Programmierpraktikum
Thema: Kryptographie

Sommersemester 2004

Termine

Dienstag	14-16 Uhr c.t.	Raum 25.13-U1.32
		Raum 25.02-02.21 (ab 18. Mai)
Donnerstag	13-18 Uhr	Raum 25.12-02.39
		(Rechnerraum)
Feiertage:		20. Mai (Christi Himmelfahrt)
		10. Juni (Fronleichnam)
letzte Vorlesung:		6. Juli
Präsentationstermin:		23. Juli, 11-13 Uhr

Kontakt

Tobias Riege
Raum 25.12-02.26
Email: `riege@cs.uni-duesseldorf.de`

Webseite: http://www.cs.uni-duesseldorf.de/~riege/praktikum/
Mailingliste: `krypto@cs.uni-duesseldorf.de`

Definition Kryptosystem

Kryptosystem: Fünftupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ mit:

1. $\mathcal{P}$ Klartextraum. Hier : $\mathcal{P} = \{a, \ldots, z\}$ bzw. $\mathbb{Z}_{26}$.
2. $\mathcal{C}$ Chiffretextraum. Meist gilt $\mathcal{C} = \mathcal{P}$.
3. $\mathcal{K}$ Schlüsselraum.
4. $\mathcal{E}$ Verschlüsselungsfunktionen $E_k : \mathcal{P} \to \mathcal{C}$.
5. $\mathcal{D}$ Entschlüsselungsfunktionen $D_k : \mathcal{C} \to \mathcal{P}$.
6. $(\forall e \in \mathcal{K})\ (\exists d \in \mathcal{K})\ [\forall p \in \mathcal{P} : D_d(E_e(p)) = p]$.

Beispiel: Verschiebungschiffre (Caesar)

Klar- und Chiffretextraum	$v \in \mathbb{Z}_{26}$
Schlüsselraum	$k \in \mathbb{Z}_{26}$
Verschlüsselungsfunktion	$E_k(v) = v + k \mod 26$
Entschlüsselungsfunktion	$D_k(v) = v - k \mod 26$

Schlüssel	$k = 5$
Klartext	`kryptographie`
Chiffretext	`pwduytlwfumnj`

Blockchiffren

Blockchiffren sind Verschlüsselungsverfahren, in denen Blöcke fester in Blöcke derselben Länge kodiert werden.

- Klartextraum $\mathcal{P} = \Sigma^n$.
- Chiffretextraum $\mathcal{C} = \Sigma^n$.
- Verschlüsselungsfunktionen $E_k : \Sigma^n \to \Sigma^n$.
- Entschlüsselungsfunktionen $D_k : \Sigma^n \to \Sigma^n$.

Theorem: Die Verschlüsselungsfunktionen einer Blockchiffre sind Permutationen.

Der Schlüsselraum ist die Menge $S(\Sigma^n)$ aller Permutationen von Σ^n. Die Anzahl aller Schlüssel (Permutationen) beträgt

$$\boldsymbol{|\mathcal{K}| = (|\Sigma|^n)!}$$

Beispiel: $n = 4,\ |\Sigma| = 26$:

$$|\mathcal{K}| = (|\Sigma|^4)! = 456976! = \text{jede Menge!}$$

Nachteil: beliebige Permutation π benötigt viel Speicherplatz, nämlich eine Tabelle mit $|\Sigma|^n$ Werten.

Einschränkung des Schlüsselraums

Lösung: Effizientes Kodieren einer Teilmenge von allen möglichen Permutationen.

Beispiel 1: Affin lineare Blockchiffren

Klar- und Chiffretextraum	$v \in \mathbb{Z}_{26}^n$
Schlüsselraum	$k = (A, b)$, $A \in \mathbb{Z}_{26}^{(n \times n)}, b \in \mathbb{Z}_{26}^n$
Verschlüsselungsfunktion	$E_k(v) = A * v + b \mod 26$
Entschlüsselungsfunktion	$D_k(v) = A' * (v - b) \mod 26$

- $A' = (a' \text{ adj } A) \mod m$
- $a' =$ Inverses von $\det A \mod m$
- adj $A =$ *Adjunkte* von A:

$$\text{adj } A = ((-1)^{i+j} \det A_{j,i}).$$

- E bijektiv $\Longleftrightarrow \det A$ teilerfremd zu m

Beispiel 2: DES (Digital Encryption Standard)

Klar- und Chiffretextraum	$v \in \{0,1\}^{64}$
Schlüsselraum	$k \in \{0,1\}^{56}$
Größe Schlüsselraum	$2^{56} \approx 7.2 * 10^{16}$

Verschlüsselungsmodi für Blockchiffren - ECB

Suchen: Verschlüsselung für beliebig lange Klartexte.

Einfachste Lösung: Electronic Codebook Mode (ECB)

Vorgehensweise:

- Teile beliebig langen Klartext in Blöcke der Länge n auf
- Zu kurzer Klartext wird mit Füllwerten verlängert
- Verschlüssele jeden Block mit dem Schlüssel zur Blockchiffre der Länge n

Beispiel: Permutationschiffre der Länge 2:

Klartext	`ananasdiaet`
Aufteilen	`an`|`an`|`as`|`di`|`ae`|`tx`
Verschlüsseln	`na`|`na`|`sa`|`id`|`ea`|`xt`
Zusammenfügen	`nanasaideaxt`

Nachteile:

- Gleiche Klartextblöcke ergeben gleiche Chiffretextblöcke, d.h. Regelmäßigkeiten im Klartext bleiben erhalten
- Blöcke können ungemerkt eingefügt, gelöscht, verändert werden, da jeder einzelne Block unabhängig von den anderen übertragen wird

Verschlüsselungsmodi für Blockchiffren - CBC

Verbesserung: Chipherblock Chaining Mode (ECB)
über Blöcken der Form $\{0,1\}^n$

Vorteil: Jeder Block wird in Abhängigkeit von den Vorgängerblöcken verschlüsselt $\Rightarrow$ kontextabhängig!

Vorgehensweise:

- $m_1, \ldots, m_t$ Klartextblöcke der Länge n
- Schlüssel $k = (e, d)$ mit Verschlüsselungsfunktion E_e und Entschlüsselungsfunktion D_d
- Wähle Initialisierungsvektor $IV \in \{0,1\}^n$
- Setze

$$c_0 = IV, \quad c_j = E_e(c_{j-1} \oplus m_j), \quad 1 \leq j \leq t$$

- Erhalte Schlüsseltextblöcke $c_1, \ldots, c_t$
- Entschlüsselung

$$c_0 = IV, \quad m_j = c_{j-1} \oplus D_d(c_j), \quad 1 \leq j \leq t$$

- Erhalte Klartextblöcke $m_1, \ldots, m_t$

Beispiel - CBC

Klartext	$m_1 = 0010, m_2 = 1110, m_3 = 0010$
Schlüssel	Permutation $\pi = (4321)$
Initialisierungsvektor	$IV = 0110$

Verschlüsselung:

$c_0 = 0110$

$c_1 = E_\pi(c_0 \oplus m_1) = E_\pi(0100) = 0010$

$c_2 = E_\pi(c_1 \oplus m_2) = E_\pi(1100) = 0011$

$c_3 = E_\pi(c_2 \oplus m_3) = E_\pi(0001) = 1000$

Entschlüsselung:

$m_1 = c_0 \oplus E_\pi^{-1}(c_1) = 0110 \oplus 0100 = 0010$

$m_2 = c_1 \oplus E_\pi^{-1}(c_2) = 0010 \oplus 1100 = 1110$

$m_3 = c_2 \oplus E_\pi^{-1}(c_3) = 0011 \oplus 0001 = 0010$

Klartext	`001011100010`
Aufteilen	`0010 | 1110 | 0010`
Verschlüsseln	`0010 | 0011 | 1000`
Zusammenfügen	`001000111000`

Weitere Modi:

Cipher Feedback Mode (CFB)

Output Feedback Mode (OFB)

Kryptanalyse

Kerkhoffs Prinzip:

Die Sicherheit eines Verschlüsselungsverfahrens darf nur von der Geheimhaltung des Schlüssels abhängen, nicht jedoch von der Geheimhaltung des Algorithmus.

Szenarien für Angriffe auf Verschlüsselungen:

- **Ciphertext-Only: Angreifer kennt nur den Chiffretext**
- Known-Plaintext: Angreifer kennt zugehörige Klartexte
- Chosen-Plaintext: Angreifer kann beliebigen Klartext verschlüsseln (möglich bei public-key Verfahren)
- Adaptive-Chosen-Plaintext: wie Chosen-Plaintext, der Angreifer kennt jedoch schon den eigentlichen Chiffretext
- Chosen-Ciphertext: Angreifer kann beliebigen Chiffretext entschlüsseln (möglich bei Verschlüsselungsverfahren zur Identifikation)
- Adaptive-Chosen-Ciphertext: wie Chosen-Ciphertext, der Angreifer kennt jedoch schon den eigentlichen Chiffretext

Relevante Verfahren für das Praktikum

Wir werden versuchen, folgende Kryptoverfahren zu brechen:

- Caesar
- Substitution
- Vigenere
- RSA (kleine Version mit ca. 100-bit Modul)

Obere Schranke: Bei Ciphertext-Only Attacken einfachster Ansatz: Durchsuchen des gesamten Schlüsselraums bis korrekter Schlüssel gefunden ist.

Analyse: Für die oben genannten Verfahren:

Caesar	26
Substitution	$26! \approx 4.03 * 10^{26}$
Vigenere	26^n bei Blocklänge n
	308915776 bei $n = 6$
RSA	$\approx 4.23 * 10^{28}$ (100-bit Modul)
	$\approx 5.84 * 10^{305}$ (1024-bit Modul)
DES	$2^{56} \approx 7.21 * 10^{16}$

Effizienter: Ausnutzen bestimmter Eigenschaften der jeweiligen Kryptosysteme, um die Anzahl der möglichen Schlüssel zu reduzieren.

Eigenschaften der deutschen Sprache

Fakt: Jede Sprache hat eine charakteristische Verteilung ihrer Buchstaben. Dies kann man bei einigen Kryptosystemen ausnutzen, da die Häufigkeiten auf den Schlüsseltext übertragen werden (monoalphabetische Verfahren).

Beispiele:

- Caesar
- Substitution
- Vigenere (mit Einschränkung)

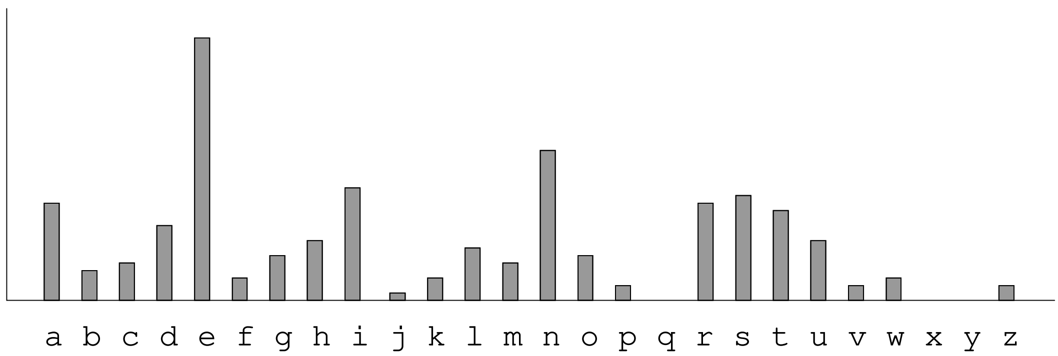

Abbildung 1: Häufigkeitsgebirge im Deutschen

Caesar: lediglich Verschiebung des Gebirges um 0-25 Stellen

Beispiel: Abgefangener Text

fna anrcnc bx byjnc mdalq wjlqc dwm frwm
nb rbc mna ejcna vrc bnrwnv trwm
na qjc mnw twjknw fxqu rw mnv jav
na ojbbc rqw brlqna na qjnuc rqw fjav

vnrw bxqw fjb krapbc md bx kjwp mnrw pnbrlqc
brnqbc ejcna md mnw nautxnwrp wrlqc
mnw naunwtxnwrp vrc taxw dwm blqfnro
vnrw bxqw nb rbc nrw wnknubcanro

md urnknb trwm txvv pnq vrc vra
pja blqxnwn byrnun byrnu rlq vrc mra
vjwlq kdwcn kudvnw brwm jw mnv bcajwm
vnrwn vdccna qjc vjwlq pdnumnw pnfjwm

vnrw ejcna vnrw ejcna dwm qxnanbc md wrlqc
fjb naunwtxnwrp vra unrbn enabyarlqc
bnr adqrp kunrkn adqrp vnrw trwm
rw mdnaanw kujnccnaw bjndbnuc mna frwm

fruubc onrwna twjkn md vrc vra pnqw
vnrwna cxnlqcna bxuunw mrlq fjacnw blqxnw
vnrwna cxnlqcna odnqanw mnw wjnlqcurlqnw anrqw
dwm frnpnw dwm cjwinw dwm brwpnw mrlq nrw

vnrw ejcna vnrw ejcna dwm brnqbc md wrlqc mxac
nautxnwrpb cxnlqcna jv mdnbcnaw xac
vnrw bxqw vnrw bxqw rlq bnq nb pnwjd
nb blqnrwnw mrn jucnw fnrmnw bx pajd

rlq urnkn mrlq vrlq anric mnrwn blqxnwn pnbcjuc
dwm krbc md wrlqc fruurp bx kajdlq rlq pnfjuc
vnrw ejcna vnrw ejcna sncic ojbbc na vrlq jw
nautxnwrp qjc vra nrw unrmb pncjw

mnv ejcna pajdbncb na anrcnc pnblqfrwm
na qjnuc rw mnw javnw mjb jnlqinwmn trwm
naanrlqc mnw qxo vrc vdnq dwm wxcq
rw bnrwnw javnw mjb trwm fja cxmc

Analyse

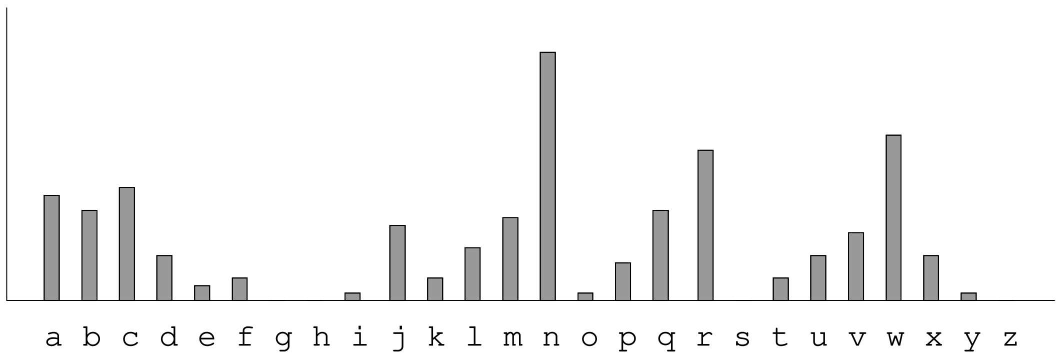

Abbildung 2: Häufigkeitsverteilung bei Chiffretext

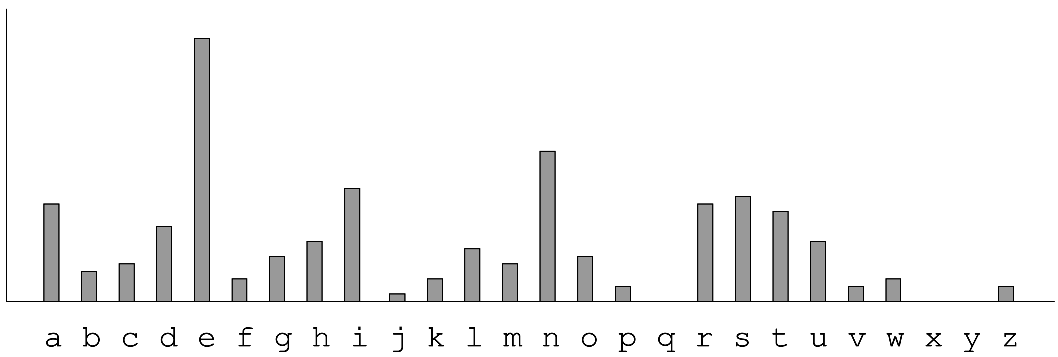

Abbildung 3: Häufigkeitsverteilung im Allgemeinen

Vermutung: Caesar-Verschiebung um neun Stellen:

$$E(v) = v + 9 \mod 26, \quad v \in \mathbb{Z}_{26}.$$

Wende entsprechende Entschlüsselungsfunktion an:

$$D(v) = v - 9 \mod 26, \quad v \in \mathbb{Z}_{26}.$$

Dechriffrierter Text

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
Meiner toechter sollen dich warten schoen
Meiner 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 grausets er reitet geschwind
Er haelt in den Armen das aechzende Kind
Erreicht den Hof mit mueh und Noth
In seinen Armen das Kind war todt

Der Erlkönig, Johann Wolfgang von Goethe, 1782

Anderer Ansatz

Alle 26 möglichen Schlüssel manuell ausprobieren.

Problem bei Substitution: Anzahl der Schlüssel: $26!$

Angriff per Exhaustive Search zwar immer noch möglich, aber mit Schwierigkeiten verbunden:

- Automatische Suche müßte erweitert werden
- Erkennung sinnvoller Klartexte per Algorithmus
- Datenbank mit sinnvollen Wörtern wäre nötig

Lösung: Betrachte Bi- und Trigramme.

Bigramm	**Häufigkeit**	**Bigramm**	**Häufigkeit**
en	3.88%	nd	1.99%
er	3.75%	ei	1.88%
ch	2.75%	ie	1.79%
te	2.26%	in	1.67%
de	2.00%	es	1.52%
Trigramm	**Häufigkeit**	**Trigramm**	**Häufigkeit**
ein	1.22%	der	0.86%
ich	1.11%	che	0.75%
nde	0.89%	end	0.75%
die	0.87%	gen	0.71%
und	0.87%	sch	0.66%

Tabelle 1: Häufigste Bi- und Trigramme im Deutschen

Beispiel Substitution

xzh rvi zlhv xvavgqvsehvi esbx rcbx vsgqzl pvjdvjvdvg mgr gmg ecllvg evsgv jvsehvi zmbx gzbx qvsgvq psllvg lvdvg evsgv pcih mgr pviyv qviyh sbx mgr rvg dizmbx mgr qsh jvsehveehzviyv hm sbx pmgrvi zmbx pzllv pzllv qzgbxv ehivbyv rzee omq opvbyv pzeevi tlsveev mgr qsh ivsbxvq fcllvq ebxpzllv om rvq dzrv esbx vijsveev mgr gmg ycqq rm zlhvi dvevg gsqq rsv ebxlvbxhvg lmqwvgxmvllvg dseh ebxcg lzgjv ygvbxh jvpvevg gmg vitmvllv qvsgvg psllvg zmt opvs dvsgvg ehvxv cdvg evs vsg ycwt vslv gmg mgr jvxv qsh rvq pzeevihcwt pzllv pzllv qzgbxv ehivbyv rzee omq opvbyv pzeevi tlsveev mgr qsh ivsbxvq fcllvq ebxpzllv om rvq dzrv esbx vijsveev evxh vi lzvmth omq mtvi gsvrvi pzxilsbx seh ebxcg zg rvq tlmeev mgr qsh dlshoveebxgvllv psvrvi seh vi xsvi qsh izebxvq jmeev ebxcg omq opvshvg qzlv psv rze dvbyvg ebxpsllh psv esbx uvrv ebxzlv fcll qsh pzeevi tmvllh ehvxv ehvxv rvgg psi xzdvg rvsgvi jzdvg fclljvqveevg zbx sbx qviy ve pvxv pvxv xzd sbx rcbx rze pcih fvijveevg zbx rze pcih pcizmt zq vgrv vi rze psir pze vi jvpvevg zbx vi lzvmth mgr disgjh dvxvgrv pzvieh rm rcbx rvi zlhv dvevg sqqvi gvmv jmveev disgjh vi ebxgvll xvivsg zbx mgr xmgrvih tlmveev ehmviovg zmt qsbx vsg gvsg gsbxh lzvgjvi yzgg sbxe lzeevg psll sxg tzeevg rze seh hmvbyv zbx gmg psir qsi sqqvi dzvgjvi pvlbxv qsvgv pvlbxv dlsbyv c rm zmejvdmih rvi xcvllv ecll rze jzgov xzme viezmtvg evx sbx mvdvi uvrv ebxpvllv rcbx ebxcg pzeeviehicvqv lzmtvg vsg fviimbxhvi dvevg rvi gsbxh xcvivg psll ehcby rvi rm jvpvevg ehvx rcbx psvrvi ehsll pslleh zq vgrv jzi gsbxh lzeevg psll rsbx tzeevg psll rsbx xzlhvg mgr rze zlhv xclo dvxvgrv qsh rvq ebxzitvg dvslv ewzlhvg evxh rz ycqqh vi ebxlvwwvgr psvrvi psv sbx qsbx gmi zmt rsbx pvitv jlvsbx c ycdclr lsvjeh rm gsvrvi yizbxvgr histth rsv jlzhhv ebxzvitv pzxilsbx dizf jvhicttvg evxh vi seh vghopvs mgr gmg yzgg sbx xcttvg mgr sbx zhqv tivs pvxv pvxv dvsrv hvslv ehvxg sg vslv ebxcg zle ygvbxhv fcvllsj tvihsj sg rsv xcvxv xvlth qsi zbx sxi xcxvg qzvbxhv mgr esv lzmtvg gzee mgr gzveevi psire sq ezzl mgr zmt rvg ehmtvg pvlbx vghevholsbxve jvpzveevi xvii mgr qvsehvi xcvi qsbx imtvg zbx rz ycqqh rvi qvsehvi xvii rsv gch seh jicee rsv sbx isvt rsv jvsehvi pvir sbx gmg gsbxh lce sg rsv vbyv dvevg dvevg evsre jvpvevg rvgg zle jvsehvi imth vmbx gmi om evsgvq opvbyv vieh xvifci rvi zlhv qvsehvi

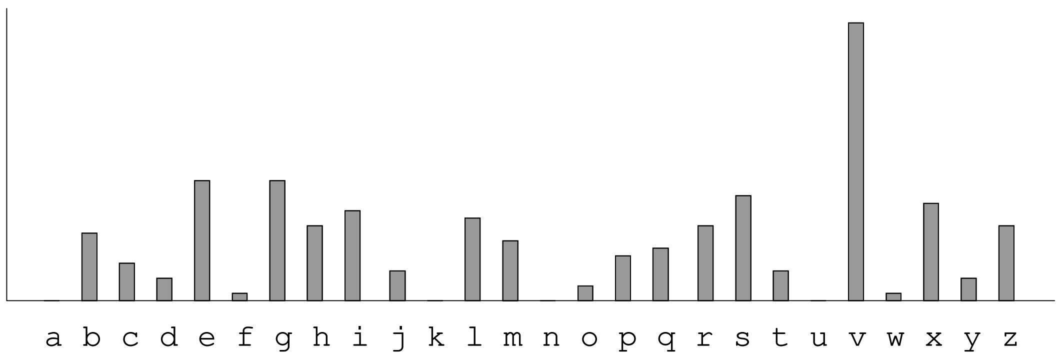

Abbildung 4: Häufigkeitsgebirge für Chiffretext

Fortsetzung(1) Kryptanalyse

Annahme: `v = E`

Bigramm	Häufigkeit	Bigramm	Häufigkeit
bx	5.14%	rE	2.23%
Ei	4.66%	sb	2.16%
Eg	3.99%	eh	2.09%
eE	2.70%	ll	1.96%
Es	2.36%	hE	1.82%
Trigramm	**Häufigkeit**	**Trigramm**	**Häufigkeit**
sbx	2.88%	eEg	1.39%
eeE	1.95%	rEi	1.30%
mgr	1.86%	seh	1.30%
ebx	1.58%	Esg	1.21%
llE	1.49%	ehE	1.21%

Tabelle 2: Häufigste Bi- und Trigramme im Chiffretext

Annahme: Entweder `eEg = DER` oder `rEi = DER`
$\Rightarrow$ `r = D` und `i = R`

Häufiges Bigramm mit eher seltenen Buchstaben: `ch`
$\Rightarrow$ `bx = CH` und auch `sCH = ICH`, `eCH = SCH`

Bigramm	Häufigkeit	Bigramm	Häufigkeit
CH	5.14%	DE	2.23%
ER	4.66%	IC	2.16%
Eg	3.99%	Sh	2.09%
SE	2.70%	ll	1.96%
EI	2.36%	hE	1.82%

Tabelle 3: Weitere Auflösung der Bigramme im Chiffretext

Fortsetzung(2) Kryptanalyse

`Hzh DER zlhE HEaEgqEIShER SICH DcCH`
`EIgqzl pEjdEjEdEg mgD gmg ScllEg SEIgE...`

Annahme: `c = O`

Bisher entschlüsselt:
`abcdefghijklmnopqrstuvwxyz`
`?CO?S???R????????DI??E?H??`

Gruppe	Gesamthäufigkeit dieser Buchstaben
E,N	27.18%
I, S, R,A,T	34.48%
C, O, D, H,U,L,G,M,B,W,F,K,Z	36.52%
P,V,J,Y,X,Q	1.82%

Tabelle 4: Buchtstabengruppen

Noch unentschlüsseltes Bigramm: `Eg` (3.99%)

Annahme: `g = N`

`...mND NmN SOllEN SEINE jEIShER zmCH NzCH...`

Folgerung: `m = U`, `z = A` und `l = L`

Drei-Buchstabenwort: `ISh` $\Rightarrow$ `h = T`

Fortsetzung(3) Kryptanalyse

Bisher entschlüsselt:
abcdefghijklmnopqrstuvwxyz
?CO?S?NTR??LU????DI??E?H?A

Betrachte wieder den teilweise entschlüsselten Chiffretext:
HAT DER ALTE HEaENqEISTER SICH DOCH
EINqAL pEjdEjEdEN UND NUN SOLLEN SEINE
jEISTER AUCH NACH qEINEq pILLEN LEdEN...

Hinweis: Die restlichen Buchstaben ergeben sich meist rein aus dem Kontext.

Beispiel: a = X, q = M, j = G, p = W, d = B

Weitere Auflösung:

STRECyE	$\Rightarrow$	y = K
oUM	$\Rightarrow$	o = Z
tLIESSE	$\Rightarrow$	t = F
fOLLEM	$\Rightarrow$	f = V
KOwF	$\Rightarrow$	w = P
uEDE	$\Rightarrow$	u = J

k und n nicht im Chiffretext enthalten (Klartext: Q und Y).

Auflösung:
abcdefghijklmnopqrstuvwxyz
XCOBSVNTRG?LU?ZWMDIFJEPHKA

Entschlüsselter Text

Auflösung: Nach Formatierung mit Zeilenumbruch ergibt sich folgender Klartext.

Hat der alte Hexenmeister
Sich doch einmal wegbegeben
Und nun sollen seine Geister
Auch nach meinem Willen leben
Seine Wort und Werke
Merkt ich und den Brauch
Und mit Geistesstaerke
Tu ich Wunder auch

Walle walle
Manche Strecke
Dass zum Zwecke
Wasser fliesse
Und mit reichem vollem Schwalle
Zu dem Bade sich ergiesse

Und nun komm du alter Besen
Nimm die schlechten Lumpenhuellen
Bist schon lange Knecht gewesen
Nun erfuelle meinen Willen
Auf zwei Beinen stehe
Oben sei ein Kopf
Eile nun und gehe
Mit dem Wassertopf

Walle walle
Manche Strecke
Dass zum Zwecke
Wasser fliesse
Und mit reichem vollem Schwalle
Zu dem Bade sich ergiesse

...

Der Zauberlehrling, Johann Wolfgang von Goethe, 1797

XML für Challenges

Umsetzung in Java: Statt normal verschlüsselten Nachrichten wollen wir auch "Challenges" an die Kommunikationspartner schicken können.

Eigenschaften:

- Nur 26 Zeichen (a-z) werden verschlüsselt
- Satzzeichen (".", ",", "?"), Zeilenumbruch und Leerzeichen werden nicht verschlüsselt, jedoch unkodiert im Chiffretext übermittelt
- Großbuchstaben und Sonderzeichen sind nicht erlaubt
- Chiffrierverfahren wird mitgeteilt
- Je nach Verfahren werden verschiedene Varianten der Kryptanalyse angewandt

XML-Format für Challenges:

```
<challenge>
<id>0</id>
<from>1</from>
<to>3</to>
<text>ejft jtu fjo uftu</text>
<cryptomethod>Caesar</cryptomethod>
<clearlength>0</clearlength>
</challenge>
```