Mattias Petersson
EDIN01 – Cryptography

2022-01 Problem 2b - BM algorithm

Shortest LFSR that generates the sequence
$s = (1, 0, 1, 2\alpha, 3\alpha, \alpha + 1)$

First create a table of $\mathbb{F}_{5^2}$, use that $p(x) = x^2 + 4x + 2, p(\alpha) = 0$

Binary	*decimal*	α
00	0	0
01	1	1
10	α	α
13	$\alpha + 3$	α^2
43	$4\alpha + 4$	α^3
22	$2\alpha + 2$	α^4
41	$4\alpha + 1$	α^5
02	2	α^6
20	2α	α^7
21	$2\alpha + 1$	α^8
31	$3\alpha + 1$	α^9
44	$4\alpha + 4$	α^{10}
32	$3\alpha + 2$	α^{11}
04	4	α^{12}
40	4α	α^{13}
42	$4\alpha + 2$	α^{14}
12	$1 + 2\alpha$	α^{15}
33	$3\alpha + 3$	α^{16}
14	$1\alpha + 4$	α^{17}
03	3	α^{18}
30	3α	α^{19}
34	$3\alpha + 4$	α^{20}
24	$2\alpha + 4$	α^{21}
11	$1\alpha + 1$	α^{22}
23	$2\alpha + 3$	α^{23}

Use this table to convert s into powers of α
$s = (1, 0, 1, 2\alpha, 3\alpha, \alpha + 1) \leftrightarrow s = (1, 0, 1, \alpha^7, \alpha^{19}, \alpha^{22})$

Initialize the B-M algorithm, with $C(D) = 1, L = 0, C_0(D) = 1, d_0 = 1, e = 1, N = 0$

s_N	d	$C_1(D)$	$C(D)$	L	$C_0(D)$	d_0	e	N
$-$	$-$	$-$	1	0	1	1	1	0

The first element we have in s is 1.

$$s_N = 1,$$
$$N = 0$$
$$d = s_N + \sum_{n=1}^{L} c_i \cdot s_{N-i} = 1 + 0 = 1$$
$$C(D) = C(D) - d \cdot d_0^{-1} \cdot C_0(D) \cdot D^e = 1 - 1 \cdot 1 \cdot 1 \cdot 1 \cdot D = 1 - D = 1 + 4D \; (\mathbb{F}_5)$$

To explain, c_i are the coefficients in $C(D)$. Since $C(D) = 1, c = (c_0, c_1, c_2, ..., c_x) = (1, 0, 0, ..., 0)$. $N > 2L$ so we update $C_1(D), L, C_0(D), d_0, e$ and propagate these values into the table, we get:

s_N	d	$C_1(D)$	$C(D)$	L	$C_0(D)$	d_0	e	N
–	–	–	1	0	1	1	1	0
1	1	1	$1+4D$	1	1	1	1	1

$$s_N = 0$$
$$N = 1$$
$$d = 0 + c_1 s_0 = 0 + 4 = 4$$
$$C(D) = 1 + 4D - (4 \cdot 1 \cdot 1 \cdot D) = 1 + 4D - 4D = 1$$

Now that $N < 2L$ we only update $C(D), e, N$:

s_N	d	$C_1(D)$	$C(D)$	L	$C_0(D)$	d_0	e	N
–	–	–	1	0	1	1	1	0
1	1	1	$1+4D$	1	1	1	1	1
0	4	1	1	1	1	1	2	2

$$s_N = 1$$
$$N = 2$$
$$d = 1 - c_1 s_1 = 1 - 0 = 1$$
$$C(D) = 1 - (1 \cdot 1 \cdot 1 \cdot D^2) = 1 - D^2 = 1 + 4D^2$$

Check if $N < 2L, 2 < 2$ is not true, as such we update accordingly (same as before, update all values in the table).

s_N	d	$C_1(D)$	$C(D)$	L	$C_0(D)$	d_0	e	N
–	–	–	1	0	1	1	1	0
1	1	1	$1+4D$	1	1	1	1	1
0	4	1	1	1	1	1	2	2
1	1	1	$1+4D^2$	2	1	1	1	3

$$
\begin{aligned}
s_N &= \alpha^7 \\
N &= 3 \\
d &= \alpha^7 + c_1 s_2 + c_2 s_1 = \alpha^7 + 0 + 0 = \alpha^7 \\
C(D) &= 1 + 4D^2 - \alpha^7 \cdot 1 \cdot 1 \cdot D \\
&= 1 + 4D^2 - \alpha^7 D \\
&= 1 - 2\alpha D + 4D^2 \\
&= 1 + 3\alpha D + 4D^2 \\
&= 1 + \alpha^{19} D + 4D^2
\end{aligned}
$$

Now things got a bit weird. Since L is larger than one (2), we need to include one more term in our calculation for d. Since c is the coefficients for D in $C(D)$ and we got $0 \cdot D$ we luckily get zeroes everywhere. When calculating C(D) we have to note that we are in mod-5 space. $-2\alpha \equiv 3\alpha$, then we just convert it by using the table at the beginning of this doc.

s_N	d	$C_1(D)$	$C(D)$	L	$C_0(D)$	d_0	e	N
–	–	–	1	0	1	1	1	0
1	1	1	$1+4D$	1	1	1	1	1
0	4	1	1	1	1	1	2	2
1	1	1	$1+4D^2$	2	1	1	1	3
α^7	α^7	1	$1+\alpha^{19}D+4D^2$	2	1	1	2	4

$$
\begin{aligned}
s_N &= \alpha^{19} \\
N &= 4 \\
d &= \alpha^{19} + c_1 s_3 + c_2 s_2 \\
&= \alpha^{19} + \alpha^7 \cdot \alpha^{19} + 1 \cdot 4 \\
&= 3\alpha + \alpha + 3 + 4 = 4\alpha + 2 = \alpha^{14} \\
C(D) &= 1 + \alpha^{19} D + 4D^2 - \alpha^{14} \cdot 1 \cdot 1 \cdot D^2 \\
&= 1 + \alpha^{19} D + 4D^2 - \alpha^{14} D^2 \\
&= 1 + \alpha^{19} D + (4 - 4\alpha - 2) D^2 \\
&= 1 + \alpha^{19} D + (\alpha + 2) D^2 \\
&= 1 + \alpha^{19} D + \alpha^{15} D^2
\end{aligned}
$$

Only interesting thing that happen here is that we can take the values of $\alpha^{19} - \alpha^{14}$ and compute immediately to get the coefficient for D^2. L is too small, update the entire table.

s_N	d	$C_1(D)$	$C(D)$	L	$C_0(D)$	d_0	e	N
$-$	$-$	$-$	1	0	1	1	1	0
1	1	1	$1+4D$	1	1	1	1	1
0	4	1	1	1	1	1	2	2
1	1	1	$1+4D^2$	2	1	1	1	3
α^7	α^7	1	$1+\alpha^{19}D+4D^2$	2	1	1	2	4
α^{19}	α^{14}	$1+\alpha^{19}D+4D^2$	$1+\alpha^{19}+\alpha^{15}D^2$	3	$1+\alpha^{19}D+4D^2$	α^{14}	1	5

$$
\begin{aligned}
s_N &= \alpha^{22} \\
N &= 5, L = 3 \\
d = \alpha^{22} + c_1 s_4 + c_2 s_3 + c_3 s_2 &= \alpha^{22} + \alpha^{19} \cdot \alpha^{19} + \alpha^{15} \cdot \alpha^7 + 0 \\
&= \alpha^{22} + \alpha^{14} + \alpha^{22} \\
&= 2(\alpha+1) + 4\alpha + 2 = 6\alpha + 4 \\
&= \alpha + 4 = \alpha^{17} \\
C(D) &= 1 + \alpha^{19}D + \alpha^{15}D^2 - \alpha^{17} \cdot (\alpha^{14})^{-1} \cdot D(1 + \alpha^{19}D + 4D^2) \\
&= 1 + \alpha^{19}D + \alpha^{15}D^2 - \alpha^{17} \cdot \alpha^{10} \cdot D(1 + \alpha^{19}D + 4D^2) \\
&= 1 + \alpha^{19}D + \alpha^{15}D^2 - \alpha^{3} \cdot D(1 + \alpha^{19}D + 4D^2) \\
&= 1 + \alpha^{19}D + \alpha^{15}D^2 - \alpha^3 D - \alpha^{22}D^2 - 4\alpha^3 D^3 \\
&= 1 + (\alpha^{19} - \alpha^3)D + (\alpha^{15} - \alpha^{22})D^2 - 4\alpha^3 D^3 \\
&= 1 + (3\alpha - 4\alpha - 3)D + (\alpha + 2 - \alpha - 1)D^2 - 4(4\alpha + 3)D^3 \\
&= 1 + (4\alpha + 2)D + D^2 + (4\alpha + 3)D^3 \\
&= 1 + \alpha^{14}D + D^2 + \alpha^3 D^3
\end{aligned}
$$

Here is the first time in this assignment we actually need to calculate d_0^{-1}. Important to note that it is just the α for which $d_0 \cdot d_0^{-1} = 1$, and in this case $d_0 = \alpha^{14} \Rightarrow d_0^{-1} = \alpha^{10}, \alpha^{10+14} = \alpha^{24} = 1$. The other calculations take a bit of time, but after that, we are done with our table, L does not need to be updated and we update the table for the last time. Shortest LFSR is the last $C(D)$ in the table.

s_N	d	$C_1(D)$	$C(D)$	L	$C_0(D)$	d_0	e	N
$-$	$-$	$-$	1	0	1	1	1	0
1	1	1	$1+4D$	1	1	1	1	1
0	4	1	1	1	1	1	2	2
1	1	1	$1+4D^2$	2	1	1	1	3
α^7	α^7	1	$1+\alpha^{19}D+4D^2$	2	1	1	2	4
α^{19}	α^{14}	$1+\alpha^{19}D+4D^2$	$1+\alpha^{19}+\alpha^{15}D^2$	3	$1+\alpha^{19}D+4D^2$	α^{14}	1	5
α^{22}	α^{17}	$1+\alpha^{19}D+4D^2$	$1+\alpha^{14}D+D^2+\alpha^3D^3$	3	$1+\alpha^{19}+4D^2$	α^{14}	2	6