Arbeitsblatt – Netzwerke

Name:	Vorname	Klasse:	Datum:
BE:	Punkte:	Zensur:	

Beim heutigen Datenverkehr in Netzwerken und der Anzahl an Spionagetools, ist es unerlässlich geworden, Verschlüsselungsverfahren einzusetzen. Die Kryptologie bildet den Bereich der Informatik, der sich mit der Verschlüsselung (Kryptographie) und der Entschlüsselung verschlüsselter Daten (Kryptoanalyse) beschäftigt. Für unsere Zwecke reichen uns die sog. *symmetrischen Verschlüsselungsverfahren*. Am Ende der Station muss jeder Schüler mindestens ein symmetrisches Verschlüsselungsverfahren beherrschen (erklären und anwenden) können. Vorab müssen jedoch einige Begriffe geklärt werden.

Klartext	der zu verschlüsselnde Text
Geheimtext	der verschlüsselte Text
Schlüssel	wandelt den Klartext in den Geheimtext um
Verschlüsselung	der Klartext wird mittels eines Schlüssels zum Geheimtext
Entschlüsselung	der Geheimtext wird mittels eines Schlüssels zum Klartext
symmetrische Verschlüsselung	der gleiche Schlüssel, der den Klartext verschlüsselt, entschlüsselt den Geheimtext
asymmetrische Verschlüsselung	der Schlüssel, der den Klartext verschlüsselt, unterscheidet sich von dem Schlüssel, der den Geheimtext entschlüsselt

Symmetrische Verschlüsselungsverfahren

Der Caesar-Code

Diese Verschlüsselungsverfahren waren bereits in der Antike bekannt. In seiner Schrift *Commentarii de Bello Gallico* schreibt Caesar über einen Militärcode,

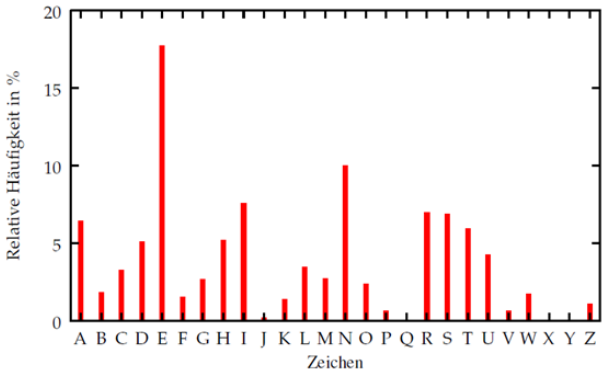
den er verwendete, um Nachrichten zu verschlüsseln. Dazu verschiebt er einfach jeden Buchstaben im Alphabet um zwei Positionen nach „vorn“, d.h. A→C, B→D, C→E usw. Man sagt, der Text wurde mit dem Caesar-Verfahren und dem Schlüssel *C* verschlüsselt. Der Schlüssel ist immer der Buchstabe, der dem *A* zugeordnet wird. Da jedem Buchstaben des Alphabets ein anderer desselben Alphabets zugeordnet wird, spricht man von einem Transpositionsverfahren. Würde man den einzelnen Buchstaben Geheimtextzeichen zuordnen (Vgl. Freimaurer-Code), spricht man von einem Substitutionsverfahren.

1. Verschlüssele die Nachricht *INFORMATIK MACHT SPASS* mit Hilfe des Caesar-Codes.

Selbstverständlich kann jede beliebige Verschiebung benutzt werden.

2. Verschlüsselt eine kurze selbstgewählte Nachricht mit einer selbstgewählten Verschiebung und reicht sie eurem Banknachbarn. Dieser soll nun Hacker spielen und versuchen, die Nachricht zu entschlüsseln.

Wie man schnell merkt, ist diese Art der Verschlüsselung nicht sonderlich schwer. Auf der einen Seite benötigt man höchstens 25 Versuche, bis man den Schlüssel gefunden hat. Das systematische Durchprobieren aller möglichen Schlüssel wird als *Brute-Force-Angriff* bezeichnet. Es gibt jedoch einen, aus kryptoanalytischer Sicht interessanteren Ansatz. Sollte der Angreifer wissen, in welcher Sprache der Text geschrieben ist, so kann er die Häufigkeitsverteilung der Buchstaben ausnutzen. Je länger der Text ist, umso sicherer ist diese Methode.



3. Beschreibe, wie man mit der Häufigkeitsanalyse einen Text mit Caesar-Verschlüsselung wieder dekodieren kann.

4. Nutze dein Wissen aus, um folgenden Text zu entschlüsseln. Er ist in deutscher Sprache geschrieben und mittels Verschiebung verschlüsselt. Gib auch den verwendeten Schlüssel an:
KPLZLY ALEA ZVSS HSZ LPUMHJOLZ ILPZWPLS KPLULU
QLKLY ZVSSAL LPULU ZHAG LUAZJOSBLZZLSU RVLUULU
KHUU OHA THU KHZ ZFZALT CLYZAHUKLU

Die Vigenere-Verschlüsselung

Die Häufigkeitsanalyse ist eines der bekanntesten Verfahren innerhalb der Kryptologie. Es kann auch zum Entschlüsseln des Vigenere-Verfahrens eingesetzt werden. Blaise de Vigenere (1523 - 1596) erweiterte die Transpositionsverschlüsselung dahingehend, dass er den Text statt mit einem Buchstaben mit einem Wort verschlüsselt. Dafür schreibt er den Schlüssel immer wieder unter den Klartext und verschlüsselt jeden Buchstaben einzeln mit dem Caesar-Code. Diesen Vorgang kann man im Kopf durchführen (sehr aufwändig), per

D	A	S	I	S	T	D	E	R	K	L	A	R	T	E	X	T
I	N	F	O	I	N	F	O	I	N	F	O	I	N	F	O	I
L	N	X	W	A	G	I	S	Z	X	Q	O	Z	G	J	L	B

Hand (ebenso aufwändig), mit der Caesar-Scheibe (schon besser) oder mit dem Vigenere-Quadrat(siehe nächste Seite).

5. Versuche selbstständig herauszufinden, wie man mit Hilfe des Vigenere-Quadrats einen Text verschlüsseln kann.

6. Erklärt, wie man einen Text mit dem Schlüssel wieder entschlüsseln kann.

7. Schreibt gegenseitig Nachrichten mit Hilfe des Vigenere-Codes und einem selbstgewählten Schlüssel.

8. Entschlüsselt folgende Nachricht, die mit dem Vigenere-Verfahren und dem Schlüssel *RSA* verschlüsselt wurde.
NWR UAEJWN KWXK WNKKCYDUVKSVDN
BSNE VEI ZAK VAJ NIXWNVJEMWRWSHIWN
XSNQ YUK NEIKTRFDVF

	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

Abbildung 1: Das Vigenere-Quadrat

Die Playfair-Verschlüsselung

Bis in den ersten Weltkrieg hinein wurde diese Verschlüsselung verwendet. Auch hierbei handelt es sich um ein symmetrisches Verschlüsselungsverfahren. Dem Großteil regelmäßiger Kinogänger wurde es bekannt, durch den Disney-Film „Das Vermächtnis des geheimen Buches“. Um mit der Verschlüsselung zu beginnen, muss der Klartext entsprechend vorbereitet werden. Als Beispiel soll der Satz aus dem Film dienen:

> Laboulaye lady will lead to Cibola temples of gold

Zuerst wird der Text in Bigramme (Buchstabenpaare) aufgeteilt.

> LA BO UL AY EL AD YW IL LL EA DT IC IB OL AT EM PL
> ES OF GO LD

Für die deutsche Sprache gelte weiterhin, dass Umlaute aufgelöst werden, J zu I sowie ß zu SS umgewandelt wird. Außerdem sind Bigramme aus Doppelbuch-

staben verboten. Es muss ersatzweise ein X eingefügt werden. Sollte am Ende ein einzelner Buchstabe übrig bleiben, wird ebenfalls ein X eingefügt.

> LA BO UL AY EL AD YW IL LX LE AD TI CI BO LA TE MP
> LE SO FG OL DX

Im nächsten Schritt muss ein Playfair-Quadrat erstellt werden, welches zur Umwandlung der Bigramme genutzt wird. Dazu wird ein Schlüsselwort in eine 5×5-Matrix eingetragen und der Rest des Alphabets eingetragen (Erinnerung: J=I). Im Film handelte es sich um das Schlüsselwort *DEATH*. Die Matrix hat also folgende Form

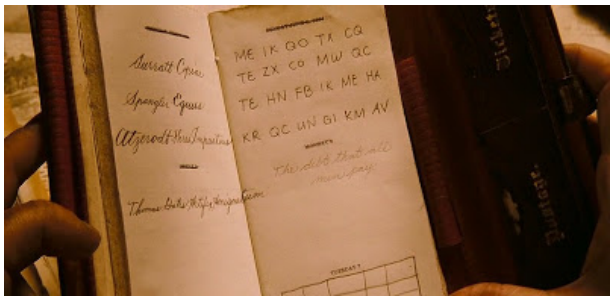
D	E	A	T	H
B	C	F	G	I
K	L	M	N	O
P	Q	R	S	U
V	W	X	Y	Z

Jetzt werden die Klarbigramme mittels der Matrix durch Geheimbigramme ersetzt. DIe Verschlüsselung funktioniert nach folgenden Regeln:

1. Stehen die Buchstaben in derselben Zeile, so werden die rechten Nachbarbuchstaben verwendet: AD→TE. Befindet man sich am rechten Ende, fängt man wieder vorn links an.
2. Stehen die Buchstaben in derselben Spalte, so werden die unteren Nachbarbuchstaben verwendet: EL→CQ. Befindet man sich am unteren Ende, fängt man oben wieder an.
3. Stehen beide Buchstaben in unterschiedlichen Zeilen und Spalten, so bilden sie die Eckpunkte eines Rechtecks. Der erste Buchstabe wird durch den Buchstaben ersetzt, der sich in derselben Zeile befindet, jedoch in der Spalte des zweiten Buchstaben. Ebenso verfährt man mit dem zweiten Buchstaben: LA→ME

Es ergibt sich folgende Verschlüsselung:

> LA BO UL AY EL AD YW IL LX LE AD TO CI BO LA TE MP
> LE SO FG OL DX
> ME IK QO TX CQ TE ZX CO MW QC TE HN FB IK ME HA
> KR QC UN GI KM AV
> bzw.
> MEIKQOTXCQTEZXCOMWQCTEHNFBIKMEHAKRQCUNGIKMAV



9. Verschlüssele die Nachricht: „Eine Klee fressende Kuh aus Jena“ mit dem Schlüssel GERA.
10. Wählt gemeinsam eine Nachricht. Jeder verschlüsselt selbstständig, indem er seinen Namen als Schlüsselwort benutzt.
11. Erkläre, wie die Entschlüsselung bei bekanntem Schlüssel funktioniert.
12. Folgende Nachricht wurde mit PlayFair und dem Schlüssel INFO verschlüsselt und soll nun wieder entschlüsselt werden:
OBUYQMFUSEZGRGLBFUHMOZOINQYBSNIPTCIWCTTUIFEGFW

Asymmetrische Verschlüsselungsverfahren

Die symmetrischen Verschlüsselungsverfahren sind natürlich nicht der Weisheit letzter Schluss. Die gezeigten bisher gezeigten Verfahren sind sehr alt und es gibt bereits viele Verfahren diese effizient zu knacken. Dennoch gibt es komplizierte symmetrische Verfahren, wie die AES(Advanced Encryption Standard)-Verschlüsselung. Ein allzu oft auftretendes Problem ist das Mithören oder Mitschneiden von Nachrichten sowie das Verwenden des gleichen Verfahrens zur Ver- und Entschlüsseln. Das Gegenteil dazu bieten die asymmetrischen Verschlüsselungsverfahren. Jeder Kommunikationspartner erhält einen öffentlichen Schlüssel (den auch jeder kennen darf) und einen geheimen Schlüssel (den natürlich nur der Nutzer kennen darf). Der öffentliche Schlüssel verschlüsselt eine Nachricht und der private Schlüssel entschlüsselt die Nachricht wieder. Ein sehr bekanntes Verschlüsselungsverfahren ist RSA, benannt nach seinen Erfindern Ronald Rivest, Adi Shamir und Leonard Adleman. Dabei kommen Primzahlen sowie Gesetze der algebraischen Zahlentheorie zum Einsatz. Im Allgemeinen ist es nämlich sehr schwer die Primfaktoren einer Zahl herauszufinden. Wer es nicht glaubt, kann auf die Schnelle probieren, die beiden Primfaktoren von 50.056.021 herauszufinden.