Queen Mary
University of London

MTH6115 Cryptography

Assignment 4 For handing in on 28th February 2011

Your solutions to Questions 4 and 5 (which may be answered simultaneously) should be handed in to the ORANGE box on the GROUND floor by 3:30 pm on Monday 28th February 2010. Note that the exercise classes for this sheet will be held on 16th and 17th February; the week after this is Reading Week.

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 Write down a string of 'random' bits, of length 40. (That is, try to avoid any obvious patterns.) How close does your string come to satisfying Golomb's postulates? Now toss a coin 40 times to generate random bits. Does this string fit Golomb's postulates better?

2 Let L be a weak substitution table on the alphabet $\mathscr{A} = \{a_0, \ldots, a_{n-1}\}$ (so that $a_i \oplus a_j = L_{ij} \in \mathscr{A}$ for all i and j, and for each column and each i there is precisely one entry a_i in that column). State conditions on L such that the following hold.

(i) The same matrix L can be used for decryption as well as encryption. That is, for all plaintexts p and keys k we have $p = z \oplus k$ as well as $z = p \oplus k$, or put another way $(p \oplus k) \oplus k = p$ for all p and k.

(ii) We have $p \oplus k = k \oplus p$ for all p and k.

(iii) Both of the above.

Show that the substitution tables in (ii) and (iii) are Latin squares. What orders can the permutations corresponding to columns in Parts (i) and (iii) have, and what about Part (ii)? For which $n \in \mathbb{N}^+$ do there exist arrays satisfying Condition (iii)? Justify your answer. For each $n \in \{1, 2, 3, 4, 5\}$ write down at least two such arrays of order n (or size $n \times n$). Try to make them 'essentially different' (whatever that means), if possible. If there are not as many as two, write down all such things.

3 A message has been converted into 7-bit ASCII and then encrypted by means of a stream cipher based on a 7-bit shift register. You intercept the ciphertext, which is the string

$$00100110111001101011011011110101000100100010101000010100.$$

Decrypt the string, given that the first two letters of the plaintext are `Cr`. ASCII codes are given elsewhere, like on Exercises 3, but we recall that A–Z are encoded using 65–90 and a–z are encoded using 97–122.

4 A message in a 4-letter alphabet $\{0, 1, 2, 3\}$ has been encrypted using a random keystring (keys uniformly distributed), and substitution table

	0	1	2	3
0	3	1	3	1
1	1	3	1	3
2	2	0	0	0
3	0	2	2	2

The message has length 5. Before intercepting the ciphertext your estimates of the probabilities of the plaintext strings are

$$\mathrm{P}(21312) = \tfrac{1}{5}, \quad \mathrm{P}(20310) = \tfrac{3}{10}, \quad \mathrm{P}(30312) = \tfrac{1}{2},$$

with the other probabilities being 0. You intercept the ciphertext 23030. Calculate the conditional probabilities of the plaintext strings given this information. Does your answer contradict Shannon's Theorem?

5 Same as previous question, but with probabilities

$$\mathrm{P}(21312) = a, \quad \mathrm{P}(20310) = b, \quad \mathrm{P}(30312) = c,$$

where of course $a, b, c \geqslant 0$ and $a + b + c = 1$. You must be very careful of any degenerate cases that may arise.