MTH6115 Cryptography Exercises 3

Hand in to BLUE BOX on SECOND FLOOR of math sci building before 4:30pm on Friday 13/2/09.
Remember: *The work you hand in should be your OWN work. If you work in groups make sure you YOURSELF understand the answers that have been obtained, and write up your answers YOURSELF. I take a dim view of copied answers, and will penalise them severely when I detect them.*

Q1 Let S be the 4-bit shift register described by the polynomial x^4+x^2+x+1.
(a) Calculate its output sequence when the initial configuration is 1010 and find its period. [10]
(b) Determine the period of the output sequence for each other initial configuration. [10]

Q2 Let S be an n-bit shift register described by the polynomial $x^n+\sum_{i=0}^{n-1} a_i x^i$.
(a) Suppose that $a_0 = 1$ and that S changes from configuration $(u_0, u_1, \ldots, u_{n-1})$ to $(v_0, v_1, \ldots, v_{n-1})$ after one tick of the clock.
(i) Express $u_0, u_1, \ldots, u_{n-1}$ in terms of $v_0, v_1, \ldots, v_{n-1}$. [10]
(ii) Use (i) to prove that the first time S repeats a configuration is when its initial configuration is repeated. [10]

(b) Give an example of a shift register and an initial configuration for which (a)(ii) does not occur. [10]

Q3 (a) How many primitive 5-bit shift registers are there? [5]
(b) Find an irreducible polynomial of degree five over $\mathbb{Z}_2$ and prove that your polynomial is indeed irreducible. [10]
(c) Determine the output sequence of the shift register described by your polynomial in (b) when the initial configuration is (0,0,0,0,1). Is this shift register primitive? Justify your answer. [10]

Q4 A message written in English is encoded into plaintext by replacing all upper case letters by lower case letters, then deleting all spaces, and then replacing each letter by its 5-bit string given in the International Telegraph Code (see overpage). It is then encrypted by a stream cipher which uses a 4-bit shift register to generate the keyword and uses the addition table of $\mathbb{Z}_2$ as its substitution table. The resulting ciphertext is given below.

1011101101101000011011000111011000011000111110111101011

You discover that the first two letters in the message are ‘th’.
(a) Determine the polynomial describing the shift register and find its initial state. [15]
(b) Decrypt the ciphertext and determine the message. [10]