PD Dr. Martin Kreuzer
Fakultät für Mathematik
Universität Regensburg

Regensburg, den 16.5.2000

Übungen zur Vorlesung "Kryptographie"

Blatt 2

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 hareauszufinden.

b) Entschlüsseln Sie den Text. (Tip: Beachten Sie die beigefügte Datei Aufgabe6.txt.)

c) Wie lauten die fehlenden 18 Zeichen den Klartextes? (Tip: Die Initialen des Verfassers sind H.B.)

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. Implementieren Sie in *CoCoA* einen linearen Kongruenzgenerator $f : \mathbb{Z}/2^{40}\mathbb{Z} \longrightarrow \mathbb{Z}/2^{40}\mathbb{Z}$ und ein daraus abgeleitetes Vigenère Kryptosystem mit pseudozufälligem Schlüssel wie folgt.

a) Schreiben Sie eine *CoCoA* Funktion `IniLinKong(...)`, die eine ganze Zahl als Argument erwartet und den kanonischen Repräsentanten ihrer Restklasse in $\mathbb{Z}/2^{40}\mathbb{Z}$ in einer globalen Variablen `MEMORY.Samen` abspeichert.

b) Schreiben Sie eine *CoCoA* Funktion `LinKong(...)`, die die Funktion $f(x) = \overline{a}x + \overline{b}$ mit $a = 31459265$ und $b = 2718281$ auf den augenblicklichen Samen anwendet, das Ergebnis wieder in `MEMORY.Samen` abspeichert, und die ersten 32 Binärstellen des Ergebnisses als ganze Zahl ausgibt.

c) Schreiben Sie eine *CoCoA* Funktion `NextLinKong(...)`, die eine Zahl $1 \leq n \leq 2^{32}$ als Argument erwartet und eine mit f erzeugte Zufallszahl aus der Menge $\{0, \ldots, n-1\}$ ausgibt.

d) Schreiben Sie eine *CoCoA* Funktion `LinKongEncrypt(...)`, die eine ganze Zahl als Schlüssel ("key") sowie eine Zeichenkette ("string") als Argument erwartet. Die

Zeichenkette soll dann mit dem Vigenère Kryptosystem chiffriert werden, wobei das Schlüsselwort durch wiederholte Anwendung von `NextLinKong(26)` gewonnen werde. Der Samen sei der "key". Der Geheimtext soll als Ergebnis ausgegeben werden.

Aufgabe 9. Gegeben sei ein lineares Schieberegister mit n Speicherzellen.

a) Finden Sie eine $n \times n$-Matrix $\mathcal{A}$, so daß der Zustand des Schieberegisters nach i Takten gegeben ist durch $t_i = t_0 \mathcal{A}^i = t_{i-1}\mathcal{A}$, wenn man mit $t_0 = (1, 0, \ldots, 0)$ beginnt.

b) Beweisen Sie, daß die maximale Periode des Schieberegisters $2^n - 1$ beträgt.

Aufgabe 10. Von dem für die Chiffrierung der Geheimnachricht

$$BGVJFMBIHTXUFSDYVLMTJYHNS$$

verwendeten Kryptosystem sei folgendes bekannt:

1) Es wurde ein Vigenère Kryptosystem mit pseudozufälligem Schlüssel verwendet.

2) Der Schlüssel wurde mit einem linearen Schieberegister der Breite 4 erzeugt, dessen Zellen Elemente von $\mathbb{Z}/26\mathbb{Z}$ enthalten.

3) Als wahrscheinliches Wort des Klartextes kommt "broadcast" in Frage.

a) Entschlüsseln Sie die Botschaft!

b) Verschlüsseln Sie den Rest des Textes "announced the Allied invasion to be expected within fortyeight hours" (eventuell mit Hilfe von *CoCoA*).

c) Bestimmen Sie die Periode des Schieberegisters mit Hilfe von *CoCoA*.

Aufgabe 11. Es werde die Version des erweiterten Euklidischen Algorithmus vorausgesetzt, die in Satz 3.4 vorgestellt wurde.

a) Beweisen Sie Satz 3.4, d.h. die Endlichkeit und Korrektheit des angegebenen Algorithmus.

b) Implementieren Sie diesen Algorithmus in einer *CoCoA* Funktion `ExtEuklid(...)`.

c) Bestimmen Sie experimentell einen Näherungswert für die Wahrscheinlichkeit dafür, daß zwei Zufallszahlen teilerfremd sind. (Tip: Verwenden Sie die eingebaute *CoCoA* Funktion `Rand(...)`.)