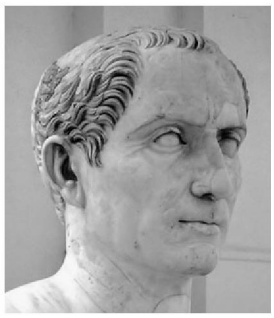
3. Monoalphabetische Substitution

Die Alternative zur Transposition ist die Substitution. Es gibt verschiedene Arten der Substitution, die jedoch alle auf demselben Prinzip beruhen: Nicht die Anordnung der Buchstaben wird verändert, sondern die Buchstaben werden durch andere Buchstaben, Zahlen oder Zeichen ersetzt.

Die einfachste Art der Substitution ist die sogenannte monoalphabetische Substitution.

Die Caesar-Verschlüsselung & ROT13



Julius Caesar

Julius Caesar war der Erste, von dem überliefert ist, dass er eine monoalphabetische Substitution verwendete, um seine geheimen Nachrichten zu verschlüsseln. Deshalb ist diese Verschlüsselung nach ihm benannt. Die Idee ist simpel: Ein Klartextalphabet wird mit einem Geheimtextalphabet verschlüsselt. Das Geheimtextalphabet ist dabei mit dem Klartextalphabet identisch, allerdings **um drei Stellen verschoben**:

Klartextalphabet:	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
Geheimtextalphabet:	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

Klartext: Lieber arm dran als Arm ab!
Geheimtext: Olhehu dup gudq dov Dup de!

8 Ein berühmtes Zitat Caesars lautet: „Proditionem amo, sed proditores non laudo.“ Frei übersetzt bedeutet das: „Ich liebe den Verrat, aber ich verachte die Verräter.“ Die Angst vor Verrätern trieb Caesar dazu, seine Botschaften zu verschlüsseln, denn wenn ein Bote eine Nachricht gar nicht lesen konnte, konnte er sie auch nicht ausplaudern. Welches Buchstabengewirr entstand aus der folgenden wichtigen Botschaft, nachdem Caesars Chefkryptograf diese verschlüsselt hatte?

DIE SPINNEN DIE GALLIER

9 Obelix ist bei der Wildschweinjagd auf eine römische Patrouille gestoßen und hat dem Römer Claudius Nimdenbus die folgende Botschaft abgenommen:

XQWHU GHQ NOHLQVWHQ VWHSSGHFNHQ NDQQ GHU
JURHVVWH GHSS VWHFNHQ

Welche Lebensweisheit erhält man, wenn man die Botschaft entschlüsselt?

Monoalphabetische Substitution

10 Der griechische Lehrer Artemidorus überreichte Caesar vor Beginn der Senatssitzung am 15. März 44 v. Chr. eine Schriftrolle mit dem folgenden Inhalt:

YHUVFKZRHUHU SODQHQ DWWHQWDW IXHU KHXWH (DXFK EUXWXV)

Caesar hatte keine Zeit und gab die Schriftrolle ungelesen an ein Stabsmitglied weiter. Wenige Stunden später war er tot. Was hätte er erfahren, wenn er die Nachricht entschlüsselt hätte?

3 *Programmieraufgabe*

Schreibe ein Programm, das einen Klartext mittels Caesar-Verschlüsselung verschlüsseln kann und zudem einen mit der Caesar-Verschlüsselung verschlüsselten Geheimtext entschlüsseln kann.

Statt das Geheimtextalphabet (wie Caesar es meist tat) um genau drei Stellen zu verschieben, kann man natürlich auch jede andere Verschiebung wählen. Ein Sonderfall stellt die Verschiebung um 13 Stellen dar, die auch als **ROT13** bezeichnet wird (ROT für rotate; engl.: rotieren). Die Besonderheit liegt darin, dass das Ver- und Entschlüsseln exakt identisch ablaufen, da die Buchstaben hier sozusagen Pärchen bilden (wird a mit N verschlüsselt, so wird n mit A verschlüsselt etc.).

11 Welche Erkenntnis verbirgt sich hinter dieser wirren Aneinanderreihung von Buchstaben?

JRAA QVR XYHRTRERA VZZRE ANPUTRORA, TRFPUVRUG AHE QNF,
JNF QVR QHZZRA JBYYRA

4 *Programmieraufgabe*

Erweitere das Programm aus Programmieraufgabe 3 um eine Möglichkeit, die Anzahl der Stellen einzugeben, um die das Geheimtextalphabet im Vergleich zum Klartextalphabet verschoben werden soll. Dabei sollen ganzzahlige Werte zwischen 1 und 25 einstellbar sein.

Einfache monoalphabetische Substitution

Die Caesar-Verschiebung hat einen großen Nachteil: Es gibt nur 25 verschiedene Geheimtextalphabete. Selbst ohne Computer ist es deshalb einem gegnerischen Spion problemlos möglich, einfach alle 25 durchzuprobieren und so recht schnell die Nachricht zu entziffern. Verwendet man als Geheimtextalphabet jedoch statt einer Verschiebung eine **beliebige Neuanordnung des Klartextalphabets**, dann gibt es etwa 400 000 000 000 000 000 000 000 000 (400 Quadrillionen) mögliche Schlüssel. Könnte ein gegnerischer Agent jede Sekunde einen möglichen Schlüssel prüfen, würde er trotzdem etwa die milliardenfache Lebensdauer des Universums benötigen, um alle Schlüssel zu testen.

Am sichersten ist eine völlig willkürliche Anordnung, allerdings hat diese den Nachteil, dass sich der Empfänger die Anordnung schlecht merken kann und sie deshalb vermutlich irgendwo notieren wird, was im Falle einer Hausdurchsuchung fatale Folgen haben könnte. Deshalb wird in der Praxis ein Codewort verwendet, das man sich leicht merken kann, z. B. „Chuck Norris“.

Dieses Codewort wird in Großbuchstaben geschrieben, und dabei werden doppelt auftretende Buchstaben nur einmal verwendet. Aus „Chuck Norris“ wird so CHUKNORIS. An diese Buchstaben werden die noch nicht vorkommenden Buchstaben angehängt, und zwar am besten so, dass das normale Alphabet am letzten Buchstaben quasi fortgesetzt wird.

CHUKNORIS endet mit einem S, danach kommt also T, dann geht es weiter mit V (U ist ja bereits in CHUKNORIS enthalten), WXYZABDEFGJLMPQ. Fertig ist das Geheimtextalphabet:

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

12 Du willst deinem Kontaktmann in Kairo, mit dem du dich auf das Codewort „Nofretete“ geeinigt hast, die folgende Botschaft schicken. Was steht in deiner Nachricht?

DIE SCHWALBE HAT UNTER FOLTER ALLES VERRATEN STOP
SOFORTIGER ABBRUCH VON OPERATION KLEOPATRA

13 Entschlüssle den folgenden Befund, den ein humorvoller Arzt in Form eines Schüttelreims notiert (und aus Datenschutzgründen mit der einfachen monoalphabetischen Substitution, Codewort „dumm gelaufen“, verschlüsselt) hat:

GDY HENSLDYY, GDY LXDB HEUEX QEEXZE, CEXFEEXZE NFXE QEUEXHEXZE

14 Du hast im Papierkorb eines gegnerischen Agenten einen verknüllten Zettel mit der folgenden Nachricht gefunden:

ZQ EQR SJQ BZHSJBZJ, YZJ SQ-MPDZQEYZJRZJ YSPLC ZEJZJ
SJQZPZP GHKJZ XS ZPQZRXZJ!

Unten auf dem Zettel hat jemand handschriftlich das Wort „Dolly“ hingeschrieben. Welche unglaubliche Nachricht hat der Agent hier erhalten?

Monoalphabetische Substitution

5 *Programmieraufgabe*

Schreibe ein Programm, das einen Klartext mittels einfacher monoalphabetischer Substitution verschlüsseln kann und zudem einen mit der einfachen monoalphabetischen Substitution verschlüsselten Geheimtext entschlüsseln kann. Das Codewort soll eingegeben und geändert werden können.

Obwohl es aufgrund der Vielzahl der möglichen Schlüssel praktisch nicht möglich ist, die einfache monoalphabetische Substitution durch systematisches Ausprobieren zu knacken, wurde bereits im neunten Jahrhundert eine Methode bekannt, mit der längere Nachrichten entschlüsselt werden konnten, wenn man nur wusste, in welcher Sprache diese verfasst waren: Man führte eine **Häufigkeitsanalyse** der Buchstaben an einem gewöhnlichen Text derselben Sprache durch und stellte so fest, welche Buchstaben in der Sprache am häufigsten vorkommen.

Im Deutschen ist der häufigste Buchstabe das e, gefolgt von n, i, s und r. Tritt im verschlüsselten Text also beispielsweise der Buchstabe L am häufigsten auf, so ist die Wahrscheinlichkeit groß, dass diesem im Klartextalphabet das e entspricht.

In der folgenden Übersicht sind die Häufigkeiten der einzelnen Buchstaben im Deutschen angegeben:

A 6,51 %	H 4,76 %	O 2,51 %	V 0,67 %
B 1,89 %	I 7,55 %	P 0,79 %	W 1,89 %
C 3,06 %	J 0,27 %	Q 0,02 %	X 0,03 %
D 5,08 %	K 1,21 %	R 7,00 %	Y 0,04 %
E 17,40 %	L 3,44 %	S 7,27 %	Z 1,13 %
F 1,66 %	M 2,53 %	T 6,15 %	
G 3,01 %	N 9,78 %	U 4,35 %	

Hat man einzelne Buchstaben entschlüsselt bzw. geraten, so schaut man sich die kurzen Wörter, insbesondere die mit drei Buchstaben, an. Die häufigsten deutschen Wörter mit drei Buchstaben sind „die“, „der“, „und“, „den“, „das“, „von“ und „sie“.

15

a) Knacke gemeinsam mit einem Partner den folgenden (mit einer einfachen monoalphabetischen Substitution verschlüsselten) Geheimtext, indem du eine Häufigkeitsanalyse durchführst.
b) Wie lautet das Codewort, das zur Generierung des Geheimtextalphabets verwendet wurde?

QL BCWVPJ BUT KPZDVVUV JESFCES
BDTWV, BUV BWFES CT GUNDVBU,
CSV JESFLGUV BCU SDUJESUZ CV IDVBU.
„NDJ NWFFKUJK BL TCK BUT BWFESU, JXZCES!“
UVKGUGVUK CST RCVJKUZ BUZ NLUKUZCES.
„BCU JKDBK MWT KPZDVVUV IURZUCUV!“
„BDJ JWFFJK BL DT AZULQU IUZULUV.“

Eine leicht zu knackende Verschlüsselung ist uns natürlich nicht gut genug. Da sämtlichen monoalphabetischen Verfahren der Makel anhaftet, dass sie mittels Häufigkeitsanalyse geknackt werden können, benötigen wir etwas ganz anderes. Dies führte zur Entdeckung polyalphabetischer Substitutionsverfahren.