Modul V1 Verschlüsselung mit der Cäsar-Chiffre

Zeitrahmen
30 Minuten

Zielgruppe
- Volksschule
- Sekundarstufe I

Requisiten
Kärtchen mit dem Alphabet in zweifacher Ausführung auf jeweils unterschiedlicher Grundfarbe.

Lehrziel
- Verstehen des Prinzips der symmetrischen Verschlüsselung
- Symmetrische Verschlüsselungsverfahren kennen lernen

Motivation
Geheime Nachrichten wecken die Neugierde. Die Kryptografie ist ein zentrales Thema der Mathematik/Informatik, war historisch gesehen schon früh von Bedeutung und wird in der heutigen virtuellen Kommunikation auch immer wichtiger.

Mit diesem Verfahren wurden lateinische Nachrichten im römischen Reich verschlüsselt.

Vorgehensweise
1. Als Einstieg wird den TN ein verschlüsselter Text gezeigt, und gefragt, was dieser bedeuten könnte.
   Beispieltext: **Tfgvm Nlitvm Prmwvi!** *(Guten Morgen Kinder!)*
   Die TN werden darüber informiert, dass es sich um einen Geheimtext handelt, so wie etwa bei der Spiegelschrift. Es wurden nach gewissen Regeln Buchstaben vertauscht.
2. Nun werden Verschlüsselungsverfahren betrachtet, die symmetrische Schlüssel verwenden und der obige Text wird aufgelöst.

   Einfache Verschlüsselung: Die Buchstaben des Alphabets werden verschlüsselt, indem sie von hinten beginnend aufgeschrieben werden. Wir verwenden dazu Kärtchen, grüne für den Klartext, rote für den verschlüsselten Text, das Chiffrat.

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	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

Ausgangssituation

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
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Gespiegeltes Alphabet

Die TN erhalten die Aufgabe, die grünen Kärtchen in der richtigen Reihenfolge aufzulegen und darunter dann die roten Kärtchen von hinten beginnend. Somit erhält man jeweils die Zuord-

nungspaare der Buchstaben. A würde also durch das Chiffre Z ersetzt werden, B durch Y usw.

Bei Entschlüsseln des Textes auf der Tafel suchen wir das zur jeweiligen Chiffre (rot) passende Klartextzeichen (grün). Wir finden etwa zum roten *T* das darüber stehende grüne *G*. Nach Entschlüsselung der Worte an der Tafel wird ein Beispielswort gemeinsam verschlüsselt indem wir zu den Klartextbuchstaben (grün) die passende Chiffre (rot) suchen und anschreiben.

Ihr habt einen verschlüsselten Text vor euch liegen, welche Informationen würdet ihr benötigen, um ihn zu entschlüsseln?

Wenn man weiß, dass auf diese Art verschlüsselt wurde, kann man sich die Entschlüsselungsbuchstaben selbst zuordnen.

Diese Art der Verschlüsselung ist also nicht sehr sicher und leicht zu brechen, daher sehen wir uns dann eine etwas komplexere Art der Verschlüsselung an.

3. Wozu wird überhaupt verschlüsselt?

Was würdet ihr sagen, wenn eure SMS, die ihr an Freunde schickt, von den Eltern oder anderen Personen mitgelesen oder sogar verändert werden könnten? Wo könnte eine Verschlüsselung von Nachrichten wichtig sein, wo war sie früher wichtig, sucht konkrete Beispiele?

- Unbefugte dürfen Nachrichten/Daten nicht lesen, z.B. electronic banking, Industriespionage, Kriegsführung, Geheimdienste
  - o Beispielsweise dürfen Informationen über ein neues Produkt einer Firma nicht an die Konkurrenzfirma gelangen.
  - o Nachrichten über geplante Angriffe oder Angriffstaktiken dürfen nicht dem Gegner in die Hände fallen.
  - o Und natürlich würde man sich auch beim privaten E-Mail-Verkehr wünschen, dass der Text nicht für alle mitlesbar ist.

  Entspricht ein E-Mail eher einer Postkarte oder einem Brief?

  Eine Postkarte kann der Briefträger leicht lesen… Aber auch Briefe können unerlaubt geöffnet und wieder verschlossen werden, allerdings ist der Zugriff zumindest erschwert.
- Unbefugte dürfen Daten nicht ändern können (Integrität)
- Damit im Zusammenhang auch der Nachweis der Urheberschaft (Authentifikation)

Verschlüsselung steht somit auch in einem engen Zusammenhang mit dem Themenbereich Sicherheit.

4. **Cäsar-Chiffre**

Den TN wird nun ein Beispieltext gezeigt. Sie werden gefragt, ob dieser mit der oben genannten Methode entschlüsselt werden kann. Bevor das Grundprinzip anhand von Kärtchen erläutert wird, werden die TN gefragt, ob sie bereits von der Cäsar-Verschlüsselung gehört haben, wenn ja sollen diese TN bereits eine Erklärung dazu abgeben, was sie darunter verstehen (eventuelle Richtigstellung durch ÜL). Für die weitere Veranschaulichung werden jeweils zwei Kärtchenreihen mit dem Alphabet durch 2 TN aufgelegt. Die zweite Reihe wird von den TN um 2 Stellen verschoben, wobei die letzten Kärtchen jeweils wieder am Anfang eingefügt werden. Sind genug TN vorhanden, also mindestens 26 so kann jedes Kind zwei Karten halten und die Karten werden an den übernächsten Nachbarn weitergegeben. Der Schlüssel ist also in diesem Fall 2.

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	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

Ausgangssituation

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
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

Verschobene Kärtchen

Somit erhält man nun die Zuordnung für die Ver- und Entschlüsselung. Wieder wird damit ein kurzes Beispielswort ver-/entschlüsselt (an der Tafel).

Cäsar-Chiffre (Schlüssel 2)

guten tag ▶ iwvgp vci
hallo kinder ▶ jcnnq mkpfgt
guten morgen kinder ▶ iwvgp optigp mkpfgt
Wir sind eine brave klasse ▶ Ykt ukpf gkpg dtcxg mncuug
das ist eine geheime nachricht ▶ Fcu kuv gkpg igjgkog pcejtkejv

Was muss man wissen, um einen Text, der auf diese Art und Weise verschlüsselt wurde, wieder zu entschlüsseln?

Die Zahl, um wie viel Positionen verschoben wurde, also den Schlüssel.

Wie könnte man die Verschlüsselung auch ohne den Schlüssel zu wissen, brechen (wenn Zeit keine Rolle spielt)?

a) Durch Ausprobieren, um wie viel Stellen verschoben wurde. Das ist in endlicher Zeit machbar
b) Kryptoanalytiker gehen von der Häufigkeit der Buchstaben aus und schließen daraus auf die Verschlüsselung. Man sucht hierbei aus dem verschlüsselten Text den häufigsten Buchstaben heraus und nimmt an, dass dieser dem häufigsten Buchstaben im Alphabet entspricht, dann sucht man den zweithäufigsten usw. Die drei häufigsten Buchstaben im deutschen Alphabet sind E (17,4%), N (9,78%) und I (7,55%).
Auch anhand von Wortanfängen bzw. Wortlängen kann man versuchen Wörter zu entschlüsseln. Beispielsweise kann man die 3 Artikel *der*, *die*, *das* sehr leicht aufgrund der Wortlänge und der gleichen Anfangsbuchstaben erkennen. Aus den Wortanfängen kann man dann darauf schließen, welcher Buchstabe es sein könnte: der-die-das ergäbe FGT-FKG-FCU, lässt man die Leerzeichen weg, kann man die Wörter auf diese Art und Weise nicht mehr so leicht analysieren.

Ohne Einhalten gemeinsamer Konventionen kann keine Kommunikation entstehen!

Quellen/Weiterführende Literatur

Hier können Sie eigene Texte mit der Cäsar-Chiffre verschlüsseln lassen:
http://willy.chemie.uni-konstanz.de/fotos/caesar.htm

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.