Übung 4

Abgabe: 15.11.2018 **bis** 12:15 Uhr

1. Periode eines LFSRs 30 Punkte

Es gibt drei verschiedene Typen von LFSRs:

- LFSRs, die eine Sequenz mit maximaler Länge erzeugen. Diesen LFSRs liegen *primitive Polynome* zu Grunde.
- LFSRs, die keine Sequenz maximaler Länge erzeugen, aber bei denen die Länge unabhängig von dem Initialisierungsvektor ist. Diesen LFSRs liegen *irreduzible Polynome* zu Grunde, die allerdings nicht primitiv sind.
  Bemerkung: Alle primitiven Polynome sind irreduzibel.
- LFSRs, die keine Sequenz maximaler Länge erzeugen und bei denen die Sequenzlänge vom Initialisierungsvektor abhängt. Diesen LFSRs liegen *reduzible Polynome* zu Grunde.

Auch wenn Sie vermutlich noch nicht wissen, was ein primitives oder irreduzibles Polynom ist, können Sie anhand der obigen Aussage das Polynom eines LFSRs einem der drei Fälle zuordnen. Gehen Sie dabei wie folgend vor:

i. Zeichnen Sie das Schaltbild des Schieberegisters.

ii. Berechnen Sie *alle* Sequenzen die durch die Polynome erzeugt werden, und geben Sie die inneren Zustände des LFSRs an. Stellen Sie den inneren Zustand tabellarisch dar. Ggf. müssen Sie verschiedene Initialisierungsvektoren benutzen um alle Sequenzen zu erzeugen.

iii. Ordnen Sie das Polynom dem passenden Typen zu.

Bemerkung: Die Ausgabe des LFSRs muss *nicht* angegeben werden.

a) $x^5 + x^4 + x^2 + x + 1$ (10 Pkt.)

b) $x^5 + x + 1$ (10 Pkt.)

c) $x^5 + x^3 + x^2 + x + 1$ (10 Pkt.)

2. Praktische Anwendung einer Stromchiffre 10 Punkte

Eine wichtige Voraussetzung für sichere Stromchiffren ist, dass diese eine möglichst lange Periode erzeugen. In dieser Aufgabe betrachten wir Periodenlängen für eine Anwendung in praktischen Systemen.
Stellen wir uns folgendes Szenario vor: Wir wollen eine Netzwerkverbindung verschlüsseln, die Teil eines ATM (Asynchronous Transfer Mode) Netzwerkes ist. Die Daten werden mit einer der standardisierten ATM Geschwindigkeiten übertragen, d.h. mit 155 Mbits/sec. (Anmerkung: 1 Mbit = 2^{20} bit). Als Verschlüsselungsalgorithmus wurde eine Stromchiffre gewählt, die auf LFSRs basiert. Was ist der minimale Grad der Stromchiffre, wenn sich die Schlüsselfolge frühestens nach 12 Stunden wiederholen soll?

3. Angriff auf eine LFSR-Stromchiffre 60 Punkte

Wir wollen in dieser Übung eine Attacke gegen eine unsichere Stromchiffre durchführen, der ein einzelnes LFSR zugrunde liegt. Über das System sind folgende Fakten bekannt:

- Es werden 8-Bit-ASCII-codierte Zeichen verschlüsselt.
- Der Grad des LFSR ist $m = 8$
- Die Nachricht beginnt mit den Buchstaben `Mo`.

Wir haben die folgende verschlüsselte Nachricht abgehört (hexadezimale Codierung):
`EC D4 13 10 75 60 05 7C 50 DB 73`

a) Was ist die maximale Periodenlänge, die ein LFSR vom Grad $m = 8$ erzeugen kann? (5 Pkt.)

b) Wie viel Bits des Schlüsselstroms s muss man kennen, damit man die Rückkopplungskoeffizienten des LFSRs berechnen kann? (5 Pkt.)

c) Rekonstruieren Sie einen Teil des Schlüsselstroms aus den Ihnen bekannten Informationen. (10 Pkt.)

d) Bestimmen Sie die Rückkopplungskoeffizienten des LFSRs. (20 Pkt.)
Hinweis: Die inverse Matrix kann z.B. mit Wolframalpha berechnet werden. Falls Sie Tools verwenden, geben Sie diese bitte an.
https://www.wolframalpha.com/examples/Matrices.html

e) Generieren Sie die zur Entschlüsselung notwendige Sequenz und berechnen Sie den gesamten Klartext. (15 Pkt.)
Bemerkung: Falls Sie die Sequenz nicht von Hand generieren möchten, können Sie dazu auch ein Programm in einer beliebigen Programmiersprache schreiben oder nutzen. Bitte geben Sie den Quellcode oder andere verwendete Referenzen an!

f) In welchem Jahr fand dieses Ereignis zum ersten Mal statt? (5 Pkt.)