Short solutions to final exam in CRYPTOGRAPHY on 16 December 2011.

Problem 1

a) Wrong. $D^4 + D^2 + 1 = (D^2 + D + 1)^2$ in $\mathbb{F}_2$.

b) Wrong. $D^4 + D^2 + 1 = (D^2 + D + 1)(D^2 + 2D + 1)$ in $\mathbb{F}_3$.

c) Wrong. Since $\mathbb{F}_2$ is a subfield of $\mathbb{F}_{2^{31}}$ we still have $D^4 + D^2 + 1 = (D^2 + D + 1)^2$.

d) Wrong. If it is not irreducible, it cannot be primitive.

e) Correct. Compute the period of $P(D)$.

$$\begin{array}{r|l} & \underline{1 + D^2} \\ \underline{D^4 + D^2 + 1} & 1 \\ & \underline{1 + D^2 + D^4} \\ & D^2 + D^4 \\ & \underline{D^2 + D^4 + D^6} \\ & D^6 \end{array}$$

Problem 2

$33965^2 = 3 \bmod 44370047, 2145407^2 = 57 \bmod 44370047, 19416874^2 = 9 = 3^2 \bmod 44370047, ...$

Since we immediately have two squares being equal, we try to compute

$$\gcd(19416874 - 3, 44370047) = 7237.$$

So $n = 7237 \cdot 6131$.

Important: If your calculator does not allow to compute things like $2145407^2 = 57 \bmod 44370047$ directly, find out how you compute it using partial results! (solve this problem with your calculator, not your computer)

Problem 3

a) A Shamir scheme (3,7) over $\mathbf{F}_{37}$, where the the secret key is known to be $K = a_0 = 1$. We have $x_i = i$, so $x_2 = 2, x_3 = 3, x_{29} = 29$ and shares $y_2 = 13, y_3 = 3$, and y_{29} is to be found.

$$\begin{pmatrix} 13 \\ 3 \\ y_{29} \end{pmatrix} = \begin{pmatrix} 1 + a_1 \cdot 2 + a_2 \cdot 2^2 \\ 1 + a_1 \cdot 3 + a_2 \cdot 3^2 \\ 1 + a_1 \cdot 29 + a_2 \cdot 29^2 \end{pmatrix},$$

Gaussian elimination over $\mathbf{F}_{37}$ gives the solution $y_{29} = 32$.

(5p)

b) $M = (1, 0, 13)$, and

$$P(M' \text{ accepted } | M \text{ observed }) = \frac{\left(\text{Number of keys } e_1 \text{ for which } \begin{cases} 13 = e_1 + e_1 \\ t' = e_1 + s_1' e_1 + s_2' e_1^2 \end{cases} \right)}{\text{Number of keys } e_1 \text{ for which } 13 = e_1 + e_1}$$

So we see that $13 = 2e_1$ and $e_1 = 13 \cdot 2^{-1} = 13 \cdot 51 = 57 \bmod 101$. Then the key is known and we can substitute with another message with probability 1, for example $M = (0, 0, 57)$.

(5p)

Problem 4

a)

$$S(D) = \frac{1 + 2D^2 + 2D^3 + D^5}{1 - D^6}$$

Now compute $\gcd(1 + 2D^2 + 2D^3 + D^5, 1 - D^6)$ using Euclidean algorithm. The result is $\gcd(1 + 2D^2 + 2D^3 + D^5, 1 - D^6) = 2D^4 + 2D^3 + D + 1$. Then $(1 - D^6)/(2D^4 + 2D^3 + D + 1) = D^2 + 2D + 1$ and the shortest LFSR has connection polynomial $C(D) = 1 + 2D + D^2$.

(5p)

b) Set up a table of $\mathbb{F}_{2^4}$. It so happens that α is not a primitive element, so the table should contain powers of some other element, being primitive.

Then use the B-M algorithm

The solution is $C(D) = 1 + (\alpha^3 + \alpha + 1)D^2 + (\alpha^2 + \alpha + 1)D^3$. (5p)

c) Since 47 is a prime, the LFSR with connection plynomial $C(D) = 1 + aD$ will have period 46 if a is a primitive element. Computing $\text{ord}(2) = 23, \text{ord}(3) = 23, \text{ord}(4) = 23, \text{ord}(5) = 46$, we find that $C(D) = 1 + 5D$ is such a connection polynomial for a shortest LFSR. (Possible orders are 1,23,46)

Problem 5

a)

$$\phi(n) = (p - 1)(q - 1) = pq - p - q + 1 = 4961736.$$

$$n = pq = 4967299.$$

So $p + q = 5564$ and then $p = 4967299/q = 4967299/(5564 - p)$, so $(5564 - p)p = 4967299$. Solving for p gives $p = 1117$ and finally $q = 4447$.

(3p)

b) $d = e^{-1} \bmod \phi(n)$, and again using Euclidean alg. we get $d = 3969389$

(3p)

c) $C = 4967298^5 = (-1)^5 = -1 = 4967298$.

(2p)

d) The signature S_i is generated by "encrypting" using the secret key d, i.e., $S_i = M_i^d \bmod n$ for $i = 1, 2$. Then $(M_1 M_2, S_1 S_2)$ is a valid message/signature pair that was not sent before.

Use of a hash function allows variable-sized messages to be hashed and protects against some attacks on this basic version.