält das D. Insgesamt ergibt sich also folgender Geheimtext:

Schlüsselwort:	G	Y	M	B	O	G	Y	M	B	O	G	Y	M	B	O	G
Klartext:	D	E	R	T	E	X	T	I	S	T	S	I	C	H	E	R
Geheimtext:	J	C	D	U	S	D	R	U	T	H	Y	G	O	I	S	X

Nun erkennt man Folgendes: Gleiche Klartextbuchstaben werden in verschiedene Geheimtextbuchstaben übersetzt: Das T wird beispielsweise in die Buchstaben U, R und H übersetzt. Auf der anderen Seite stammen die gleichen Buchstaben aus dem Geheimtext von verschiedenen Klartextbuchstaben ab: Das D stammt einmal von einem R und einmal von einem X ab. Das Entschlüsseln verläuft entsprechend: Für unser Beispiel sucht man im Vigenère-Quadrat in der Zeile G (Schlüssel) die Stelle des Geheimtextbuchstaben J und erhält so in der ersten Zeile des Quadrats den Klartextbuchstaben D.

Das Vigenere Quadrat

Kler	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

In der ersten Zeile stehen die Klartextbuchstaben, in der ersten Spalte die Schlüsselbuchstaben. Man geht vom Klartextbuchstaben abwärts und vom Schlüsselbuchstaben nach rechts. Am Kreuzungspunkt dieser Linien steht der Geheimtextbuchstabe. Zum Entschlüsseln geht man erst in der Schlüsselspalte abwärts bis zum richtigen Schlüsselbuchstaben G und von da nach rechts bis zum Geheimtextbuchstaben J und findet von da aus aufwärts den Klartextbuchstaben D.

(aus Einheit_Krypto_Hertel.pdf)