Informatik

Kryptographie und Kryptoanalyse

Seit jeher ist es notwendig gewesen, Mitteilungen vor unbefugtem Lesen zu schützen.

- **Kryptographie** ist das Forschungsgebiet, das sich mit den Methoden der Ver- und Entschlüsselung von Nachrichten beschäftigt.
- Die **Kryptoanalyse** versucht und entwickelt Methoden, verschlüsselte Nachrichten mit unbekanntem Schlüssel zu entschlüsseln.

Informatik

Kryptographie und Kryptoanalyse

! negroM netuG

Informatik
Kryptographie und Kryptoanalyse

Caesar-Verschiebung

YHQL YLGL YLFL

XGPK XKFK XKEK

WFOJ WJEJ WJDJ

VENI VIDI VICI

Informatik
Kryptographie und Kryptoanalyse

Caesar-Verschiebung

Eine besonders einfache Form der Verschlüsselung ist die **Caesar-Verschiebung.** Dabei werden die Buchstaben im Alphabet einfach um ein paar Stellen verschoben:

```
abcdefghijklmnopqrstuvwxyz
DEFGHIJKLMNOPQRSTUVWXYZABC
```

Damit kann ein Satz verschlüsselt werden:

```
ach, was muss man oft von boesen
DFK, ZDV PXVV PDQ RIW YRQ ERHVHQ
```

```
kindern hoeren oder lesen
NLQGHUQ KRHUHQ RGHU OHVHQ
```

Die Analyse eines durch Caesar-Verschiebung verschlüsselten Textes ist sehr einfach.

Informatik
Kryptographie und Kryptoanalyse

Monoalphabetische Substitution

Eine Verallgemeinerung der Caesar-Verschiebung ist die **monoalphabetische Substitution** der Zeichen. Dabei wird jedes Zeichen durch -stets dasselbe- andere ersetzt, aber die Reihenfolge der Buchstaben ist nicht mehr gegeben.

Beispiel

```
abcdefghijklmnopqrstuvwxyz
ZYWUHGFQMEDCBTVAOILPRJKSNX
```

Damit wird der bekannte Satz folgendermaßen verschlüsselt:

```
ach, was muss man oft von boesen
ZWQ, KZL BRLL BZT VGP JVT YVHLHT

kindern hoeren oder lesen
DMTUHIT QVHIHT VUHI CHLHT
```

Informatik
Kryptographie und Kryptoanalyse

Monoalphabetische Substitution

Die monoalphabetische Substitution ist durch **Häufigkeitsanalyse** zu brechen. Normalerweise kommen die verschiedenen Buchstaben in Texten unterschiedlich häufig vor:

Buchstaben-häufigkeit	**häufige Zweier-gruppen**	**häufige Dreier-gruppen**	**häufige Wörter**
e 17,5 %	er	ein	am
n 9,8 %	en	ich	in
i 7,7 %	ch	nde	zu
r 7,5 %	de	die	es
s 6,8 %	ei	und	
a 6,5 %	nd	der	die
t 6,1 %	te	che	der
d 4,8 %	in	end	und
h 4,2 %	ie	gen	den
u 4,2 %	ge	sch	
l 3,5 %			
g 3,1 %			
o 3,0 %			
c 2,7 %			
m 2,6 %			
b 1,9 %			
f 1,7 %			
w 1,5 %			
k 1,5 %			
z 1,1 %			
p 1,0 %			
v 0,9 %			
j 0,3 %			
y 0,1 %			
x < 0,1 %			
q < 0,1 %			

Informatik
Kryptographie und Kryptoanalyse

Monoalphabetische Substitution

Gegeben sei der folgende durch monoalphabetische Substitution verschlüsselte Text:

```
NZ XRFNI SXNP LHNIPMZLPIQNF,
QPN YREENI NPIRIQNF ZH KPNO;
ZPN LHIIENI SDZRJJNI IPUYE LHJJNI,
QRZ XRZZNF XRF CPNK SD EPNT.

"RUY KPNOZENF, LRIIZE QD IPUYE ZUYXPJJNI,
ZH ZUYXPJJ QHUY YNFDNONF SD JPF!
```

Informatik
Kryptographie und Kryptoanalyse

Monoalphabetische Substitution

Gegeben sei der folgende durch monoalphabetische Substitution verschlüsselte Text:

```
NZ XRFNI SXNP LHNIPMZLPIQNF,
QPN YREENI NPIRIQNF ZH KPNO;
ZPN LHIIENI SDZRJJNI IPUYE LHJJNI,
QRZ XRZZNF XRF CPNK SD EPNT.

"RUY KPNOZENF, LRIIZE QD IPUYE ZUYXPJJNI,
ZH ZUYXPJJ QHUY YNFDNONF SD JPF!
QFNP LNFSNI XPKK PUY RISDNIQNI,
DIQ QPN ZHKKNI KNDUYENI QPF."

QRZ YHNFE NPIN TRKZUYN IHIIN,
QPN ERE, RKZ HO ZPN ZUYKPNT.
ZPN ERNE QPN LNFSNI RDZKHNZUYNI,
QNF WDNIMKPIM NFEFRIL ZH EPNT.

NZ XRF RI NPI'J ZHIIERMJHFMNI,
QPN KNDEN XRF'I RKKN ZH TFHY,
IPUYE ZH QPN LHNIPMZEHUYENF,
QPN RDMNI ZRZZNI PYF SD.

"RUY TPZUYNF, KPNOZENF TPZUYNF,
XPKKZE QD QPF CNFQPNINI MFHZZ' KHYIZ
ZH XPFT QNPI INES PIZ XRZZNF
DIQ TPZUY' JPF QNI LHNIPMZZHYI."

NF XRFT QRZ INES PIZ XRZZNF,
NZ MPIM OPZ RDT QNI MFDIQ;
QNF NFZEN TPZUY, QNI NF TPZUYNE,
QRZ XRF QNZ LHNIPMZ ZHYI.

ZPN TRZZE PYI PI PYFN RFJN
DIQ LDNZZE ZNPINI EHENI JDIQ:
"RUY JDNIQKNPI, LHNIIENZE QD ZVFNUYNI,
ZH XRNF JNPI WDIM' YNFS MNZDIQ !"

XRZ IRYJ ZPN CHI PYFNJ YRDVEN?
NPIN MHKQNIN LHNIPMZLFHI:
"ZPNY QR XHYK NQKNF TPZUYNF,
YRZE QNPI' CNFQPNIENI KHYI!"

ZPN ZUYKHZZ PYI RI PYF YNFSN
DIQ ZVFRIM JPE PYJ PI QPN ZNN:
"MDE IRUYE, JNPI CRENF DIQ JDEENF,
PYF ZNYE JPUY IPJJNFJNY!"

KPNQ RDZ QNF KRYIMNMNIQ

JHFRK CHI QNF MNZUYPUYEN:
YRNEENI ZPN PYFN OHEZUYRTE FPUYEPM
CNFZUYKDNZZNKE, XRNFN QRZ IPUYE VRZZPNFE!
```

Informatik
Kryptographie und Kryptoanalyse

Monoalphabetische Substitution

Die Häufigkeitsanalyse des Textes ergibt folgendes Resultat:

Buchstaben		Zweier-gruppen		Dreier-gruppen		einzelne Wörter	
N	151	NI	37	ZUY	15	QPN	8
I	99	NF	36	NPI	10	ZH	7
Z	91	UY	31	QPN	10	ZPN	7
P	87	PN	27	UYE	9	DIQ	5
F	65	PI	17	ZPN	9	QRZ	5
Y	59	EN	16	DIQ	8	IPUYE	4
R	53	ZU	15	PUY	8	QNF	4
E	52	QN	14	UYN	7	NZ	3
Q	49	IQ	13	ENI	6	PYF	3
H	39	RZ	13	HNI	6	QD	3
D	31	NP	12	LHN	6	QNI	3
K	31	QP	12	PYF	6	RUY	3
U	31	XR	12	PZU	6	SD	3
J	27	ZH	11	QNF	6	TPZUYNF	3
M	23	ZZ	11	RZZ	6	XRF	3
X	19	IP	10	TPZ	6	XRZZNF	3
T	16	NZ	10	XRF	6	CHI	2
L	15	YE	10	YNF	6	EPNT	2
S	12	YN	10	ENF	5	INES	2
C	7	ZE	10	IPM	5	JNPI	2
O	7	DI	9	KPN	5	JPF	2
V	4	PY	9	NIP	5	KPNOZENF	2
W	2	ZP	9	PMZ	5	LNFSNI	2
A	0	HN	8	QNI	5	NF	2
B	0	IN	8	QRZ	5	NPIN	2
G	0	JN	8	ZZN	5	PI	2

Informatik
Kryptographie und Kryptoanalyse

Monoalphabetische Substitution

Folgende Zeichen und Wörter können nach kurzer Überlegung erkannt werden:

Buchstaben			Zweier-gruppen		Dreier-gruppen		einzelne Wörter	
N	e	151	en	NI 37	sch	ZUY 15	QPN	die 8
I	n	99	er	NF 36	ein	NPI 10	ZH	so 7
Z	s	91	ch	UY 31	die	QPN 10	ZPN	sie 7
P	i	87	ie	PN 27	cht	UYE 9	DIQ	und 5
F	r	65	in	PI 17		ZPN 9	QRZ	das 5
Y	h	59	te	EN 16		DIQ 8	nichtIPUYE	4
R	a	53		ZU 15		PUY 8	QNF	der 4
E	t	52		QN 14		UYN 7	NZ	es 3
Q	d	49		IQ 13		ENI 6	PYF	3
H	h	39		RZ 13		HNI 6	QD	du 3
D	u	31		NP 12		LHN 6	QNI	den 3
K		31		QP 12		PYF 6	RUY	3
U	c	31		XR 12		PZU 6	SD	3
J		27		ZH 11		QNF 6	TPZUYNF	3
M		23		ZZ 11		RZZ 6	XRF	3
X		19		IP 10		TPZ 6	XRZZNF	3
T		16		NZ 10		XRF 6	CHI	2

Wir machen einen ersten Entschlüsselungsversuch mit folgenden Ersetzungen:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
___utr_on____e_ida__c___hs
```

Informatik
Kryptographie und Kryptoanalyse

Monoalphabetische Substitution

Bei dem fraglichen Text reicht dieser Versuch völlig, den Rest zu erschließen:

```
es _aren __ei _oeni_s_inder,
die hatten einander so _ie_;
sie _onnten _usa__en nicht _o__en,
das _asser _ar _ie_ _u tie_.

"ach _ie_ster, _annst du nicht sch_i__en,
so sch_i__ doch herue_er _u _ir!
```

Informatik
Kryptographie und Kryptoanalyse

Monoalphabetische Substitution

Bei dem fraglichen Text reicht dieser Versuch völlig, den Rest zu erschließen:

```
es _aren __ei _oeni_s_inder,
die hatten einander so _ie_;
sie _onnten _usa__en nicht _o__en,
das _asser _ar _ie_ _u tie_.

"ach _ie_ster, _annst du nicht sch_i__en,
so sch_i__ doch herue_er _u _ir!
drei _er_en _i__ ich an_uenden,
und die so__en _euchten dir."

das hoert eine _a_sche nonne,
die tat, a_s o_ sie sch_ie_.
sie taet die _er_en aus_oeschen,
der _uen__in_ ertran_ so tie_.

es _ar an ein'_ sonnta__or_en,
die _eute _ar'n a__e so _roh,
nicht so die _oeni_stochter,
die au_en sassen ihr _u.

"ach _ischer, _ie_ster _ischer,
_i__st du dir _erdienen _ross' _ohns
so _ir_ dein net_ ins _asser
und _isch' _ir den _oeni_ssohn."

er _ar_ das net_ ins _asser,
es _in_ _is au_ den _rund;
der erste _isch, den er _ischet,
das _ar des _oeni_s sohn.

sie _asst ihn in ihre ar_e
und _uesst seinen toten _und:
"ach _uend_ein, _oenntest du s_rechen,
so _aer _ein _un_' her_ _esund !"

_as nah_ sie _on ihre_ hau_te?
eine _o_dene _oeni_s_ron:
"sieh da _oh_ ed_er _ischer,
hast dein' _erdienten _ohn!"

sie sch_oss ihn an ihr her_e
und s_ran_ _it ih_ in die see:
"_ut nacht, _ein _ater und _utter,
ihr seht _ich ni__er_eh!"

_ied aus der _ahn_e_end

_ora_ _on der _eschichte:
haetten sie ihre _otscha_t richti_
_ersch_uesse_t, _aere das nicht _assiert!
```

Informatik
Kryptographie und Kryptoanalyse

Monoalphabetische Substitution

Das Ergebnis der Entschlüsselung:

```
es waren zwei koenigskinder,
die hatten einander so lieb;
sie konnten zusammen nicht kommen,
das wasser war viel zu tief.

"ach liebster, kannst du nicht schwimmen,
so schwimm doch herueber zu mir!
drei kerzen will ich anzuenden,
und die sollen leuchten dir."

das hoert eine falsche nonne,
die tat, als ob sie schlief.
sie taet die kerzen ausloeschen,
der juengling ertrank so tief.

es war an ein'm sonntagmorgen,
die leute war'n alle so froh,
nicht so die koenigstochter,
die augen sassen ihr zu.

"ach fischer, liebster fischer,
willst du dir verdienen gross' lohns
so wirf dein netz ins wasser
und fisch' mir den koenigssohn."

er warf das netz ins wasser,
es ging bis auf den grund;
der erste fisch, den er fischet,
das war des koenigs sohn.

sie fasst ihn in ihre arme
und kuesst seinen toten mund:
"ach muendlein, koenntest du sprechen,
so waer mein jung' herz gesund !"

was nahm sie von ihrem haupte?
eine goldene koenigskron:
"sieh da wohl edler fischer,
hast dein' verdienten lohn!"

sie schloss ihn an ihr herze
und sprang mit ihm in die see:
"gut nacht, mein vater und mutter,
ihr seht mich nimmermeh!"

lied aus der lahngegend

moral von der geschichte:
haetten sie ihre botschaft richtig
verschluesselt, waere das nicht passiert!
```

Informatik
Kryptographie und Kryptoanalyse

Transposition

Eine andere Möglichkeit stellt die **Transposition** der Zeichen dar:

```
ach, was muss man oft von boesen

A    W    U    A    T         E
 C    A    S    N         B    N
  H    S    S         V    O
   ,              O    O    E
        M    M    F    N    S

AWUAT ECASN BNHSS VO,  OOE MMFNS

kindern hoeren oder lesen
K    R    E    O    L
 I    N    R    D    E
  N         E    E    S
   D    H    N    R    E
    E    O              N

KREOLINRDEN EESDHNREEO  N
```

Informatik
Kryptographie und Kryptoanalyse

Transposition

Gegeben sei der folgende durch Transposition verschlüsselte Text:

```
WTSUC EEPRHWRTACTI  EH NRST UDEO NN?I DAD
EDESKSEREI R INI MNDSVIE;TATM T
EDBLMREE   NNIAH  NRAKW MTNOD, AHE
ETIETAR CR R IH IMFHEHH.ANRAN-S ,E SS LW

MH  BICENBDANHI,IUN TN R GG? WGS E-SASODSOST EI
S   NHIVDEITEAURG?HT L SEDKNTREOI,,NEC
```

Informatik
Kryptographie und Kryptoanalyse

Transposition

Gegeben sei der folgende durch Transposition verschlüsselte Text:

```
WTSUC EEPRHWRTACTI  EH NRST UDEO NN?I DAD
EDESKSEREI R INI MNDSVIE;TATM T
EDBLMREE   NNIAH  NRAKW MTNOD, AHE
ETIETAR CR R IH IMFHEHH.ANRAN-S ,E SS LW

MH  BICENBDANHI,IUN TN R GG? WGS E-SASODSOST EI
S   NHIVDEITEAURG?HT L SEDKNTREOI,,NEC
DEGRDIEN O FNKMNS? OI'C-EET HRN UWLIKNE
MHI TENSNRI,TEEN  BI EEEFSSIL.O NS-

"BD,IDE, TUS G   KEMLKOHIIIM RENMM!
GOIIHIAEEE RRNLLM; EE'IS   TCSSI HPPCD
MBLIDAAUUNENNNMDMDCTE  ;HENAS'  NT BS R
MUAHDAETT'ENIT  NDNEMG .ERAUG"  NEEMHCLW

MTIRH HEEN,ODTIR  EU,N,VUR   ANENVMTDSIAEE TC
WEGERTAN IS?SKMSP- OIEREER IRN VCLILEH
SIIINEGBG I,E,K    IRBRMNULUEDHEHI!
IRESTINETA N NTEDDD EUE.UBRSR-ELNE RA LW

",R,TEW    HIFKDMNLENUI?LIA RSNBM TEEIG
MO  ACEESDRHICOITONHLCEEETLHNN EE  ;TRNWS
MO NACIEEF EHHICUDCENNHEEHNETHNT  ER LRTRENIE
UG  NC"NETUGHDNANE   NDNEWUZ  IINESDNEDNII.

MTIRSDTEEN,IU IR  E DN,VUHNO  ANSIRVMTDTCTAEE  H
EICME?RGH R-LSTDNK EU OTREOEO SRNEATT
MHN HEEN I'NI,SC AN OHEU MH S;SENS OI,EG
EIE  USN WS. EAEO-SNLI C TDGHDEEREINNA

"EH DCG;IB,REHECE EIOSH MINET DIZENALICT ELICH S T
UTCL 'E-N HIB WDDTGRIA U ,ACLB W UHTINISC .SILOHG"
MTIRT HEEN, E IR  FRAN,VJA N  AESM!VMTTSIAEEZTC
EIM GRGILEL RETKH IAOAEDNETIS!N N -

DESEEHERERTWM T  I G'RGNVRSEEDAA,IS,TU TC
ETN C R  DHK IAAZIHNRSENA M NDEDEAD,LENEE
ETOMNR FUDRD E EEMHNINIEOC T THH U;
IENI NN NT  DDOSAA TERSW.IM ANEKR

JWGOOO EHLVTAFOHNGNENA  NG
```

Transposition

Die Entschlüsselung einer regelmäßigen Transposition ist mit Hilfe eines kurzen Programmes sehr einfach, da man lediglich bei 1 beginnend probieren muss:

```
>D ^KNACKTR("Gedicht3Tr.txt","Gedicht3OK.txt")
N=1
wtsuc eeprhwrtacti  eh nrst udeo nn?i dad
O.K. ? n
N=2
wht snurcs te eupdrehow rntna?cit id a de
O.K. ? n
N=3
wautcdsteuioc    neeneh?p irn hrdwsartdt
O.K. ? n
N=4
wwhotr  stnnuarnccs? ttiei  e udp dareedh
O.K. ? n
N=5
wrisnth tnsw  ?ureuicthd  a edecnoaetr dp
O.K. ? n
N=6
weahu?tpc disrtne uhirodcw s a r tndete n
O.K. ? n
N=7
wer reitet so spaet durch nacht und wind?
O.K. ? y
```

Informatik
Kryptographie und Kryptoanalyse

Transposition

Das Ergebnis der Entschlüsselung:

```
wer reitet so spaet durch nacht und wind?
es ist der vater mit seinem kind;
er hat den knaben wohl in dem arm,
er fasst ihn sicher, er haelt ihn warm.-

mein sohn, was birgst du so bang dein gesicht?-
siehst, vater, du den erlkoenig nicht?
den erlenkoenig mit kron’ und schweif?-
mein sohn, es ist ein nebelstreif.-

"du liebes kind, komm, geh mit mir!
gar schoene spiele spiel’ ich mit dir;
manch’ bunte blumen sind an dem strand;
meine mutter hat manch’ guelden gewand."

mein vater, mein vater, und hoerest du nicht,
was erlenkoenig mir leise verspricht?-
sei ruhig, bleibe ruhig, mein kind!
in duerren blaettern saeuselt der wind.-

"willst, feiner knabe, du mit mir gehn?
meine toechter sollen dich warten schoen;
meine toechter fuehren den naechtlichen reihn
und wiegen und tanzen und singen dich ein."

mein vater, mein vater, und siehst du nicht dort
erlkoenigs toechter am duestern ort?-
mein sohn, mein sohn, ich seh’ es genau;
es scheinen die alten weiden so grau.-

"ich liebe dich, mich reizt deine schoene gestalt;
und bist du nicht willig, so brauch’ ich gewalt."-
mein vater, mein vater, jetzt fasst er mich an!
erlkoenig hat mir ein leids getan!-

dem vater grauset’s, er reitet geschwind,
er haelt in den armen das aechzende kind,
erreicht den hof mit muehe und not;
in seinen armen das kind war tot.

johann wolfgang von goethe
```

Polyalphabetische Substitution

Monoalphabetische Substitution und Transposition sind ausgesprochen leicht zu brechende Verschlüsselungstechniken. Etwas sicherer ist die **polyalphabetische Substitution,** bei der ein und derselbe Buchstabe durch **verschiedene** andere ersetzt wird.

Eine polyalphabetische Substitution könnte etwa folgendermaßen realisiert werden:

1. Vereinbare ein **Schlüsselwort**.
2. Schreibe dieses -wenn nötig wiederholt- unter den zu verschlüsselnden Text.
3. Suche aus der ASCII-Zeichentabelle die Werte für jedes Zeichen des Textes und des Schlüsselwortes und schreibe diese jeweils unter jedes Zeichen.
4. Addiere die jeweiligen Zahlenwerte und subtrahiere 62 davon. Wenn das Resultat größer als 96 ist, subtrahiere 96. Anschließend addiere 31.
5. Sieh in der ASCII-Zeichentabelle nach und setze das entsprechende Zeichen ein.

Informatik
Kryptographie und Kryptoanalyse

Polyalphabetische Substitution

Beispiel:

A	c	h	,		w	a	s		m	u	s	s		m	a	n		o	f	t
65	99	104	44	32	119	97	115	32	109	117	115	115	32	109	97	110	32	111	102	116
g	e	h	e	i	m	g	e	h	e	i	m	g	e	h	e	i	m	g	e	h
103	101	104	101	105	109	103	101	104	101	105	109	103	101	104	101	105	109	103	101	104
41	73	81	114	106	101	73	89	105	83	95	97	91	102	86	71	88	110	87	76	93
)	I	Q	r	j	e	I	Y	i	S	_	a	Ä	f	V	G	X	n	W	L	Ü

"A" entspricht 65 und "g" 103, x=65+103-62=106, da x größer als 96 ist: x=x-96=10, x=x+31=41, entspricht: ")", etc.

Bei diesem Verfahren werden sowohl große und kleine Buchstaben als auch Zwischenräume und Satzzeichen einbezogen.

Informatik
Kryptographie und Kryptoanalyse

Polyalphabetische Substitution

Gegeben sei der folgende durch polyalphabetische Substitution verschlüsselte Text:

```
mGÜoH.KÖod<ZjPi0KPlg5ZjÖd=fAPn<KÖ
>TNop7ZOÜä2Y^vnIHObj7JOanIZSTaW
jSjDa.XjSd.YObävKOa‘<fÜPyIKÖä
-tRüä.XjÄÖ0rjf‘2RjTmIPKon,NVX‘/t
ßTNoi>TjÜj,NWPgcf+ÖävKOa‘IYKmä.Xv
-tRüä.XjÄÖ0rjf‘2RjTmIPKon,NVX‘/
>TNod7fNThI3OTmIÜKaä<KRaä?OOÄä GÜb‘;
>TNop7ZOÜä§GÖvnIHObj7JOanIZSTaW

mGj_gEZdÄd,Njc‘2R^TiIYSRcIJSTäoR_c‘7
>TNo‘2TOoE>TQUm*Äjcm*ZjW‘;Lga
<OOoo*ZjPp/fOXi.Xj5gEZOoo>ZOÜ
-GÜor*XjZ‘2Tjb^1bXTmI§_Vä?UXod1Xx
mKWoA2YMW‘;fQXi0fNPnI2ST_I‘_oC.XdTiU
8Ha^c5fÜX‘ILKÄn,NOoOETOok/UPUäVsw
6GXon*NjXc7fSÜä-GÜoR*YÜTmIY^TmCKX
-GXÜä0OXVä.Xjdi=KÖop7JjTm<UPU)

qKSÜuI+Rac*XNc5I*OaäoOÜRc.X
```

Informatik
Kryptographie und Kryptoanalyse

Polyalphabetische Substitution

Auch polyalphabetische Substitution kann -wenn der Text lang genug ist oder viele mit demselben Wort verschlüsselte Texte vorliegen, durch eine Häufigkeitsanalyse erschlossen werden. Jedes Zeichen wird auf genau so viele verschiedene Arten dargestellt, wie das Schlüsselwort lang ist. Dasselbe gilt natürlich auch für häufige Wörter.

Beispiel (das Schlüsselwort sei "geheim"):

d	i	e	d	i	e	d	i	e	d	i	e	d	i	e	d	i	e
100	105	101	100	105	101	100	105	101	100	105	101	100	105	101	100	105	101
g	e	h	e	h	e	h	e	i	e	i	m	i	m	g	m	g	e
103	101	104	101	104	101	104	101	105	101	105	109	105	109	103	109	103	101
76	79	78	74	82	75	77	79	79	74	83	83	78	87	77	82	81	75
L	O	N	J	R	K	M	O	O	J	S	S	N	W	M	R	Q	K

Aus dem Abstand des Auftretens lässt sich dann zunächst die Länge des Schlüsselwortes bestimmen und anschließend eine Häufigkeitsanalyse für das Zeichen, das jeweils an der ersten (zweiten, dritten, etc.) Stelle des Schlüsselwortes steht durchführen.

Informatik
Kryptographie und Kryptoanalyse

Polyalphabetische Substitution

Ist das Schlüsselwort einer polyalphabetischen Substitution etwa ein **Vorname,** können mit Hilfe einer entsprechenden Datenbank alle Namen durchprobiert werden. Ergeben sich bei einem solchen mehrere sinnvolle Wörter (ebenfalls automatisch prüfbar) kann das Resultat dem Benutzer zur Entscheidung dargeboten werden:

```
>D ^KNACKPO("Gedicht6Po.txt")
Was für Vornamen (w=weiblich/m=männlich) ? m

Schlüsselwort: Heino
Das Xeer tst aygefüwlt mtt Waßser
und  nten+ist’ß beszndерß tieq.
Am Uqer dteses+Meerps sa) er,
d.h.+er llg, wpil eü ja ßchlipf.
O.K. (j/n) ?  n

Schlüsselwort: Heinz
Das Meer ist angefüllt mit Wasser
und unten ist’s besonders tief.
Am Ufer dieses Meeres saß er,
d.h. er lag, weil er ja schlief.
O.K. (j/n) ?  j
```

Merke: Niemals Vornamen als Schlüssel- oder Passwort verwenden!

Informatik
Kryptographie und Kryptoanalyse

Polyalphabetische Substitution

Das Ergebnis der Entschlüsselung:

```
Das Meer ist angefüllt mit Wasser
und unten ist’s besonders tief.
Am Ufer dieses Meeres saß er,
d.h. er lag, weil er ja schlief.
Und nun nochmal: Am Meere saß er,
d.h. er lag, weil er ja schlief
und in dem Meer war sehr viel Wasser
und unten war’s besonders tief.

Da plötzlich teilten sich die Fluten
und eine Jungfrau trat herfür
sie tat auf einer Flöte tuten
das war kein schöner Zug von ihr.
Dem Fischer ging das Lied zu Herzen,
obwohl sie falsche Töne pfoff ---
man sah ihn in das Wasser sterzen
dann ging er unter und ersoff.

Heinz Ehrhardt: Der Fischer
```

Informatik
Kryptographie und Kryptoanalyse

Polyalphabetische Substitution

Gegeben sei der folgende durch polyalphabetische Substitution verschlüsselte Text:

```
r$R.5t^.DpR":vS NüQöQfUsDt
HtUr6#loF"SsCtOv?t‘.5xQ!6
6xZsQZavÜ/Qw?tlYFwz

rrT:QxT QWQ K/U!E/bü=äQ QbQv?tZ:
FüP.:ölOFvQ.DrTw>öQ ?/§ LüQö
2ql#?sl(F;lo3/aö5/f#_

(p_.:w^.DrTä6rW"6;l%:tPsCzM#E/_s
>x‘.5t^.$rTö2$fsÜ/Po?ül$6!PoF#l!6
FüP.>pOvE/9#9;l#?slä2rT"QÖav_

DrToF#l!:tlrLöXw4wlw?/Pw6/3s8tZr
8!MrQ&UsQsa:Qv^o5/cw6/P#_

ytUöK/1 9p^rEIlR:tlYFw
```

Polyalphabetische Substitution

Ist das Schlüsselwort einer polyalphabetischen Substitution hinreichend **kurz**, können systematisch alle Möglichkeiten ausprobiert werden (sog. **brute force attack**). Ergeben sich dabei mehrere sinnvolle Wörter kann das Ergebnis in eine extra Datei geschrieben werden, die sich der Benutzer hinterher ansehen kann:

```
>D ^KNACKPR("Gedicht4Pr.txt")
Mögliche Schlüsselwörter:

Schlüsselwort: P.+-
AuF deR saFtigGrünEn WIese
weIdet‘ausGereChneT diEse
eiNe KUh, Eine‘Kuhn

Schlüsselwort: P.k-
Auf der saftiggrünen Wiese
weidet ausgerechnet diese
eine Kuh, eine Kuh.

Schlüsselwort: PNk-
AUf dEr sAftiGgrüNen 7iesE
wEideT auSgerEchnEt dIese
eIne +uh,‘einE KuH.

Schlüsselwort: p.k-
!uf Der SaftIggrÜnen‘WieSe
WeidEt aUsgeRechNet DiesE
Eine‘Kuhl eiNe KUh.
```

Informatik
Kryptographie und Kryptoanalyse

Polyalphabetische Substitution

Merke: Schlüssel- oder Passwörter sollten eine hinreichende Länge haben (mindestens acht Zeichen) und nicht nur aus Buchstaben und Zahlen bestehen.

Prinzipiell können Schlüssel beliebig lang sein (z.B. die amerikanische Unabhängigkeitserklärung oder das 1. Buch Mose). Darüberhinaus kann man mehrere Schlüssel hintereinander anwenden und/oder zusätzlich noch transponieren.

Die wohl bekannteste elektromechanische Verschlüsselungsmaschine, die unter Verwendung der 26 großen lateinischen Buchstaben eine polyalphabetische Substitution durchführt ist die **ENIGMA**.

Der **D**ata **E**ncryption **S**tandard (**DES**) realisiert eine polyalphabetische Substitution auf der Basis von 64-Bit-Blöcken durch wiederholte Substitution und Transposition.

Informatik
Kryptographie und Kryptoanalyse

Polyalphabetische Substitution

Das Ergebnis der Entschlüsselung:

```
Auf der saftiggrünen Wiese
weidet ausgerechnet diese
eine Kuh, eine Kuh.

Ach, ihr Herz ist voller Sehnen,
und im Auge schimmern Tränen
ab und zu, ab und zu.

Was ihr schmeckte, wiederkaut se
mit der Schnauze, dann verdaut se
und macht Muh, und macht Muh.

Träumend und das Maul bewegend
schaut sie dämlich in die Gegend
grad wie du, grad wie du.

Heinz Erhardt: Die Kuh
```

Informatik
Kryptographie und Kryptoanalyse

Schlüsselaustausch

Alle bisher vorgestellten Verfahren verwenden zum Ver- und Entschlüsseln **denselben Schlüssel**, weswegen diese **symmetrisch** genannt werden. Kritischer Vorgang aller symmetrischen Verfahren ist der **Schlüsselaustausch**. Da sowohl Absender zum Ver- als auch der Empfänger zum Entschlüsseln denselben Schlüssel verwenden, muss ein -etwa wegen eines bekannt gewordenen Schlüssels- neu zu vereinbarender auf einem gesonderten **sicheren** Wege vom einen zum anderen gebracht werden. Dies ist normalerweise mit einem sehr großen Aufwand verbunden oder gar unmöglich.

Informatik
Kryptographie und Kryptoanalyse

Diffie-Hellman-Merkle-Verfahren

Das **Diffie-Hellman-Merkle-Verfahren** versucht, mit Hilfe einer Modulrechnung, Abhilfe zu schaffen. Folgenden Rechenschritte müssen Partner A und B durchführen:

	Aktionen von A	**Aktionen von B**
1.	A wählt eine Zahl a und hält sie geheim (z.B. 3)	B wählt eine Zahl b und hält sie geheim (z.B. 6)
2.	A berechnet $\alpha = 7^a \bmod 11$ $7^3 \bmod 11 = 343 \bmod 11 = 2$	B berechnet $\beta = 7^b \bmod 11$ $7^6 \bmod 11 = 117649 \bmod 11 = 4$
3.	A sendet α an B (also: 2)	B sendet β an A (also: 4)
4.	A berechnet $4^3 \bmod 11$ $4^3 \bmod 11 = 64 \bmod 11 = 9$	B berechnet $2^6 \bmod 11$ $2^6 \bmod 11 = 64 \bmod 11 = 9$

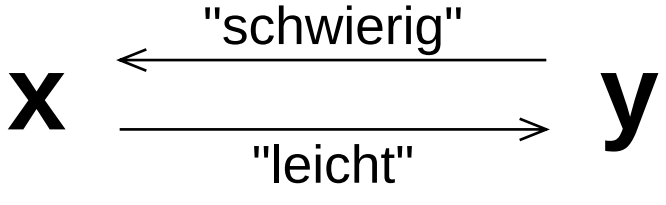
Beide Partner erhalten durch ihre Berechnungen stets **dasselbe Ergebnis.** Der Abhörer kann weder aus der öffentlich bekannten Funktion $7^x \bmod 11$ noch aus den ausgetauschten Zahlen α und β **ohne großen Aufwand** Rückschlüsse auf das von beiden ermittelte Ergebnis ziehen. **Man kann also in einem öffentlichen Gespräch miteinander ein Geheimnis erzeugen!**

Informatik
Kryptographie und Kryptoanalyse

RSA

Zur Vermeidung der Nachteile symmetrischer Verfahren, wurde vorgeschlagen, zum Ver- und Entschlüsseln **verschiedene** Schlüssel zu verwenden. Der zum Verschlüsseln wird **öffentlich** bekannt gegeben, der zum Entschlüsseln bleibt **geheim.** Ein solches Verfahren heißt **Public-Key-System** oder **asymmetrische** Verschlüsselung.

Asymmetrische Verfahren beruhen darauf, dass die Berechnung von einem Schlüssel y aus einem Schlüssel x **leicht**, die Umkehrung, also die Berechnung von x aus y hingegen **schwierig** (d.h. **zeitaufwendig**) ist.



***R**ivest*, ***S**hamir* und ***A**dleman* haben als erste ein solches funktionierendes Verfahren publiziert (und sich patentieren lassen).

Informatik
Kryptographie und Kryptoanalyse

RSA

Schlüsselbestimmung

1. Wähle zwei verschiedene Primzahlen p und q (z.B. 17 und 23).
2. Berechne **n:=p·q** und **z:=(p-1)·(q-1)** (n=391 und z=352 (=2^5·11)).
3. Wähle ein c mit 3≤c<z **und** ggT(c,z)=1 (z.B. 301 (=7·43)).
4. Bestimme das kleinste d, für das **c·d mod z = 1 mod z** gilt (d=69).

Der *öffentliche Schlüssel zum Verschlüsseln* besteht aus den zwei Zahlen n=391 und c=301. Der geheime Schlüssel zum Entschlüsseln ist die Zahl d=69.

Informatik
Kryptographie und Kryptoanalyse

RSA

Verschlüsselung

1. Nimm ein Zeichen oder eine Reihe von Zeichen (Länge abhängig von n) und notiere die zugehörigen Zahlen aus der ASCII-Tabelle und bilde daraus eine Zahl x (z.B. das Zeichen "A", dann ist x=65).
2. Berechne **$y = x^c \bmod n$** (hier: $y = 65^{301} \bmod 391 = 158$).
3. Übertrage y (also 158) zum Partner (der den Schlüssel erzeugt und veröffentlicht hat).

Entschlüsselung

1. Empfange das verschlüsselte Zeichen y (hier: 158).
2. Berechne **$x = y^d \bmod n$** (hier: $x = 158^{69} \bmod 391 = 65$).
3. Sieh in der ASCII-Tabelle nach (hier: x = 65 = "A").

Informatik
Kryptographie und Kryptoanalyse

RSA

Schlüsselbestimmung

1. Wähle zwei verschiedene Primzahlen p und q (z.B. 499 und 773).
2. Berechne **n:=p·q** und **z:=(p-1)·(q-1)** (n=385.727 und z=384.456 (=2^3·3·83·193)).
3. Wähle ein c mit 3≤c<z **und** ggT(c,z)=1 (z.B. 16.541 (=7·17·139)).
4. Bestimme das kleinste d, für das **c·d mod z = 1 mod z** gilt (d=312.125).

Der *öffentliche Schlüssel zum Verschlüsseln* besteht aus den zwei Zahlen n=385.727 und c=16.541. Der *geheime Schlüssel zum Entschlüsseln* ist die Zahl d=312.125.

Informatik
Kryptographie und Kryptoanalyse

RSA

Verschlüsselung

1. Nimm ein Zeichen oder eine Reihe von Zeichen (Länge abhängig von n) und notiere die zugehörigen Zahlen aus der ASCII-Tabelle und bilde daraus eine Zahl x (z.B. die Zeichen "IK", dann ist x=73·256+75=18.763).
2. Berechne **$y = x^c \bmod n$** (hier: $y = 18.763^{16.541} \bmod 385.727 = 248.160$).
3. Übertrage y (also 118.399) zum Partner (der den Schlüssel erzeugt und veröffentlicht hat).

Entschlüsselung

1. Empfange das verschlüsselte Zeichen y (hier: 248.160).
2. Berechne **$x = y^d \bmod n$** (hier: $x = 248.160^{312.125} \bmod 385.727 = 18.763$).
3. Zerlege die erhaltene Zahl und sieh in der ASCII-Tabelle nach (hier: x = 18.763 = 73·256+75 = "IK").

RSA

Die Sicherheit des RSA-Verfahrens beruht darauf, dass die genannten Rechnungen -auch für sehr große Zahlen- schnell durchgeführt werden können, die **Zerlegung** von n **in** seine **Primfaktoren** p und q jedoch sehr schwierig ist. Allerdings müssen die Zahlen p und q sehr groß gewählt werden (mehrere hundert Stellen), damit niemand vom Produkt n darauf zurückrechnen kann.

In der folgenden Tabelle wird der Zeitbedarf für die Faktorisierung von n geschätzt, wobei davon ausgegangen wurde, dass sich die Geschwindigkeit von Computern alle zwei Jahre verdoppelt.*

n	**1984**	**1994**	**2004**
10^{50}	181 s	5,66 s	0,181 s
10^{70}	9,5 h	0,297 h	34,2 s
10^{100}	344 T	10.75 T	8,3 h
10^{120}	52,57 J	600 T	19,3 h
10^{140}	2.200 J	68,75 J	803 T
10^{200}	48 Mio J	1,5 Mio J	48.000 J
10^{280}	4,4 Bio J	140 Mrd J	4,4 Mrd J

*: inzwischen alle 18 Monate!

Informatik
Kryptographie und Kryptoanalyse

RSA

Ein Stärke des RSA-Verfahrens, nämlich dass kein Schlüsselaustausch erforderlich ist, ist gleichzeitig eine Schwäche! **Jeder** kann jetzt dem Schlüsselausgeber eine Nachricht verschlüsselt zusenden, dieser kann jedoch nicht nachprüfen, ob der Verfasser der Nachricht derjenige ist, den er vorzugeben scheint.

Dieses Problem zu Lösen ist Aufgabe von Verfahren der **Authentifizierung.** Das RSA-Verfahren ist dazu allerdings ebenfalls verwendbar: Man stellt als Sender ebenso einen eigenen Schlüssel her wie der Empfänger, verschlüsselt jedoch seine Nachricht mit seinem geheimen Schlüssel und veröffentlicht den anderen. Jetzt kann jeder entschlüsseln, aber nur einer konnte verschlüsseln.

Literatur

[1] Bauer, Friedrich L.: Decrypted Secrets : Methods and Maxims of Cryptology. 2nd, Rev. and Ext. Ed. Berlin : Springer, 2000. - ISBN 3-540-66871-3

[2] Creutzig, Christopher ; Buhl, Andreas ; Zimmermann, Philip: PGP Pretty Good Privacy : Der Briefumschlag für Ihre elektronische Post. 4. Aufl. Bielefeld : Art d'Ameublement, 1999. - ISBN 3-9802182-9-5

[3] Singh, Simon: Geheime Botschaften : Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. München : Hanser, 2000. - ISBN 3-446-19873-3

[4] Weber, Michael: Verteilte Systeme. Heidelberg : Spektrum, 1998. - ISBN 3-8274-0221-2