Di., 23.10.2012 Informatik Q2 M (Kr)

Polyalphabetische Vigenère-Ver-/Entschlüssung Name: ____www.r-krell.de___

1 Vigenère von Hand:

a) Verschlüssele von Hand mit dem Schlüsselwort „HUND“ die folgenden (Klar-)Texte:
a1) „Das ist einfach“
a2) „Juhu ich kanns“
wobei die Leerstellen in den Geheimtext übernommen werden sollen, jede Leerstelle aber einen Buchstaben des Schlüsselworts verbraucht.

b) Entschlüssele mit dem Schlüsselwort „ROT“ den Geheimtext
„Asmqh bztgdm sl pxjgxi.“

Vigenère-Quadrat

	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	C	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

2 Kennt ein Angreifer nur den Geheimtext - z.B. „Fqgfz btefqgf, eil qlu gjkau yfqgf. Bjxs xjvxs nol fqgf, vvw ltov btefqgf...“, aber das Schlüsselwort nicht, muss er zunächst dessen Länge erraten:

a) Kasiski-I (1863; ähnlich wohl auch Babbage 1854): Es wird nach mehrfach auftretenden Zeichenkombinationen aus 3 oder besser noch mehr Zeichen im Geheimtext gesucht, z.B.

```
Fqgfz btefqgf, eil qlu gjkau yfqgf. Bjxs xjvxs nol fqgf, vvw ltov btefqgf...
 123456789 123456789 123456789 123456789 123456789 123456789 123456789 12.
```

Ermittle die Abstände gleichartiger Gruppen und versuche, einen gemeinsamen kleinen Teiler zu finden! Was wird hinter dem Auftreten solcher Gruppen vermutet?

b) Kasiski-II (Autokorrelation). Man schreibt den Geheimtext im Original und den Geheimtext jeweils um 1, 2, 3, 4,.. Zeichen verschoben übereinander, zunächst mit der Verschiebung 1:

```
Fqgfz btefqgf, eil qlu gjkau yfqgf. Bjxs xjvxs nol fqgf, vvw ltov btefqgf...
.Fqgfz btefqgf, eil qlu gjkau yfqgf. Bjxs xjvxs nol fqgf, vvw ltov btefqgf..
```

Hier stehen einmal gleiche Buchstaben übereinander. Versuch mit einer Verschiebung um 2:

```
Fqgfz btefqgf, eil qlu gjkau yfqgf. Bjxs xjvxs nol fqgf, vvw ltov btefqgf...
..Fqgfz btefqgf, eil qlu gjkau yfqgf. Bjxs xjvxs nol fqgf, vvw ltov btefqgf.
```

Es gibt keine Übereinstimmung. Nächster Versuch mit der Verschiebung um 3 Zeichen:

```
Fqgfz btefqgf, eil qlu gjkau yfqgf. Bjxs xjvxs nol fqgf, vvw ltov btefqgf...
...Fqgfz btefqgf, eil qlu gjkau yfqgf. Bjxs xjvxs nol fqgf, vvw ltov btefqgf
```

Gefunden wurden 8 Übereinstimmungen. Nächster Versuch mit der Verschiebung um 4:

```
Fqgfz btefqgf, eil qlu gjkau yfqgf. Bjxs xjvxs nol fqgf, vvw ltov btefqgf...
f...Fqgfz btefqgf, eil qlu gjkau yfqgf. Bjxs xjvxs nol fqgf, vvw ltov btefqg
```

Es gibt nur 1 Koinzidenz. Beträgt die Verschiebung ein Vielfaches der Schlüssellänge, wird eine höhere Zahl an Übereinstimmungen erwartet: Häufige Klartextbuchstaben (etwa das ‚e‘) treffen auf gleiche Schlüsselbuchstaben und werden gleich verschlüsselt, stehen also eher gleich übereinander. Welche Schlüssellänge wäre hier zu vermuten?

c) Friedman-Formel (1920 oder 1925): Hier werden die Länge n des Geheimtextes und die absolute Häufigkeit n_i für jeden der 26 Buchstaben des Alphabets ermittelt (i=1..26; n_2 ist also die Anzahl der ‚b‘s, n_5 die Zahl der ‚e‘s, usw.). Daraus wird nach der Formel

$\kappa = \frac{\sum_{i=1}^{26} n_i \cdot (n_i - 1)}{n \cdot (n-1)} \approx \frac{\sum_{i=1}^{26} n_i^2}{n^2}$ die Kennzahl κ (kappa) ermittelt. Bei einem langen, normalem deutschen Klartext ist κ = 0,0762 = 7,62 %, während bei einem Text, der nur aus gleichen Buchstaben besteht (z.B. beim Text „mmmmmm"), κ bei 1 (=100%) liegen kann. Bei einem langen Zufalls-‚Text' mit Gleichverteilung aller Buchstaben hat κ mit $\kappa_{min} = \frac{1}{26} = 0{,}0385 =$ 3,85 % den kleinstmöglichen Wert. Je länger und zufälliger das Schlüsselwort bei der Vigenère-Verschlüsselung ist, desto mehr nähert sich das aus dem Geheimtext ermittelte κ dem Minimum. Ein größeres κ lässt hingegen auf ein kurzes, regelmäßig wiederholtes Schlüsselwort schließen. Laut Friedman kann die Länge x des Schlüsselworts bei verschlüsseltem deutschen Klartext durch $x \approx \frac{0{,}0377 \cdot n}{\kappa \cdot (n-1) - 0{,}0385 \cdot n + 0{,}0762} \leq \frac{0{,}0377}{\kappa - 0{,}0385}$ abgeschätzt werden, wobei sich die 0,0377 aus 0,0762-0,0385 ergibt. Das κ wird wie oben aus dem Geheimtext ermittelt (die Formel gilt umso besser, je länger die Nachricht ist, weil sie dann eher normalem deutschen Text entspricht. Außerdem ist bei großem n der Unterschied zwischen $n \cdot (n-1)$ und n^2 geringer und die einfachere Näherung kann eher verwendet werden).

Im Geheimtext „Fqgfz btefqgf, eil qlu gjkau yfqgf. Bjxs xjvxs nol fqgf, vvw ltov btefqgf..." kommen die 6 Buchstaben c, d, h, m, p, r gar nicht (0-mal), die 7 Buchstaben a, i, k, n, w, y, z je 1-mal, die Zeichen o, s, u je 2-mal, die 5 Buchstaben b, e, j, t, x je 3-mal, die beiden Buchstaben l und v je 4-mal, g und q je 6-mal und das f sogar 10-mal vor. Insgesamt enthält der Text also n=58 echte Buchstaben (ohne Leer- und Satzzeichen). Berechne damit das κ des Geheimtextes und schätze die Länge x des Schlüsselworts ab! (Wegen des recht kurzen Textes ist dem Ergebnis hier nicht unbedingt zu trauen)

3 Gibt es aus dem Kasiski- und/oder Friedman-Test eine Vermutung über die Länge des Schlüsselwortes (hier 3), so müssen jetzt drei Teiltexte gebildet werden. Jeder Teiltext ist mono-alphabetisch nach Cäsar nur durch eine Alphabet-Verschiebung verschlüsselt. Kann ein ausreichend langer, normaler Klartext vorausgesetzt werden (hier nicht sicher!), sollte das häufigste Geheimtextzeichen von jedem Teil das e chiffrieren und die Verschiebung erkennen lassen. Ermittle jeweils die häufigsten Zeichen, vermute den zur Verschiebung passenden Schlüsselbuchstaben und entschlüssele den gesamten Geheimtext schließlich mit dem gefundenen Schlüsselwort!

```
Fqgfz btefqgf, eil qlu gjkau yfqgf. Bjxs xjvxs nol fqgf, vvw ltov btefqgf....
F  f  b  f  f  e     u  j  u  f  f  B  s  j  s  o  f  f  v     o  b  f  f...
 q  z  t  q  ,  i  q     k     q  .  j     v     l  q  ,  v  l  v  t  q  ...
  g     e  g     l  l  g  a  y  g     x  x  x  n     g     w  t     e  g ...
```

(Wenn es nicht klappt: in der mittleren Zeile ist bei meinem zu kurzen Text zufällig kein ‚e' verschlüsselt. Sonst wäre m häufiger als q oder v. Auch in der letzten Zeile sollte man evtl. dem normalerweise zweit- oder dritthäufigsten Buchstaben eine Chance geben...)

Als Hilfe werden die relativen Buchstabenhäufigkeiten n_i/n (in %) für typischen deutschen (Klar-)Text gegeben, wie sie z.B. auf http://de.wikipedia.org/wiki/Häufigkeitsanalyse grafisch dargestellt sind (aus Copyright-Gründen hier in der Internetfassung nicht abgedruckt): In normalem deutschen Text sind am häufigsten: das e, dann n und i, gefolgt von r, t, s und a.