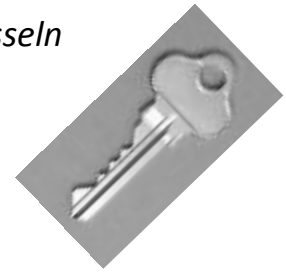
Lehreinheit E-V2 – *Verschlüsselung mit symmetrischen Schlüsseln*



Zeitrahmen
70 Minuten

Zielgruppe
- Sekundarstufe I
- Sekundarstufe II

Inhaltliche Voraussetzung
- V1 Caesar-Chiffre
- Für Punkt 2: Addieren/Subtrahieren mit Binärzahlen

Lehrziel
Verstehen des Prinzips der symmetrischen Verschlüsselung.
Symmetrische Verschlüsselungsverfahren kennen lernen und die Schlüsselqualität abwiegen sowie Schwächen der symmetrischen Verschlüsselung erkennen.

Motivation
Geheime Nachrichten wecken die Neugierde. Kryptografie ist ein zentrales Thema der Mathematik und Informatik. Sie war, historisch gesehen, schon früh von Bedeutung und wird in der heutigen virtuellen Kommunikation auch immer wichtiger. Nach einfach durchschaubaren Verschlüsselungs-Verfahren wie der Caesar-Chiffre im Modul V1 sollen nun auch komplexere und sicherere Verfahren kennen gelernt werden.

Requisiten
- Kärtchen mit dem Alphabet (2fache Ausführung)
- Plakat mit Vigenère-Quadrat
- Arbeitsblatt V_AB 2.1 und V_AB 2.2

Partizipanden
gesamte Klasse

Unterlagen
V-AB1, V-AB2

Vorgehensweise

1. Vorstellung der **Vigenère-Chiffre**:

   Wir haben gesehen, dass die Caesar-Chiffre relativ leicht zu brechen ist. Sehen wir uns also eine Verbesserung davon an. Bei der Vigenère-Chiffre hat man ein sogenanntes Vigenère-Quadrat, das sechsundzwanzigmal die Buchstabenfolge des Alphabets enthält, jeweils mit einem anderen Anfangsbuchstaben.

   Den TN wird ein Plakat eines Vignère-Quadrats (siehe Abb. 1) gezeigt, um die weiteren Erklärungen zu vereinfachen.
   Zur Ver- und Entschlüsselung wird ein Schlüsselwort benötigt. Dieses Schlüsselwort gibt an, welche Zeile des Vigenère-Quadrats für welchen Buchstaben verwendet wird.

Klar	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

Abbildung 1: Vigenère-Quadrat (Singh, Simon: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. München: dtv 2004.)

Gemeinsam wird ein Beispiel am Flipchart/an der Tafel durchgeführt, wobei ein TN an der Tafel schreibt. Die anderen geben Anweisungen:

Schlüsselwort: *SCHULE*

G	E	H	E	I	M	E	N	A	C	H	R	I	C	H	T	Klartext
S	C	H	U	L	E	S	C	H	U	L	E	S	C	H	U	Schlüssel
Y	G	O	Y	T	Q	W	P	H	W	S	V	A	E	O	N	Verschlüsselt

Das Schlüsselwort wird wiederholt unter die geheime Nachricht geschrieben. Der Buchstabe des Schlüssels gibt für den jeweiligen zu verschlüsselnden Buchstaben an, mit welcher Zeile der darüber stehende Buchstabe des Klartextes verschlüsselt werden muss. Will man also den ersten Buchstaben, G, verschlüsseln, so geht man aufgrund des darunter liegenden S (aus der Schlüsselzeile) in die mit S beginnende Zeile 18 des Vigenère-Quadrats und sucht den Buchstaben der in der Spalte für G steht. In diesem Fall ist dies Y.

Es werden mit den TN gemeinsam zumindest einige Buchstaben verschlüsselt. Um Verständnis zu erzielen, muss nicht der ganze Klartext verschlüsselt werden. Wichtig wäre allerdings, den Anfang dieses Wortes auch noch mit einem anderen Schlüssel zu verschlüsseln. (z.B. mit einem kurzen Wort wie GUT oder ART, um den Effekt der Wortlänge zu erkennen.

Anregende Fragen:

- Welche Informationen braucht man um den Text wieder zu entschlüsseln? Reicht das Vigenère-Quadrat dafür?
  Nein, das Vigenère-Quadrat reicht nicht, man muss auch das Schlüsselwort wissen.
- Könnte man auch hier durch reines Probieren auf den Klartext bzw. das Schlüsselwort kommen, oder ist diese Verschlüsselung sicher?
  Die Entschlüsselung ist schwieriger, kennt man jedoch die Länge des Schlüsselwortes, das sich ja immer wieder wiederholt, wird ähnlich entschlüsselt wie bei der Caesar-Chiffre (durch Häufigkeitsanalyse).
- Wie sollte eine gutes Schlüsselwort aussehen?
  Je länger das Schlüsselwort ist, umso schwieriger ist die Kryptoanalyse. Ideal sind daher lange Worte oder aufgrund der Länge komplette Schlüsselsätze.

2. Verschlüsselung **binär codierter Texte**

Ergänzung (Voraussetzung Binärzahlen C4): Da im Computer sowohl Zahlen als auch Text durch Binärzahlen dargestellt werden, sollte hier auch veranschaulicht werden, wie nun mit Binärzahlen verschlüsselt werden kann.

Wie werden Buchstaben am Computer dargestellt/codiert?

Es gibt verschiedene Möglichkeiten die Buchstaben unseres Alphabets zu codieren. Eine davon ist der ASCII-Code (American Standard Code for Information Interchange), eine einfache Zuordnung im ASCII-Code mit den 26 Buchstaben unseres Alphabets zeigt die Tabelle.

ASCII-Tabelle f. Großbuchstaben:

	Binär	Dezimal		Binär	Dezimal
A	1000001	65	N	1001110	78
B	1000010	66	O	1001111	79
C	1000011	67	P	1010000	80
D	1000100	68	Q	1010001	81
E	1000101	69	R	1010010	82
F	1000110	70	S	1010011	83
G	1000111	71	T	1010100	84
H	1001000	72	U	1010101	85
I	1001001	73	V	1010110	86
J	1001010	74	W	1010111	87
K	1001011	75	X	1011000	88
L	1001100	76	Y	1011001	89
M	1001101	77	Z	1011010	90

Nimmt man als zu verschlüsselnde Botschaft das Wort HALLO so ergibt dieses in einer auf die beiden Zeichen „0“ und „1“ beschränkten Darstellungsform in ASCII-Code den Klartext:

HALLO = 1001000 1000001 1001100 1001100 1001111

Verschlüsselt wird dieser „Text“, indem zu dieser Zahlenfolge jene eines Schlüsselwortes addiert wird. Wir wollen dafür in Analogie zur unter 1.) durchgeführten Verschlüsselung das Schlüsselwort DAVID wählen.

Hier werden die TN nun selbst wieder aktiv. Sie sollen zum Schlüsselwort DAVID die binäre Folge in der vereinfachten ASCII-Tabelle finden.

DAVID = 1000100 1000001 1010110 1001001 1000100

Nun kann man sowohl das binär dargestellte Schlüsselwort als auch den Klartext nicht als Text sondern als Ziffernfolge von Binärziffern auffassen. Somit kann man das binäre Schlüsselwort (allenfalls entsprechend oft wiederholt) zum binären Klartext addieren.

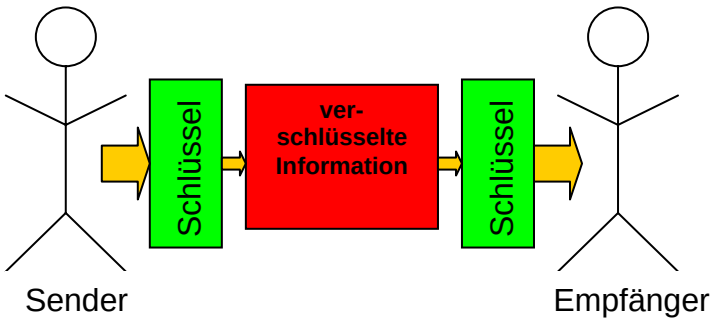
Lösung:

Klartext:	HALLO
Klartext in ASCII:	1001000 1000001 1001100 1001100 1001111
Schlüssel DAVID: +	1000100 1000001 1010110 1001001 1000100
Verschlüsselt:	10001101 0000011 0100011 0010110 0010011
+ Übertrag	1
Gesendete Nachricht	0001101 0000011 0100011 0010110 0010100

- Ist die Leistungsfähigkeit dieses Verfahrens gleich oder anders als bei der Vigenère-Verschlüsslung?
- Warum brauchen wir hier keine Tabelle? Wodurch wird die Tabelle im hier vorgestelltn Verfahren simuliert?

3. Am Arbeitsblatt V-AB1 sind noch einige zusammenfassende **Begriffe** erklärt.
Man kann zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren unterscheiden. In dieser Einheit haben wir einige symmetrische Verfahren kennen gelernt.
Zuerst betrachten wir aber generell, wie eine Ver- und Entschlüsselung funktioniert. Zur Verschlüsselung benötigt man einen so genannten Schlüssel. Dieser verändert die zu verschlüsselnde Information. Bei der Entschlüsselung muss dieser Schlüssel der Person, die die Nachricht entschlüsselt, bekannt sein. Bei der symmetrischen Verschlüsselung ist der Schlüssel für die Ent- und Verschlüsselung gleich. Beiden Personen muss der Schlüssel bekannt sein (siehe Grafik):

Bild für die Tafel:



4. **Entschlüsselung**
Wie funktioniert die Entschlüsslung bei der Vigenère-Chiffre?
- mit der Tabelle?
  Nachricht: DLDAEGSKXS,
  Schlüssel: ART
- über das Binärsystem?
  Nachricht: 0011001 0010111 0011000 0000011 0011110,
  Schlüssel: 1000001 1010010 1010100

Die Entschlüsslung mit der Tabelle sollte aufgrund der Verschlüsslung selbst entdeckt werden und daher zuerst geübt werden. (Man geht eben in umgekehrter Richtung durch die Tabelle.)
Haben die SchülerInnen dieses Prinzip erkannt, sollte auch die Entschlüsselung im Binärcode selbst entdeckbar sein. Für SchülerInnen die die Entschlüsslung nicht selbst entdecken, sollte auf jeden Fall an der Tafel (möglicherweise durch andere SchülerInnen) die Entschlüsslung dargestellt werden.

Entschlüsselung:	
Empfangene Nachricht	0001101 0000011 0100011 0010110 0010100
Schlüssel DAVID: -	1000100 1000001 1010110 1001001 1000100
	11001000 1000001 1001100 1001100 1010000
- Übertrag	1
Klartext	1001000 1000001 1001100 1001100 1001111

Damit das verschlüsselte Wort die gleiche Länge hat, wird der Übertrag bei der Verschlüsselung addiert und bei der Entschlüsselung wieder subtrahiert.

Zum Abschluss erklären wir noch einige Fachbegriffe:

- *Kryptografie* beschäftigt sich mit der Verschlüsselung bzw. mit dem Finden von neuen Verschlüsselungsverfahren.
- *Kryptoanalytiker* versuchen Verschlüsselungen zu brechen.
- *Kryptologie* (kryptós, „verborgen“, und logos = Lehre) umfasst Kryptoanalyse und Kryptografie(kryptós, „verborgen“, und gráphein, „schreiben“).

Die TN sollten sich Erklärungen zu diesen Begriffen am Handout notieren.

5. Wir haben gesehen, dass zur Entschlüsselung dem Empfänger der Schlüssel immer bekannt sein muss. Das heißt, der Sender muss dem Empfänger den Schlüssel irgendwie mitteilen.
   Wie kann aber der Schlüssel selbst sicher übertragen werden?
   Mögliche Schülerantworten:
   i. persönlich den Schlüssel übergeben
   ii. durch zuverlässigen „Boten“ überbringen lassen
   iii. mit einem anderen Schlüssel verschlüsselt überbringen (aber wie übergeben wir dann diesen Schlüssel?)

Die Schlüsselverteilung ist also sehr aufwändig und stellte schon immer ein Problem und vor allem einen Schwachpunkt in der Verschlüsselung dar. Diese Sicherheitslücke wurde durch neue Verfahren der Verschlüsselung, der sogenannten asymmetrischen Verschlüsselung gelöst. Hier haben Sender und Empfänger jeweils unterschiedliche Schlüssel zur Ver- bzw. Entschlüsselung. Man kann sich das so vorstellen, dass der Sender die Nachricht in einen Koffer mit einem Vorhängeschloss, das im vorher vom künftigen Empfänger zugesandt wurde, packt (den Koffer kann also jeder befüllen), das Schloss verschließt und den Koffer abschickt. Für das Vorhängeschloss hat aber nur der Empfänger den Schlüssel. Man nennt dieses Verfahren auch Public-Key-System.

Quellen:

http://www.netplanet.org/kryptografie/verfahren.shtml (14. 1. 2009)

Hier können Sie eigene Texte mit der Caesar-Chiffre verschlüsseln lassen:

http://willy.chemie.uni-konstanz.de/fotos/caesar.htm (14. 1. 2009)

Hromkovič, Juraj: Sieben Wunder der Informatik. Eine Reise an die Grenze des Machbaren mit Aufgaben und Lösungen. Wiesbaden: Teubner 2006.

Singh, Simon: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. München: dtv 2004.

Schulz, Ralph-Hardo: Codierungstheorie. Eine Einführung. Wiesbaden: Vieweg Verlag 2003.