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.

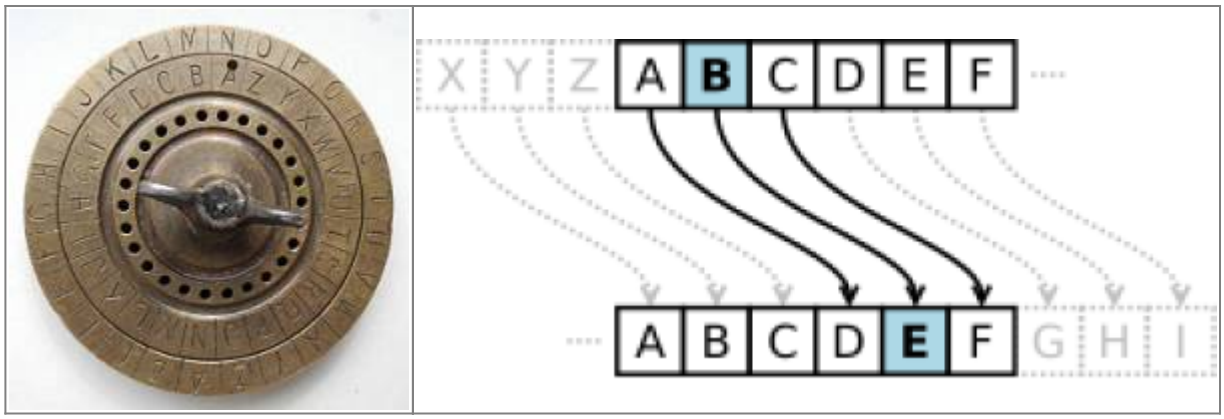
Einleitung: Die symmetrische Verschlüsselung

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.

Studyflix: Die Cäsar-Verschlüsselung

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: Vigenère Verschlüsselung

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.

Studyflix: Die Vigenère Verschlüsselung

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

Buchstabe	Zahl	Schlüssel-Buchstabe	
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
```

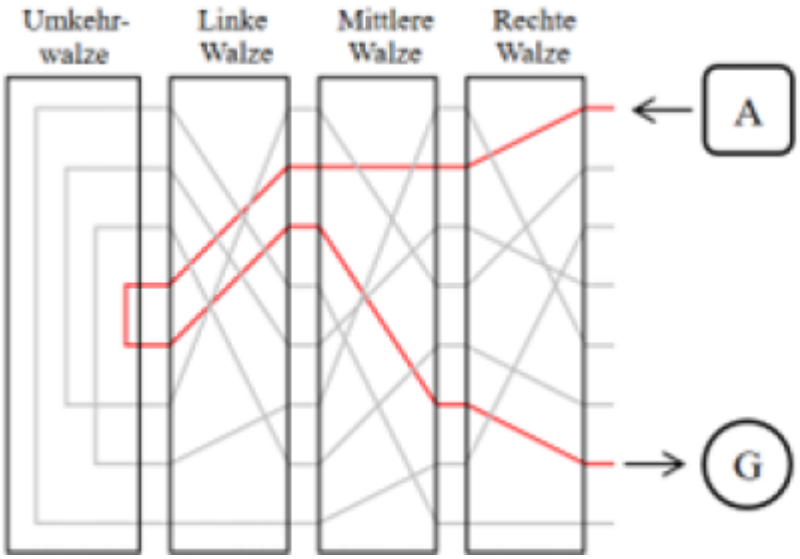
Chiffre-Zahl	Schlüssel-Zahl	Differenz	mod 26	Klartext-Buchstabe
17	10	7	7	H
4	4	0	0	A
9	24	-15	11	L
21	10	11	11	L
18	4	14	14	O

3. Ergebnis

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

3 Polyalphabetische Verfahren: Enigma-Verschlüsselung

Eine Erweiterung der polyalphabetischen Verfahren ist die **Enigma**, die von den Deutschen im 2. Weltkrieg eingesetzte Verschlüsselungsmaschine. Dass den Engländern eine solche Maschine in die Hände fiel und sie dadurch in der Lage waren, gewisse verschlüsselte Meldungen zu entschlüsseln, war mit kriegsentscheidend.



Allein durch die drei Walzen waren 26 * 26 * 26 = 17’576 Walzenstellungen möglich. Das entspricht einer 14Bit-Verschlüsselung. Hinzu kamen die variablen Steckverbindungen. Der gesamte Schlüsselraum ein Enigma mit drei aus einem Vorrat von fünf ausgewählten Walzen und einer Umkehrwalze sowie bei Verwendung von zehn Steckern lässt sich aus dem Produkt ermittelten 60 Walzenlagen, 676 Ringstellungen, 16’900 Walzenstellungen und 150'738'274'937’250 Stecker Möglichkeiten berechnen. Er beträgt:

```
60 * 676 * 16’900 * 150'738'274'937’250 = 103'325'660'891'587'134'000'000 =
10 exp(23) Möglichkeiten
```

Es gibt verschiedene Emulatoren, die die Funktionsweise der **Enigma** aufzeigen. Der nachfolgende Link zeigt einen solchen Enigma-Online-Emulator.

```
* https://www.101computing.net/enigma-machine-emulator/
```

4 Polyalphabetische Verfahren: Bit-Operations-Verfahren

In der Kryptographie digitaler Nachrichten kommen vor allem Bitoperationsverfahren zur Anwendung. Die bekanntesten davon sind

- DES (Schlüssellänge, 56 Bit)
- IDEA (Schlüssellänge, 128 Bit)

- RC4 (Schlüssellänge, variabel)

DES und IDEA sind sogenannte Blockverschlüsselungsverfahren. D.h. sie werden zum Verschlüsseln von als Ganzes vorhandenen Daten eingesetzt. RC4 ist ein Stromverschlüsselungsverfahren, welches zum Beispiel bei SSL zum Einsatz kommt.

Der DES-Schlüssel entspricht heutigen Sicherheitsbedürfnissen nicht mehr. Man nimmt an, dass die NAS (National Security Agency) einen DES-Schlüssel in wenigen Sekunden knacken kann. Amerikanische Regierungsstellen dürfen seit 1998 kein einfaches DES mehr verwenden.

Deshalb wurde das Triple-DES Verfahren eingeführt, welches ohne den Algorithmus zu ändern, die effektive Schlüssellänge verdreifacht, indem das Verfahren einfach dreimal angewendet wird. Man verschlüsselt die Information mit DES und dem Schlüssel 1, dann entschlüsselt man mit dem Schlüssel 2 und schließlich verschlüsselt man erneut mit Schlüssel 1. Die theoretische Schlüssellänge beträgt daher 3*56=168 Bit. Ausserdem ist das System voll kompatibel zu DES, wenn Schlüssel 1 und 2 gleich sind.

5 Schlüsselmanagement

Bei symmetrischen Verfahren ist es nötig, dass jeweils beide Kommunikationspartner Kenntnis vom Schlüssel haben. Der Schlüssel muss auf einem separaten, sicheren Weg ausgetauscht werden. Ausserdem müssen unter Umständen sehr viele Schlüssel verwaltet werden. In einem Netzwerk von Kommunikationspartnern, die alle miteinander Meldungen austauschen wollen, sind dies:

- 2 Partner: 1 Schlüssel
- 3 Partner: 3 Schlüssel
- 5 Partner: 10 Schlüssel
- 10 Partner: 45 Schlüssel
- 20 Partner: 190 Schlüssel
- **Allgemein: n * (n-1) / 2**

Wir sehen, dass die Verwaltung der Schlüssel nahezu quadratisch wächst, und damit die Verwaltung der Keys sehr aufwendig und fehleranfällig ist.

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
