Prof. Dr. M. Kreuzer
P. Ackermann

Abgabe: 25.04.2005, 10h

Kryptografie
Übungsblatt 2

Aufgabe 4:

a) Schreiben Sie ein Programm `Friedman(...)`, das als Eingabe eine Zeichenkette erwartet und als Ausgabe den Friedmanschen Koinzidenzindex dieser Zeichenkette berechnet.

b) Schreiben Sie ein Programm `KeyLength(...)`, das das Programm `Friedman(...)` als Unterprogramm verwendet und einen Näherungswert für die Schlüsselwortlänge eines Vigenère-verschlüsselten Textes bestimmt.

c) Wenden Sie die beiden Programme auf den Text in `Aufgabe3.txt` an.

Aufgabe 5:
Finden Sie das Schlüsselwort und entschlüsseln Sie den Geheimtext aus `Aufgabe3.txt`.

Aufgabe 6:
Von einem Geheimtext konnten vier Blöcke zu je 32 Zeichen mitgehört werden:

SSNK LHON IWMM EUNT AHUL INNA HNCI NFCI
ERON ACBA MZGH NKTH WCDE SINK CAIE ANIM
DUAA UZSD INNE GNWS ROIL ELEE HUJR MEGI
TAMK ANAN SIEA IURS ETTB FUSI CFFH ETEE

a) Versuchen Sie mit Hilfe einer Frequenzanalyse, die Sprache des Klartextes und das verwendete Kryptosystem herauszufinden.

b) Entschlüsseln Sie den Text. Sie können dazu die Datei `Aufgabe6.txt` verwenden.

c) Wie lauten die fehlenden 18 Zeichen des Klartextes?

Aufgabe 7:
Gegeben sei ein linearer Kongruenzgenerator $f : \mathbb{Z}/2^{32}\mathbb{Z} \longrightarrow \mathbb{Z}/2^{32}\mathbb{Z}$. Drei aufeinanderfolgende Werte seien $x_0 = 1394449523$, $x_1 = 3456347474$ und $x_2 = 1689033221$.

a) Wie lauten die nächsten beiden Glieder x_3 und x_4?

b) Berechnen Sie x_{10^n} für $n = 1, 2, \ldots, 10$.

Aufgabe 8:

a) Verschlüsseln Sie

Mailand oder Madrid, Hauptsache Italien

mit Hilfe des Vernam-Kryptosystems. Erzeugen Sie den Schlüssel durch die Kongruenzabbildung $f : \mathbb{Z}/2^{40}\mathbb{Z} \longrightarrow \mathbb{Z}/2^{40}\mathbb{Z}$, $f(x) = \overline{31459265}x + \overline{2718281}$, mit Samen 123456, wobei Sie die Pseudozufallszahlen folgendermaßen erhalten: Liefert der Kongruenzgenerator die Zahl $a_n a_{n-1} \cdots a_1$, so sei die resultierende Pseudozufallszahl $a_{11} a_{10} \cdots a_4$.

b) Entschlüsseln Sie die mit dem Kryptosystem in a) mit selbem Kongruenzgenerator und Samen 654321 verschlüsselte Nachricht

045825060908039412426 43.