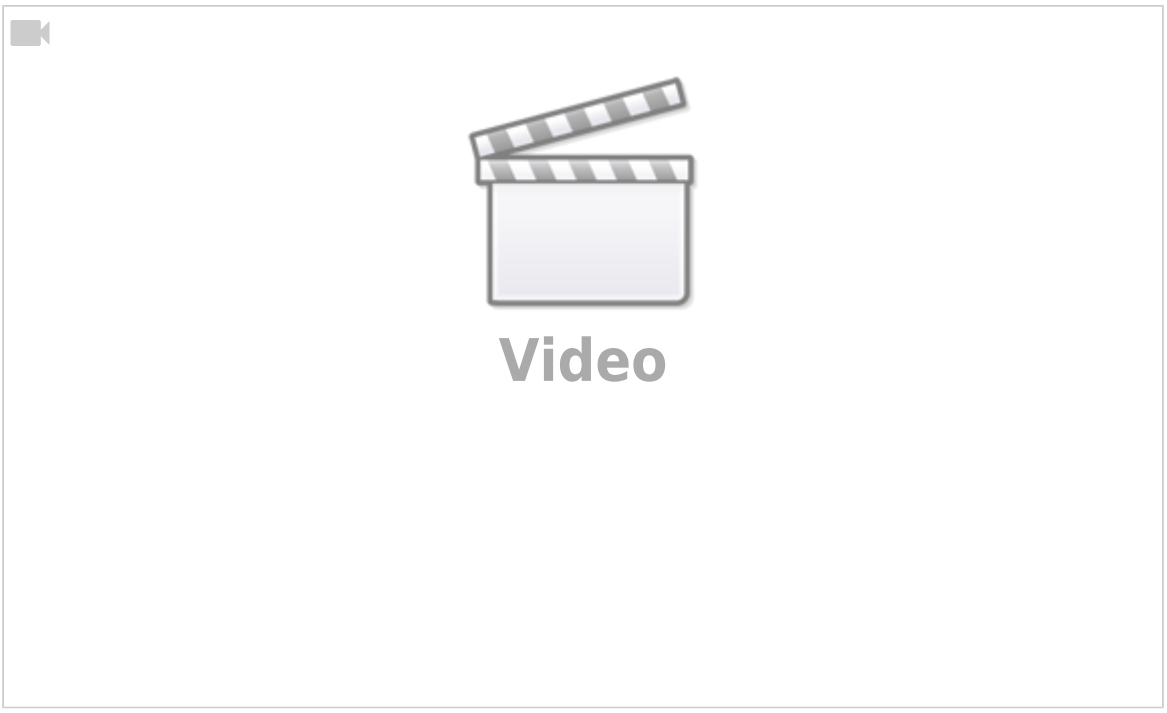
Weiterentwicklung des Substitutionsverfahrens: Vigenère-Chiffre

Durch Häufigkeitsanalysen sind monoalphabetische Substitutionsverfahren unsicher, selbst wenn das Geheimtextalphabet nicht nur verschoben, sondern "zerwürfelt" ist - wenn also die Buchstaben des Geheimtextalphabets in zufälliger Reihenfolge vorliegen. Angriffe auf monoalphabetische Substitutionsverfahren erfolgen immer nach der **Exhaustionsmethode**; sie werden auch als **Brute-Force-Attacken** bezeichnet.

Die Weiterentwicklung der Substitutionsverfahren, die Angriffe auf den Code durch Häufigkeitsanalysen unmöglich macht, ist die **polyalphabetische Substitution** wie wie die Vigenère-Chiffre, die 300 Jahre lang als unangreifbar galt. Hier verwendet man für aufeinanderfolgende Buchstaben jeweils verschiedene Alphabete, so dass sich die Häufigkeiten der Buchstaben im Geheimtext ausgleichen:



Arbeitshilfe: Vigenere-Quadrat

Verwende die

Arbeitshilfen zur Vigenère-Chiffre

und bearbeite folgende Aufgaben.

Schlüssel:

Schlüsselwort k festlegen, z.B. k=TOM

Verschlüsseln:

Klartext m	A	U	S	K	L	A	R	T	E	X	T	W	I	R	D	C	H	I	F	F	R	E	T	E	X	T
Schlüssel k	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O

Nun wird das erste A mit dem Schlüsselalphabet T verschlüsselt (also wie mit einem Caesar-Ring in der Stellung „T unter A“). Das U wird mit dem Alphabet O, das S mit T und das K wieder mit T verschlüsselt:

Geheimtext c	T	I	E	D	Z	M	K	H	Q	Q	H	I	B	F	P	V	V	U	Y	T	D	X	H	Q	Q	H

Entschlüsseln:

Man schreibt den Schlüssel unter den Geheimtext und verfolgt die Buchstaben zurück: Der Geheimtextbuchstabe findet sich im Inneren des Vigenere-Quadrats, der Schlüssel auf der einen und der Klartext auf der anderen Achse.

Geheimtext c	T	I	E	D	Z	M	K	H	Q	Q	H	I	B	F	P	V	V	U	Y	T	D	X	H	Q	Q	H
Schlüssel k	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O	M	T	O
Klartext m	A	U	S	K	L	A	R	T	E	X	T	W	I	R	D	C	H	I	F	F	R	E	T	E	X	T

Klartextbuchstaben in dieser Zeile suchen --->

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
		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
0	A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Schlüsselbuchstaben in dieser Spalte suchen --->

↑ Chiffretextbuchstaben im Inneren der Tabelle suchen ↑

(A1)

(A) Erkläre das Prinzip von Brute-Force-Attacken (Recherche!).

(B) Vereinbare mit deinem Nachbarn ein Schlüsselwort. Jeder chiffriert einen kurzen Text (wenige Wörter), ihr tauscht die Geheimtexte aus und jeder dechiffriert die Nachricht des anderen.

Angriffe auf die Vigenère-Chiffre

Der Kasiski-Test

Recherchiere Angriffsverfahren auf polyalphabetische Substitutionsverfahren. Stelle einen Angriff, der auf dem **Kasiski-Test** beruht, schematisch (Flussdiagramm) dar.

Autokorrelation

Die Vigenère-Chiffre ebnet zwar die Häufigkeitsunterschiede zwischen den Gruppen ein, aber innerhalb einer Gruppe sind immer die gleichen Buchstaben häufig (bzw. selten). Das nutzt man aus, indem man den Geheimtext buchstabenweise verschiebt und seine Übereinstimmungen mit sich selber zählt. Wenn nach der richtigen Verschiebung (nämlich um genau eine Schlüssellänge) alle Buchstaben wieder mit denen ihrer eigenen Gruppe zusammentreffen, fällt das bei der Zählung sofort auf:

(A2)

Gegeben ist das folgende Textfragment, welches mit der Vigenère Methode verschlüsselt ist. Es ist bekannt, dass die Schlüssellänge 3 ist. Versuche den Klartext zu ermitteln.

```
VRUJEGXEAVNGVBXEDXISILR
```

(A3)

```
RQICVCXVOLIIFCIIUMWKZQRWJZQROQOVMEMKUIRKRWVKNWHRNUYVNAXVYIREEMXQONYEFBMFIQII
```

ZV