Problems in cryptology, week 3

Exercise 4.1. *Show that the polynomial $x^4 + x + 1$ is irreducible over the field GF(2).*

Exercise 4.2. *Find $(0110)^{1/2}$. $\pi(\alpha) = \alpha^4 + \alpha + 1$.*

Exercise 4.3. *Determine the elements in GF(3^2). $\pi(x) = x^2 + x + 2$ is irreducible over GF(3)*

Exercise 4.4. *Give the addition and multiplication tables for*

a) *GF(5)*

b) *GF(7)*

Exercise 4.5. *Give the multiplication table for GF(2^2), $\pi(x) = x^2 + x + 1$.*

Exercise 4.6. *Show that in all fields of characteristic p the following equality holds.*

$$(x + y)^p = x^p + y^p$$

Exercise 4.7. *Find gcd($1 + D^7, 1 + D^2 + D^5 + D^6$) over GF(2).*

Exercise 4.8. *The stop-and-go-generator is built using two linear feedback shift registers, L_1 and L_2. If L_2 outputs 1, then L_2 is clocked and the output bit of L_2 is the new keystream bit. If L_1 outputs 0 then L_2 is not clocked and the new keystream bit is the previous bit from L_2. As an example, if L_1 produces (101001...) and L_2 produces $(a_0, a_1, a_2, \ldots)$ then the keystream sequence is $(a_0, a_0, a_1, a_1, a_1, a_2, \ldots)$.*

a) *Describe a distinguishing attack on the generator.*

b) *One day, you manage to intercept a transmission that you know have been encrypted using the stop-and-go-generator. The intercepted bitstream is*

$$C = (1001\ 1101\ 0110\ 1001\ 0001\ 0010\ 1110\ 0101).$$

You know that the intercepted bitstream is the encryption of one of the messages m_1, m_2 or m_3. Determine which message was encrypted.

m_1 : (1110 1000 1011 1111 1101 0001 0111 1100)

m_2 : (1101 1010 1100 0101 1001 1101 1011 1111)

m_3 : (1010 1100 1001 0110 1000 0101 0010 0101)

Exercise 4.9. *Determine the sequence corresponding to each of the following D-transforms*

a) $\frac{1}{D^{-1}+2}$ *in GF(3)*

b) $\frac{D^{-1}}{D^{-1}+2}$ *in GF(3)*

c) $\frac{1}{D^{-2}+D^{-1}+1}$ *in GF(2)*

Exercise 4.10. *Determine the period for each of the following polynomials*

a) $1 + D + D^2 + D^3 + D^4$ *in GF(2)*

b) $1 + D + D^2 + D^4$ *in GF(2)*

c) $1 + D^3 + D^6$ *in GF(2)*

d) $1 + 3D^2$ *in GF(5)*

e) $1 + 3D + 3D^2$ *in GF(5)*

Exercise 4.11. *Determine the cycle set for each of the following connection polynomials*

a) $1 + D^2 + D^4$ *in GF(2)*

b) $1 + D^4$ *in GF(2)*

c) $1 - D - 2D^2$ *in GF(3)*

d) $1 - 2D - D^2$ *in GF(3)*

e) $1 - D - D^2$ *in GF(3)*

Exercise 4.12. *Determine the cycle set for* $C(D) = 1 - 8D + 2D^2$ *in GF(13).*