Übung 4

Abgabetermin: 17. November 2011 **vor** der Vorlesung

1. *Known-Plaintext Attacke gegen LFSR-Stromchiffre*

   Wir führen eine Known-Plaintext Attacke gegen eine Stromchiffre durch, die auf LFSRs basiert. Wir wissen, dass der Klartext wie folgt ausgesehen hat:

   `1010 1010 1010 0101 0101 0101 1001`

   Auf dem Kommunikationskanal haben wir die folgende Bitfolge abgehört:

   `0000 1101 1110 1011 1100 1000 1010`

   (a) Was ist der Grad m des Generators der Stromchiffrierung? Gehen Sie von einem LFSR mit maximaler Periodenlänge aus. (5 Pkt.)

   (b) Was ist der Initialisierungsvektor? (z_{0-2}) (5 Pkt.)

   (c) Bestimmen Sie die Rückkopplungskoeffizienten (C_{0-2}) des LFSRs . (5 Pkt.)

2. *Periode eines LFSR*

   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.
     Anmerkung: Alle primitiven Polynome sind irreduzibel.
   - LFSRs, die keine Sequenz maximaler Länge erzeugen und bei denen die Sequenzlänge von dem Initialisierungsvektor der Register 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. Wir werden jetzt einige Beispiele betrachten. Finden Sie *alle* Sequenzen die durch die folgenden Polynome erzeugt werden. Zeichnen Sie zunächst das Schaltbild für jedes Schieberegister. Beachten Sie, dass Sie u.U. verschiedene Initialsierungsvektoren benutzen müssen, um alle Sequenzen zu erzeugen:

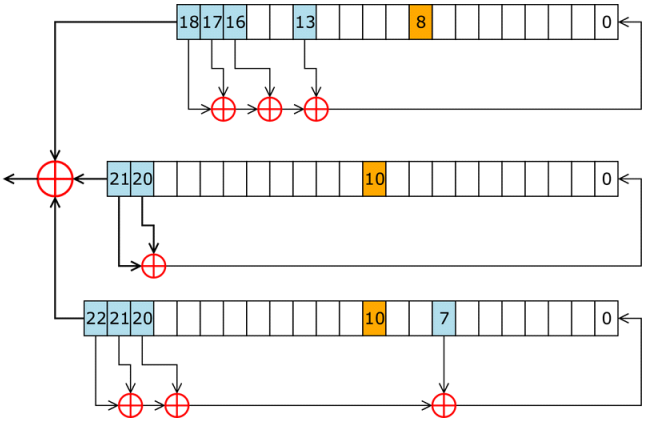
   (a) $x^4 + x^2 + 1$ (10 Pkt.)

   (b) $x^4 + x^3 + x^2 + x + 1$ (10 Pkt.)

   (c) $x^4 + x + 1$ (10 Pkt.)

3. *Die A5/1 Stromchiffre im Handy*

In Europa werden die Sprachdaten einer Kommunikation mit einem GSM-Handy mit Hilfe der A5/1 Stromchiffre verschlüsselt. Die Stromchiffre besteht aus drei parallel geschalteten LFSRs der Länge 19, 22 und 23, deren Ausgänge mit einem XOR am Ende verschaltet werden. Das Blockschaltbild und die Rückkopplungen des A5/1 sind in folgender Darstellung (Quelle: Wikipedia) abgebildet:



Um die A5/1 Stromchiffre überhaupt sicher zu machen, werden die drei LFSR nicht regelmäßig sondern nach dem Mehrheitsprinzip getaktet, d.h. in jedem der drei LFSR gibt es ein Taktregister (orange im Blockdiagramm gekennzeichnet), mit denen bestimmt wird, welche der drei LFSRs getaktet werden sollen. Beinhalten mindestens zwei Taktregister gleichzeitig eine Null, werden nur die LFSRs getaktet, die die Null im Taktregister haben. Falls andersherum mindestens zwei Taktregister aber eine logische Eins zeigen sollten, werden alle Register mit einer logischen Eins getaktet.
Beispiel: Taktregister 8 von LFSR 1 und Taktregister 10 von LFSR 2 sind Null und das Register 10 des LFSR 3 ist eine Eins. In diesem Fall werden nur LFSR 1 und 2 getaktet und LFSR 3 bleibt unverändert.

(a) Wie viele Bits des Zustandsregisters muss ein Angreifer herausbekommen, um den A5/1 zu brechen (d.h. den vollständigen Schlüsselstrom vorherzusagen)? Wie hoch wäre also der Aufwand für den Angreifer, wenn er den Zustand des A5/1 erraten müsste (wie viele Möglichkeiten gibt es, die es durchzuprobieren gilt)? (10 Pkt.)

(b) Berechnen Sie das aktuelle und die *folgenden* 8 Ausgabebits des A5/1 auf Basis der gegebenen LSFR-Zustände. Geben Sie für jede Runde die Inhalte der 3 LFSRs, die Taktbits und das Ausgabebit an. Kennzeichnen Sie die Taktbits und die für die Rückkopplung relevanten Bits. Nutzen Sie hierzu die angehängte Lösungsvorlage. (62 Pkt.)

$$\begin{aligned}
\text{LFSR}_{19} &= (z_{18}, \ldots, z_0) = (1100010010010100101) \\
\text{LFSR}_{22} &= (z_{21}, \ldots, z_0) = (1000101000011111000110) \\
\text{LFSR}_{23} &= (z_{22}, \ldots, z_0) = (11100101100100100100001)
\end{aligned}$$

Hinweis: Es ist aus korrekturtechnischen Gründen zwingend erforderlich ist, dass Sie die angehängte Lösungsvorlage nutzen. Andere Lösungen werden **nicht angenommen**.

Lösungsvorlage zu Übung 4, Aufgabe 3b)

Name:
Matrikelnr:

Partner:
Matrikelnr:

Kreisen Sie das jeweilige Taktregister ein (oder kennzeichnen Sie diese farblich).
Unterstreichen Sie die für die Rückkopplung relevanten Bits (oder kennzeichnen Sie diese farblich).

Runde 0:

$\text{LFSR}_{19} = (z_{18}, \ldots, z_0) \;=\; (\_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_)$
$\text{LFSR}_{22} = (z_{21}, \ldots, z_0) \;=\; (\_\_\ \_\_)$
$\text{LFSR}_{23} = (z_{22}, \ldots, z_0) \;=\; (\_\_\ \_\_)$
$Ausgabe \;=\; \_\_ \oplus \_\_ \oplus \_\_ = \_\_$
$Taktregister \;=\; \_\_ \oplus \_\_ \oplus \_\_$

Runde 1: __ LFSR_{19} __ LFSR_{22} __ LFSR_{23} wird getaktet (ankreuzen).

$\text{LFSR}_{19} = (z_{18}, \ldots, z_0) \;=\; (\_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_)$
$\text{LFSR}_{22} = (z_{21}, \ldots, z_0) \;=\; (\_\_\ \_\_)$
$\text{LFSR}_{23} = (z_{22}, \ldots, z_0) \;=\; (\_\_\ \_\_)$
$Ausgabe \;=\; \_\_ \oplus \_\_ \oplus \_\_ = \_\_$
$Taktregister \;=\; \_\_ \oplus \_\_ \oplus \_\_$

Runde 2: __ LFSR_{19} __ LFSR_{22} __ LFSR_{23} wird getaktet (ankreuzen).

$\text{LFSR}_{19} = (z_{18}, \ldots, z_0) \;=\; (\_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_)$
$\text{LFSR}_{22} = (z_{21}, \ldots, z_0) \;=\; (\_\_\ \_\_)$
$\text{LFSR}_{23} = (z_{22}, \ldots, z_0) \;=\; (\_\_\ \_\_)$
$Ausgabe \;=\; \_\_ \oplus \_\_ \oplus \_\_ = \_\_$
$Taktregister \;=\; \_\_ \oplus \_\_ \oplus \_\_$

Runde 3: __ LFSR_{19} __ LFSR_{22} __ LFSR_{23} wird getaktet (ankreuzen).

$\text{LFSR}_{19} = (z_{18}, \ldots, z_0) \;=\; (\_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_\ \_\_)$
$\text{LFSR}_{22} = (z_{21}, \ldots, z_0) \;=\; (\_\_\ \_\_)$
$\text{LFSR}_{23} = (z_{22}, \ldots, z_0) \;=\; (\_\_\ \_\_)$
$Ausgabe \;=\; \_\_ \oplus \_\_ \oplus \_\_ = \_\_$
$Taktregister \;=\; \_\_ \oplus \_\_ \oplus \_\_$

Runde 4: __ LFSR_{19} __ LFSR_{22} __ LFSR_{23} wird getaktet (ankreuzen).

$$
\begin{aligned}
\text{LFSR}_{19} = (z_{18}, \ldots, z_0) &= (\_\_\ \_\_) \\
\text{LFSR}_{22} = (z_{21}, \ldots, z_0) &= (\_\_\ \_\_) \\
\text{LFSR}_{23} = (z_{22}, \ldots, z_0) &= (\_\_\ \_\_) \\
Ausgabe &= \_\_ \oplus \_\_ \oplus \_\_ = \_\_ \\
Taktregister &= \_\_ \oplus \_\_ \oplus \_\_
\end{aligned}
$$

Runde 5: __ LFSR_{19} __ LFSR_{22} __ LFSR_{23} wird getaktet (ankreuzen).

$$
\begin{aligned}
\text{LFSR}_{19} = (z_{18}, \ldots, z_0) &= (\_\_\ \_\_) \\
\text{LFSR}_{22} = (z_{21}, \ldots, z_0) &= (\_\_\ \_\_) \\
\text{LFSR}_{23} = (z_{22}, \ldots, z_0) &= (\_\_\ \_\_) \\
Ausgabe &= \_\_ \oplus \_\_ \oplus \_\_ = \_\_ \\
Taktregister &= \_\_ \oplus \_\_ \oplus \_\_
\end{aligned}
$$

Runde 6: __ LFSR_{19} __ LFSR_{22} __ LFSR_{23} wird getaktet (ankreuzen).

$$
\begin{aligned}
\text{LFSR}_{19} = (z_{18}, \ldots, z_0) &= (\_\_\ \_\_) \\
\text{LFSR}_{22} = (z_{21}, \ldots, z_0) &= (\_\_\ \_\_) \\
\text{LFSR}_{23} = (z_{22}, \ldots, z_0) &= (\_\_\ \_\_) \\
Ausgabe &= \_\_ \oplus \_\_ \oplus \_\_ = \_\_ \\
Taktregister &= \_\_ \oplus \_\_ \oplus \_\_
\end{aligned}
$$

Runde 7: __ LFSR_{19} __ LFSR_{22} __ LFSR_{23} wird getaktet (ankreuzen).

$$
\begin{aligned}
\text{LFSR}_{19} = (z_{18}, \ldots, z_0) &= (\_\_\ \_\_) \\
\text{LFSR}_{22} = (z_{21}, \ldots, z_0) &= (\_\_\ \_\_) \\
\text{LFSR}_{23} = (z_{22}, \ldots, z_0) &= (\_\_\ \_\_) \\
Ausgabe &= \_\_ \oplus \_\_ \oplus \_\_ = \_\_ \\
Taktregister &= \_\_ \oplus \_\_ \oplus \_\_
\end{aligned}
$$

Runde 8: __ LFSR$_{19}$ __ LFSR$_{22}$ __ LFSR$_{23}$ wird getaktet.

LFSR$_{19}$ $= (z_{18}, \ldots, z_0)$ = (__ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __)
LFSR$_{22}$ $= (z_{21}, \ldots, z_0)$ = (__ __)
LFSR$_{23}$ $= (z_{22}, \ldots, z_0)$ = (__ __)
$Ausgabe$ = __ $\oplus$ __ $\oplus$ __ = __
$Taktregister$ = __ $\oplus$ __ $\oplus$ __

Runde __ (zur Korrektur verwenden): __ LFSR$_{19}$ __ LFSR$_{22}$ __ LFSR$_{23}$ wird getaktet.

LFSR$_{19}$ $= (z_{18}, \ldots, z_0)$ = (__ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __)
LFSR$_{22}$ $= (z_{21}, \ldots, z_0)$ = (__ __)
LFSR$_{23}$ $= (z_{22}, \ldots, z_0)$ = (__ __)
$Ausgabe$ = __ $\oplus$ __ $\oplus$ __ = __
$Taktregister$ = __ $\oplus$ __ $\oplus$ __

Runde __ (zur Korrektur verwenden): __ LFSR$_{19}$ __ LFSR$_{22}$ __ LFSR$_{23}$ wird getaktet.

LFSR$_{19}$ $= (z_{18}, \ldots, z_0)$ = (__ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __)
LFSR$_{22}$ $= (z_{21}, \ldots, z_0)$ = (__ __)
LFSR$_{23}$ $= (z_{22}, \ldots, z_0)$ = (__ __)
$Ausgabe$ = __ $\oplus$ __ $\oplus$ __ = __
$Taktregister$ = __ $\oplus$ __ $\oplus$ __

Runde __ (zur Korrektur verwenden): __ LFSR$_{19}$ __ LFSR$_{22}$ __ LFSR$_{23}$ wird getaktet.

LFSR$_{19}$ $= (z_{18}, \ldots, z_0)$ = (__ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __)
LFSR$_{22}$ $= (z_{21}, \ldots, z_0)$ = (__ __)
LFSR$_{23}$ $= (z_{22}, \ldots, z_0)$ = (__ __)
$Ausgabe$ = __ $\oplus$ __ $\oplus$ __ = __
$Taktregister$ = __ $\oplus$ __ $\oplus$ __