LU05b - Die Symmetrische Verschlüsselung

Lernziele

- Den Begriff **Symmetrische Verschlüsselung** in eigenen Worten erklären können.
- Die **vier grundlegenden Varianten** von symmetrischen Verschlüsselungen nennen und mit konkreten Beispielen ergänzen können.
- Einfache Begriffe mit Hilfe der Vigenère Verschlüsselung ohne technische Hilfsmitteln ver- und und entschlüsseln können.
- Die Enigma-Verschlüsselung und deren Komponenten nennen und Gründe nennen können, warum dieses Verfahren erfolgreich war.
- Anzahl von Schlüsselpaaren zu einer gegebenen Anzahl von Usern berechnen können.

Einleitung: Die symmetrische Verschlüsselung

Symmetrische Verschlüsselungsverfahren zeichnen sich dadurch aus, dass zum Verschlüsseln und zum Entschlüsseln der gleiche Schlüssel verwendet wird.

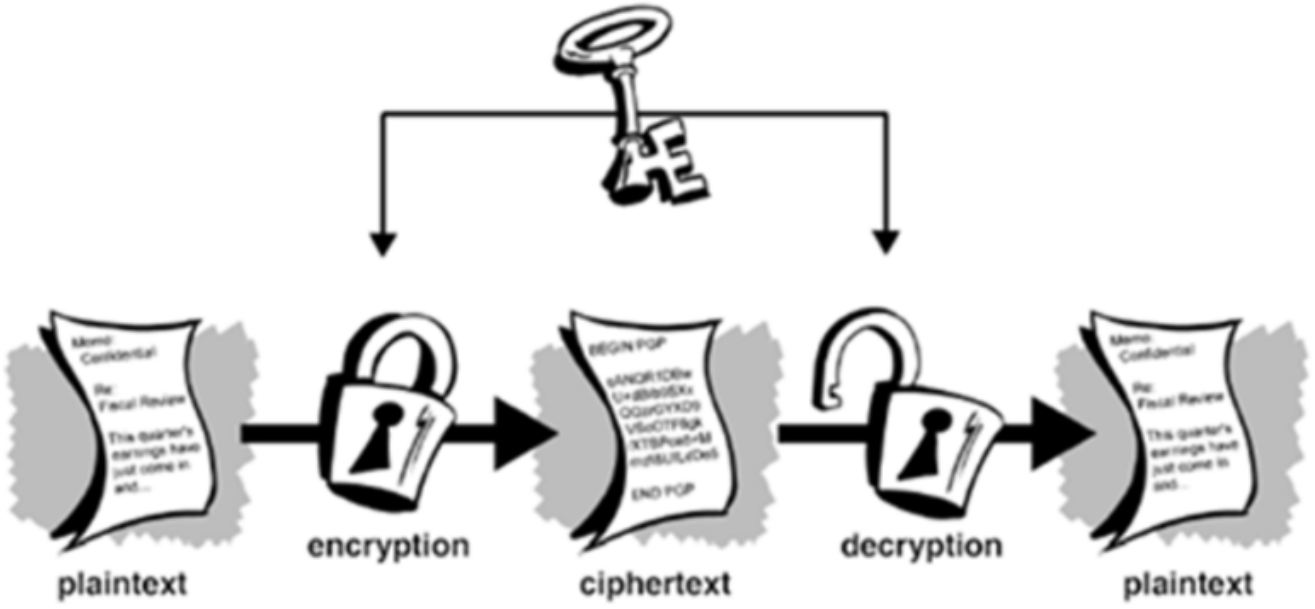
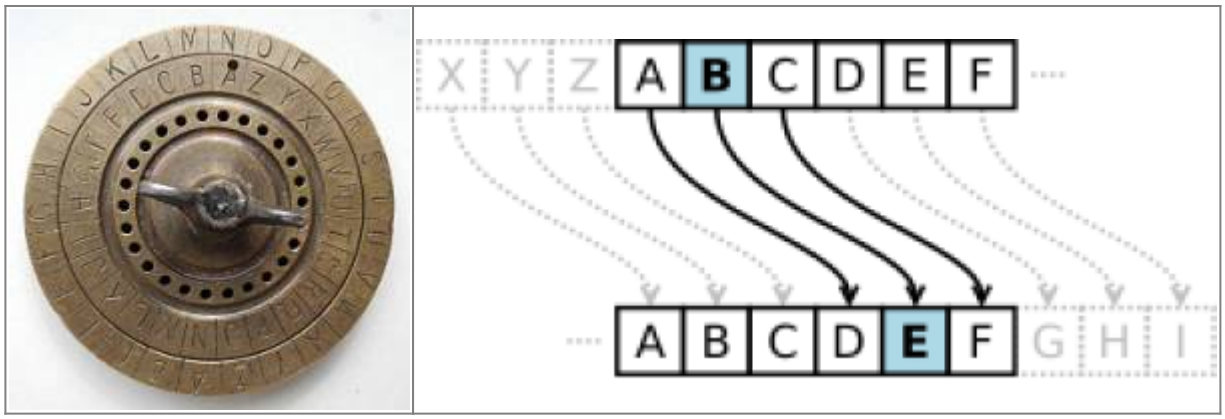


Abbildung 1: Der Ablauf einer symmetrischen Verschlüsselung

1 Monoalphabetische Verfahren

Monoalphabetische Verfahren gehören zu den ältesten bekannten Verschlüsselungen. Schon Cäsar setzte sie bei seinen Feldzügen ein.



Sie beruhen darauf, dass in einem Text jedem Buchstaben fix ein anderer Buchstabe zugeordnet ist. Die Definition dieser Zuordnung bildet den Schlüssel. Einfache monoalphabetische Verfahren addieren zu jedem Buchstaben einen fixen Betrag, wobei nach Z wieder A folgt.

Ein Spezialfall davon ist der rot13-Algorithums, welcher die Buchstaben jeweils um 13 Stellen verschiebt. Bei 26 Buchstaben im Alphabet bedeutet das, dass bei zweimaliger Anwendung wieder der ursprüngliche Text erscheint. Dieser Algorithmus ist unter anderem in Newsgroups verbreitet. Gute Newsreader enthalten dementsprechend auch die Funktion, diesen Algorithmus auf einer Meldung direkt anwenden zu können.

Ausprobieren:

- https://rot13.com/
- Es können verschiedene Offset gesetzt werden.

2 Polyalphabetische Verfahren

Polyalphabetische Verfahren definieren mehrere (mindestens 2) Verschlüsselungsalphabete. Diese sind Teil des Algorithmus. Der Schlüssel gibt an, in welcher Reihenfolge sie verwendet werden sollen. Eines der bekannteren polyalphabetischen Verfahren ist die **Vigenère Verschlüsselung**

	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Der Schlüssel kann hier ein eigentliches Passwort sein, welches angibt, welche der Zeilen der Reihe nach zum Verschlüsseln genommen werden soll.

2.1. Beispiel einer Verschlüsselung

Vigenère-Verschlüsselung von **HALLO** mit Schlüssel **KEY**

1. Vorbereitung

- Klartext: **HALLO**
- Schlüssel (wiederholt bis zur Länge des Klartextes): **KEYKE**

Buchstabe	**Zahl**	**Schlüssel-Buchstabe**	
H	7	K	10
A	0	E	4
L	11	Y	24
L	11	K	10
O	14	E	4

2. Verschlüsselung

```
Formel:  ( Klartext-Zahl + Schlüssel-Zahl ) mod 26
```

Klartext-Zahl	Schlüssel-Zahl	Summe	mod 26	
7	10	17	17	R
0	4	4	4	E
11	24	35	9	J
11	10	21	21	V
14	4	18	18	S

3. Ergebnis

- Klartext: **HALLO**
- Schlüssel: **KEYKE**
- **Chiffre: REJVS**

2.2 Beispiel einer Entschlüsselung

Wir wollen die Geheimnachricht **REJVS** wieder zu **HALLO** mit dem Schlüssel **KEY** entschlüsseln.

1. Vorbereitung # Vigenère-Entschlüsselung von **REJVS** mit Schlüssel **KEY**

- Chiffre: **REJVS**
- Schlüssel (wiederholt): **KEYKE**

Chiffre-Buchstabe	Zahl	Schlüssel-Buchstabe	Zahl
R	17	K	10
E	4	E	4
J	9	Y	24
V	21	K	10
S	18	E	4

2. Entschlüsseln

```
Formel: ( Chiffre-Zahl - Schlüssel-Zahl + 26 ) mod 26
```

Chiffre-Zahl	Schlüssel-Zahl	Differenz	mod 26	Klartext-Buchstabe
17	10	7	7	H
4	4	0	0	A
9	24	-15	11	L
21	10	11	11	L
18	4	14	14	O

3. Ergebnis

- Chiffre: **REJVS**
- Schlüssel: **KEYKE**
- **Klartext: HALLO**

—

Quellen

- https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsselung
- https://de.wikipedia.org/wiki/ROT13
- https://de.wikipedia.org/wiki/Vigen%C3%A8re-Chiffre
