Queen Mary
University of London

MAS 335 Cryptography

Assignment 2 For handing in on 2nd February 2005

---

1 Show that every permutation on the set $\{0,1,\ldots,n-1\}$ is affine if and only if $n \leq 3$.

2 The following has been enciphered with a Vigenère cipher using a keyword of length 4; the ciphertext has been written in blocks of size 4 for your convenience. Decrypt it.

```
VSUP MMNI BWAN XWSR KICK LITQ HPFQ KMNH
BRIV XWEV LXHC GJOT YMNK MIOP XWTJ XWHG
ILET WISU PLOE TRCQ NRTJ XVFN HGKQ YEHW
GHRG WWHG XTWK EPKP HAIH MLEY HPFJ TWTC
DINQ GIBW MMFU AIHC LENK GJIP BXEH ESCM
LLEY HRTP HXIE XYNV BPAN FSSV TPLQ YLET
LLEG ILAX XFEG GPOU MREX XVTJ XPEU LGOO
UMNC MSRK VWDG IINF LSNE HYNV BRGU HMNV
AIFK KWTU XGTK HRYQ NAIN EJIP WEQW BGKV
HYRV AVOW ZLSG MXHG HVYC GHTJ XXWQ DMNF
LSFP NQBG KWUU XHFQ KMNH BRIV XGOW GXIP
Z
```

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

(b) Same question for degree 6.

(c) How many necklaces can be made of five beads, each either black or white, on a circular string, if two necklaces which differ only by a rotation are counted as the same (so that BBWWW and WBBWW are the same, for example)? How many of these have no "symmetry", that is, no rotation gives exactly the same necklace? Now answer the same question for six beads.

4 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

01001101110110110111101111111101101011011110010 11

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 `Ad`. Decrypt the string.

5 Complete the following figure to a Latin square.

1	2	3	4	5
2	1	4	5	3

6 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.