Solutions to final exam in CRYPTOGRAPHY on 12 December 2007.

Problem 1

a)

$$S(D) = \frac{D^2 + D^3 + D^4 + D^6}{1 + D^7}$$

We find that $\gcd(D^6 + D^4 + D^3 + D^2, D^7 + 1) = D^4 + D^2 + D + 1$ so

$$S(D) = \frac{D^2}{D^3 + D + 1}$$

which gives the shortest LFSR as $1 + z^2 + z^3$.

b) By Berlekamp-Massey's algorithm we get $< C(D), L >=< 1 - \alpha D - \alpha^7 D^2 - \alpha D^4, 3 >$.

Problem 2

a) Using Lagrange's formula, we get

$$\begin{aligned} a(0) &= 21 \cdot 12^{-1} - 70 \cdot 8^{-1} + 300 \cdot 24^{-1} \\ &= 42 \cdot 24^{-1} - 210 \cdot 24^{-1} + 300 \cdot 24^{-1} \\ &= 31 \cdot 24^{-1} \mod 101. \end{aligned}$$

Since $24^{-1} = 80 \mod 101$, we get $K = a(0) = 56$.

b)

$$\begin{aligned} P_I &= \frac{\#\{\text{keys}(e_1, e_2) \text{s.t.} t = e_1 + \sum_{i=1}^{3} s_i e_2^i\}}{\#\{\text{keys}(e_1, e_2)\}} \\ &= [\text{for each } e_2 \text{ we have } t = e_1 + k \text{ which has a solution for exactly one } e_1] \\ &= \frac{3}{9} = \frac{1}{3} \end{aligned}$$

Turning to P_S, if we can find a message M such that the probability is 1, we are done. But let's study $M = (1, 1, 1, 0)$. If $e_2 = 2$ then $e_1 = 1$. Otherwise, $e_1 = 0$. Then for $M' = (2, 1, 0, t)$ we have

$$t = \begin{cases} 0 + 0 = 0, e_2 = 0 \\ 0 + 2 + 1 + 0 = 0, e_2 = 1 \\ 1 + 2 \cdot 2 + 1 \cdot 2^2 = 0, e_2 = 2 \end{cases}$$

so

$$P(M' = (2, 1, 0, 0) \text{ valid} | M = (1, 1, 1, 0) \text{ valid}) = 1.$$

(In fact, we can see that for this M we can "move" "mass" between s_1 and s_3 so $M'' = (0, 1, 2, 0)$ is also valid.)

We conclude that $P_S = 1$.

Problem 3

If $u_i^{(1)} = 0$ there are four equally likely values for $(u_i^{(2)}, u_i^{(3)})$ and only one yields $z_i = 1$. Thus $P(z_i = 0 | u_i^{(1)} = 0) = \frac{3}{4}$ and due to symmetry we have $P(u_i^{(j)} = z_i) = \frac{3}{4}, j = 1, 2, 3$. Since this is not 50%, we get an idea: for each shift register, the initial state that produces the sequence most similar to z is likely to be the correct key. Similar of course means small hamming distance.

Using LFSR 3 and initial state 01, we get the outsequence $[011]^\infty$. Comparing 36 bits of this sequence to z gives the hamming distance 7. Shifting the sequence one step gives $[110]^\infty$ (we now test the key 11) and the hamming distance exceeds 7. (We can quit once we realize that it will exceed it. If this optimistic guess doesn't work out, we can always do a more thorough analysis.) In the same way, the other shift gives a larger hamming distance. Assuming the all-zero state is not interesting (again, if we are wrong, we will notice), we conclude that $K_3 = 01$.

Comparing $[011]^\infty$ to z we realize that the other LFSRs *have to* give their second and fourth bit to 0 and 1, respectively. This might save us some work in the following paragraph.

Using the initial state 001 with the second LFSR gives the sequence $[0011101]^\infty$ and a comparison of the two possible shifts with z gives the best choice as $K_2 = 001$ ($d_H = 11 < 16$).

Considering the sum of $[01]^\infty$ and $[001]^\infty$ and comparing it to z gives no further information about the first key. We simply have to try all initial states that match ?0?1. We use the initial state 0001 to construct the sequence $[000111101011001]^\infty$. Of the four possible shifts, the most likely one is 0001. A quick check reveals that the majority decision logic indeed gives z. So the key is $(0001, 001, 01)$.

Problem 4

a) With $x = 989148867$ and $y = 78$, we have $x^2 \equiv y^2 \pmod{n}$ which means that $(x-y)(x+y) = x^2 - y^2 \equiv 0 \pmod{n}$. But we can quite easily find $p = \gcd(x - y, n) = 67801$. The other factor is $q = \frac{n}{p} = 56701$.

b) We assume that $p = 5507, q = 4507$ are prime numbers and find $\phi(n) = (p-1)(q-1) = 24810036$. d such that $ed \equiv 1 \pmod{\phi(n)}$ is found, using Euclid's algorithm, as $d = 3544291$. We now want to encrypt C, i. e. compute $D(C) = C^d \pmod{n}$.

We use the chinese remainder theorem:

$$\begin{aligned} M_p &= C^d (\text{mod } p) = C^{d(\text{mod } p-1)} (\text{mod } p) \\ &= C^{3933} (\text{mod } p) \\ M_q &= C^d (\text{mod } q) = C^{d(\text{mod } q-1)} (\text{mod } q) \\ &= C^{2575} (\text{mod } q) \end{aligned}$$

Note that $3933 = 2^{11} + 2^{10} + 2^9 + 2^8 + 2^6 + 2^4 + 2^3 + 2^2 + 2^0$. We find that

$$\begin{aligned} M_p &\equiv 4493 (\text{mod } p) \\ M_q &\equiv 986 (\text{mod } q) \end{aligned}$$

and the chinese remainder theorem gives $M = 10000$.

Problem 5
We have from the problem formulation that

$$\begin{aligned} c_1 &= 0 \\ c_2 = c_3 = c_4 = c_5 &= 1 \\ m_1 = m2 = m3 = m4 = m5 &= 1 \end{aligned}$$

and instantly gather that

$$\begin{aligned} s'_1 &= c_1 + m_1 = 1 \\ s'_2 = s'_3 = s'_4 = s'_5 &= 0 \end{aligned}$$

which gives some bits from the original LFSR: $s_3 = s'_1 = 1$ and $s_6 = s_9 = s_12 = s_15 = 0$.

Now, we generally have that for $i \geq 6$, the original bit number i can be calculated as $s_i = s_{i-5} + s_{i-2}$. We use this and aim at deducing the initial state:

$s_1 = s_1$	$s_2 = s_2$	$\underline{s_3 = 1}$
$s_4 = s_4$	$s_5 = s_5$	$s_6 = s_1 + s_4 = 0 \Leftrightarrow \underline{s_1 = s_4}$
$s_7 = s_2 + s_5$	$s_8 = s_3 + s_6 = 1$	$s_9 = s_4 + s_7 = \underline{s_4 + s_2 + s_5 = 0}$
$s_{10} = s_5 + s_8 = s_5 + 1$	$s_{11} = s_6 + s_9 = 0$	$s_{12} = s_7 + s_{10} = s_2 + s_5 + s_5 + 1 = 0 \Leftrightarrow \underline{s_2 = 1}$
$s_{13} = s_8 + s_{11} = 1$	$s_{14} = s_9 + s_{12} = 0$	$s_{15} = s_{10} + s_{13} = s_5 + 1 + 1 = \underline{s_5 = 0}$

We have found that $(s_1, s_2, s_3, s_4, s_5) = (s_1, 1, 1, s_1, 0)$. We finally use $s_4 + s_2 + s_5 = 0$ to conclude that $s_1 = 1$. Since we need s'_{10}, we work out s_i up to $i = 30$ and find that the sequence $\mathbf{s}' = (1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$. Comparing this to $\mathbf{c}$, we find $\mathbf{m} = (1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$.
