PD Dr. Martin Kreuzer
Fakultät für Mathematik
Universität Regensburg

Regensburg, den 8.5.2000

Übungen zur Vorlesung "Kryptographie"

Blatt 1

Aufgabe 1. Vgl. die am 4.5.2000 ausgeteilten Zettel.

Aufgabe 2. Von der nachstehenden, in Geheimschrift übermittelten Nachricht sind die letzten 10 Zahlen verlorengegangen. Wie lauten sie? Welches kryptographische System wurde benutzt?

10, 4, 13, 13, 12, 4, 8, 20, 1, 16, 14, 15, 12, 20, 7, 12, 2, 12, 20, 4, 12, 15, 17, 4, 19, 1, 8, 20, 1, 19, 8, 20, 18, 2, 4, 19, 2, 14, 2, 15, 4, 14, 12, 15, 6, 16, 13, 2, 15, 1, 5, 8, 13, 10, 4, 8, 4, 13, 12, 4, 14, 4, 18, 2, 12, 1, 4, 15, 12, 1, 8, 19, 1, 12, 4, 14, 18, 2, 12, 12, 17, 20, 16, 19, 2, 14, 13, 12, 15, 10, 2, 4, 6, 8, 13, 1, 4, 8, 15, 16, 20, 1, 19, 4, 10, 4, 13, 13, 12, 4

Aufgabe 3. a) Schreiben Sie ein *CoCoA* Programm `Kasiski(...)`, das als Eingabe eine Zeichenkette ("String") erwartet und als Ausgabe eine Liste von Zahlen errechnet, die aus den Distanzen mindestens zweimal vorkommender Zeichenketten der Länge ≥ 3 besteht. Die Distanz sei hierbei definiert als die Differenz der Nummern der Anfangsbuchstaben.

b) Schreiben Sie ein weiteres *CoCoA* Programm `Divisors(...)`, das die soeben berechnete Liste nimmt und eine Liste von Kandidaten für die Schlüssellänge beim Kasiski-Test bestimmt. Erklären Sie, wie Sie den Fall von "Ausreißern" handhaben.

c) Wenden Sie die beiden Programme auf den Text in Aufgabe 5 an.

Aufgabe 4. a) Schreiben Sie ein *CoCoA* Programm `Friedmann(...)`, das als Eingabe eine Zeichenkette erwartet und als Ausgabe den Friedmannschen Koinzidenzindex dieser Zeichenkette berechnet.

b) Schreiben Sie ein weiteres *CoCoA* Programm `KeyLength(...)`, das das Programm `Friedmann(...)` als Unterprogramm verwendet und einen Näherungswert für die Schlüsselwortlänge eines Vigenère-verschlüsselten Textes bestimt.

c) Wenden Sie die beiden Programme auf den Text in Aufgabe 5 an.

Aufgabe 5. Entschlüsseln Sie den folgenden Geheimtext, von dem bekannt sei, daß er mit dem Vigenère-Kryptosystem aus einem deutschen Klartext gewonnen wurde. Finden Sie auch das Schlüsselwort.

(bitte wenden)

$UEQPF$	$VCKAH$	$VNRZU$	$RNLAO$	$KIRVG$
$JTDVR$	$VRICV$	$IDLMY$	$IYSBC$	$COJQS$
$ZNYMB$	$VDLOK$	$FSLMW$	$EFRZA$	$VIQMF$
$JTDIH$	$CIFPS$	$EBXMF$	$FTDMH$	$ZGNMW$
$KAXAU$	$VUHJH$	$NUULS$	$VSJIP$	$JCKTI$
$VSVMZ$	$JENZS$	$KAHZS$	$UIHQV$	$IBXMF$
$FIPLC$	$XEQXO$	$CAVBV$	$RTWMB$	$LNGNI$
$VRLPF$	$VTDMH$	$ZGNMW$	$KRXVR$	$QEKVR$
$LKDBS$	$EIPUC$	$EAWJS$	$BAPMB$	$VSZCF$
$UEGIT$	$LEUOS$	$JOUOH$	$UAVAG$	$ZEZIS$
$YRHVR$	$ZHUMF$	$RREMW$	$KULKV$	$KGHAH$
$FEUBK$	$LRGMB$	$JIHLI$	$IFWMB$	$ZHUMP$
$LEUWG$	$RBHZO$	$LCKCW$	$THWDS$	$ILDAG$
$VNEMJ$	$FRVQS$	$VIQMU$	$VSWMZ$	$CTHII$
$WGDJS$	$XEOWS$	$JTKIH$	KEQ	