Queen Mary
University of London

MAS 335 Cryptography

Assignment 3 For handing in on 7th February 2008

Your solutions to these questions should be handed in to the RED box on the SECOND floor by 3.30pm on Thursday.

Remember: The work you hand in should be your OWN work. If you copy other people's work, you do not learn it properly yourself, and you will do MUCH WORSE in the final exam than if you do your own coursework.

1 (a) How many irreducible polynomials of degree 5 over $\mathbb{Z}/(2)$ are there? How many are primitive?

(b) Same question for degree 6.

[Justify your answers from first principles: answers which quote Theorem 8 from the notes will not get many marks.]

2 The *seven-bit ASCII code* represents letters, digits, and punctuation as characters from the set of integers in the range $32 \ldots 127$; the capital letters `A...Z` are represented by $65 \ldots 90$, and lower-case letters `a...z` by $97 \ldots 122$. Integers in the range $0 \ldots 31$ are used for control codes. The integers are then written in base 2, as 7-tuples of zeros and ones. So, for example, `At` is written as 10000011110100. (For more detail see the course Web page.)

You intercept the string

1101000000100111110000011000101110000101110110111

You have reason to believe that it is a message in seven-bit ASCII encrypted by means of a stream cipher based on a seven-bit shift register, and that the first two letters of the message are `Re`. Decrypt the string.

3 Let A be a Latin square, with rows and columns numbered $1, \ldots, q$ and with entries from the set $\{1, \ldots, q\}$. Write down a condition on the entries a_{ij} of A which is necessary and sufficient for A to have the following property:

If A is used as the substitution table for encrypting a stream cipher, then *the same square* can be used in the same way for decrypting the cipher.

(Remember that we encrypt the plaintext symbol i with key symbol j as the ciphertext symbol a_{ij}. The question asks for a Latin square for which the same rule works for the decryption.)

Find two different examples of Latin squares of order $q = 5$ having this property. Show that such a Latin square exists for any value of q.

4 Write down a string of 'random' bits, of length 32. (That is, try to avoid any obvious patterns.) How close does your string come to satisfying Golomb's postulates? Now toss a coin 32 times to generate random bits. Does this string fit Golomb's postulates better?