Queen Mary
University of London

B. Sc. Examination 2004

MAS 335 Cryptography

Duration: 2 hours

Date and time: 11 May 2004, 10:00–12:00

You may attempt as many questions as you wish and all questions carry equal marks. Except for the award of a bare pass, only the best 5 questions answered will be counted.

Calculators are NOT permitted in this examination. The unauthorised use of a calculator constitutes an examination offence.

Question 1 (20 marks)

(a) What is an *affine permutation* of the set $\mathbb{Z}/(n)$ of integers modulo n? [2]

(b) Prove that the number of affine permutations is equal to $n\phi(n)$, where ϕ is Euler's function. [4]

(c) Suppose that $x, y \in \mathbb{Z}/(n)$ and $\gcd(y-x, n) = 1$. Prove that, for any $u, v \in \mathbb{Z}/(n)$, there is at most one affine permutation which maps x to u and y to v. [4]

(d) The following is the encryption of a short piece of English text with an affine substitution cipher. Decrypt it. [10]

```
wncni wnikw bschw minrn rsvsf uswws pksgj
nrsep ivsfw skrcp kscpb kgpni paspk u
```

Question 2 (20 marks)

(a) What is a one-time pad? [3]

(b) State and prove Shannon's Theorem. [12]

(c) Explain why each of the following ciphers fails to be a one-time pad: [5]

(i) a Vigenère cipher;

(ii) the Japanese Army Air Force cipher 6633, a stream cipher whose key is a random string of digits and whose substituution table is

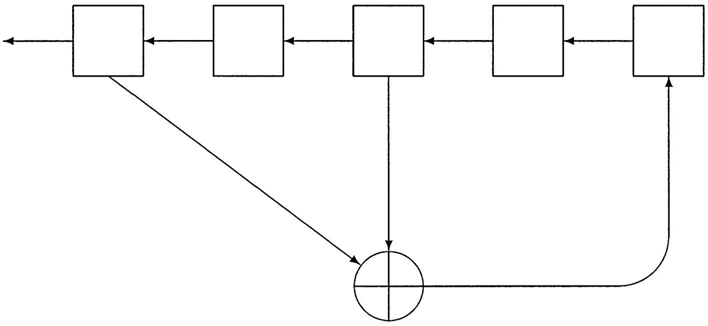
4	9	5	3	2	7	0	1	6	8
7	5	0	9	3	2	1	8	1	4
3	1	7	2	8	0	9	6	9	7
0	8	4	7	0	1	3	4	5	2
5	3	2	4	9	3	8	2	7	6
9	0	1	6	7	5	4	7	2	3
2	6	8	0	0	9	7	5	3	1
6	2	6	1	4	8	6	0	8	5
1	7	9	8	1	4	5	9	0	7
8	4	3	5	5	6	2	3	4	0

Question 3 (20 marks)

(a) Describe an n-bit binary *shift register* and explain how it is used to produce a pseudo-random binary sequence. What is meant by saying that a shift register is *primitive*? [6]

(b) State *Golomb's postulates*. Prove that the output of a primitive shift register satisfies Golomb's first postulate. State without proof whether it satisfies the other postulates. [7]

(c) Show that the shift register shown in the diagram below is primitive. What is the period of its output? (You may use theorems about shift register polynomials provided that you state them clearly.) [7]



Question 4 (20 marks)

(a) What is the *order* of x mod p, where p is a prime number not dividing x? [2]

(b) What is a *primitive root* of a prime number p? [3]

(c) Is 2 a primitive root of 61? [7]

(d) Explain carefully the operation of the *El-Gamal cipher*. On what hard problem does the security of this cipher depend? [8]

Question 5 (20 marks)

(a) Define *Carmichael's function* $\lambda(n)$. Give, without proof, a formula for $\lambda(n)$ in the case where n is the product of two distinct primes. [4]

(b) You are given that 14351 is the product of two distinct primes, and that $\lambda(14351) = 1008$. Use this information to factorise 14351. [5]

(c) You are given that the map $T_{11} : x \mapsto x^{11}$ mod 341 is equal to its own inverse on $\mathbb{Z}/(341)$. Use this information to factorise 341. (The marks for this question are for the method rather than the factorisation.) [5]

(d) Explain the relevance to the security of the RSA cipher of the fact that, if n is a product of two primes, then knowledge of $\lambda(n)$, or knowledge of an inverse pair $\{T_d, T_e\}$ of power maps, enables the factors of n to be found efficiently. [6]

Question 6 (20 marks)
Write an essay of approximately 500 words on *one* of the following topics:

(a) Quantum ciphers: are they unbreakable?

(b) The history of frequency analysis.

END OF EXAMINATION