MTH6115 Cryptography Exercises 3 Solutions

Q1 (a) The output sequence is

$$1010011\ 1010\ldots$$

Its period is 7.

(b) Every configuration in the same cycle as 1010 will have period 7.
The output sequence when the initial configuration is 0001 is

$$0001011\ 0001\ldots$$

This also has period 7 and every configuration in the same cycle as 0001 will have period 7.
The output sequence when the initial configuration is 0000 or 1111 has period 1.

Q2(a)(i) We have $v_0 = u_1, v_1 = u_2, \ldots, v_{n-2} = u_{n-1}$ and $v_{n-1} = \sum_{i=0}^{n-1} a_i u_i$. Thus $u_1 = v_0, u_2 = v_1, \ldots, u_{n-1} = v_{n-2}$ and

$$u_0 = v_{n-1} + \sum_{i=1}^{n-1} a_i u_i = v_{n-1} + \sum_{i=1}^{n-1} a_i v_{i-1}.$$

(ii) Suppose that $(v_0, v_1, \ldots, v_{n-1})$ is the first configuration which is repeated by the shift register. Part (i) tells us that the configuration $(u_0, u_1, \ldots, u_{n-1})$ which precedes $(v_0, v_1, \ldots, v_{n-1})$ is completely determined by $(v_0, v_1, \ldots, v_{n-1})$. Thus, if $(v_0, v_1, \ldots, v_{n-1})$ were not the initial configuration, then $(u_0, u_1, \ldots, u_{n-1})$ would have been repeated before $(v_0, v_1, \ldots, v_{n-1})$. This would contradict the choice of $(v_0, v_1, \ldots, v_{n-1})$. Hence $(v_0, v_1, \ldots, v_{n-1})$ is the initial configuration.

(b) Consider for example the 3-bit shift register described by the polynomial $x^3 + x$, with initial configuration $(1, 0, 0)$. The next two configurations are (0,0,0) and (0,0,0). Thus the first configuration to be repeated is not the initial configuration.

Q3(a) The number of primitive 5-bit shift registers is $\Phi(2^5-1)/5 = \Phi(31)/5 = 6$.

(b) Let $p(x) = x^5 + a_4x^4 + a_3x_3 + a_2x^2 + a_1x + a_0$ be irreducible. Since x is not a factor of $p(x)$ we have $a_0 = 1$ and since $x + 1$ is not a factor we have $a_4 + a_3 + a_2 + a_1 = 1$. This leaves 8 possible values for (a_4, a_3, a_2, a_1). We can find which of these give irreducible polynomials as follows.

Consider for example $p(x) = x^5 + x^2 + 1$. We know that $p(x)$ has no factor of degree one. So if $p(x)$ factorises, we must have $x^5 + x^2 + 1 = (x^2 + bx + 1)(x^3 + cx^2 + dx + 1)$. Equating powers of x we get $b + d = 0$, $1 + bd + c = 1$, $1 + bc + d = 0$, $b + c = 0$. The first equation gives $b = d$, and the last equation gives $b = c$. We can now rewrite the second and third equations as $b^2 + b = 0$ and $b^2 + b = 1$ which clearly have no solution. Hence $p(x)$ is irreducible.
(A similar analysis works for the other irreducible polynomials $x^5 + x^3 + 1$, $x^5+x^4+x^3+x^2+1$, $x^5+x^4+x^2+x+1$, $x^5+x^4+x^3+x+1$, $x^5+x^4+x^3+x^2+1$.)

(b) The output sequence for the shift register described by $x^5 + x^2 + 1$ is

$$0000100101100100111110001101110101\ 00001\ldots$$

The shift register is primitive since it cycles through all 31 non-zero configurations of $\mathbb{Z}_2^5$.

Q4 Since the first two letters in the message are ‘th’, the first 8 bits in the plaintext are 00001001. Since the first 8 bits in the ciphertext are 10111011 So the first 8 bits in the keyword are given by

$$0000100101 \oplus 1011101101 = 10110010$$

Let the polynomial describing the shift register be $x^4 + a_3x^3 + a_2x^3 + a_1x + a_0$. Then we have the following system of simultaneous equations.

$$\begin{array}{rcllll} 0 & = & a_0 & & +a_2 & +a_3 \\ 0 & = & & a_1 & +a_2 & \\ 1 & = & a_0 & +a_1 & & \\ 0 & = & a_0 & & & +a_3 \end{array}$$

This has the unique solution $a_0 = a_3 = 1$ and $a_1 = a_2 = 0$. So the polynomial describing the shift register is $x^4 + x^3 + 1$. Since the first 8 bits in the keyword are 10110010, the initial configuration of the shift register is (1011). Hence the output sequence of the shift register is

$$101100100011110\ 1011001000111\ 10101100100011110\ 1011001000...$$

Since the substitution table is just the addition table for $\mathbb{Z}_2$, we can find the plain text by adding the keyword to the ciphertext. Thus the plaintext is

$$00001001010101010000100000001100110100000000011100100011$$

We can now use the table for the International Telegraph Code to decode the plaintext and obtain the message ‘threeonetwo’.