Queen Mary
University of London

MTH6115 Cryptography

Assignment 3 For handing in on 14th February 2011

Your solutions to Questions 4 should be handed in to the ORANGE box on the GROUND floor by 3:30 pm on Monday 14th February 2011.

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. You should also endeavour to do ALL the questions, not just those you hand in for assessment.*

1 For the shift register with polynomial $x^5 + x + 1$ over $\mathbb{Z}_2$, and for each nonzero initial configuration $x_0x_1x_2x_3x_4$, determine the period of the sequence so generated. Is this shift register primitive, and is the polynomial irreducible or reducible? Justify your answer. Let A be the matrix associated with the above shift register. Find a column vector u such that u, Au, A^2u, A^3u, A^4u are linearly independent.

2 Consider the shift registers that are represented by each of the 16 $\mathbb{Z}_2$-polynomials $x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. Determine the periods of all the initial configurations which repeat later on. For those that do not, determine the first configuration it maps to that does so repeat.

3 Determine the irreducible polynomials of degree 6 over $\mathbb{F}_2 = \mathbb{Z}_2$. Which of these give rise to primitive shift registers? Justify your answer. Do the same for other degrees, such as 5, 7 and 8.

4 A piece of text was encrypted using 7-bit ASCII, then encrypted using a keystring obtained from a 6-bit shift register. The encrypted message is given below.

01100000110011110010100110100110000110011001011100110101111010011101000101100110101011101111110011010100101111110101001110010

Your spies have informed you that the first two letters of the original text are `jn`. Decrypt it. The ASCII codes map A–Z to 65–90 and a–z to 97–122, and these are converted to 7-bit ASCII by converting 33 to 0100001 rather than 1000010 (that is with the left-most column being the 64s column, not the 1s column). 'Space' has ASCII code 32, and the punctuation `!',-.:;?@` has codes 33, 39, 44, 45, 46, 58, 59, 63, 64 respectively. Is the underlying shift register primitive? Justify your answer.

5 Consider the field $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4+x^3+1)$, and let α be the element corresponding to x therein. For $0 \leqslant i \leqslant 14$ express α^i as a $\mathbb{Z}_2$-linear combination of $1, \alpha, \alpha^2, \alpha^3$. Write out the output of the shift register corresponding to $x^4 + x^3 + 1$, with initial configuration 0001.

6 Using the standard English alphabet, V and V' denote (possibly equal) Vigen‘ere ciphers of length 7, and S denotes a substitution cipher. Alice and Bob choose a cipher of the form $VS = V \circ S$ (apply V first), while Angelina and Brad opt for a cipher of the form SV. How many different ciphers are available to (a) Alice and Bob, and (b) Angelina and Brad. Who (if either of the pairs) has the more secure cipher, and why? In an attempt to increase security, both pairs preëncrypt with a Vigenère cipher of length 7 (so that Alice and Bob's cipher has the form $V'VS$ and Angelina and Brad's cipher has the form $V'SV$). Who (if either of the pairs) now has the more secure cipher, and why? Has the security increased for either (or both) pair(s), and if so, which pair(s)?