Queen Mary
University of London

B. Sc. Examination 2006

MAS 335 Cryptography

Duration: 2 hours

Date and time: 8 May 2006, 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 $\mathbb{Z}/(n)$? Prove that there are exactly $n\phi(n)$ affine permutations of $\mathbb{Z}/(n)$, where ϕ is Euler's function. [6]

(b) Decrypt the following, which has been encrypted with an affine substitution cipher:

```
JKTW TRQH NXOS TRTV DIJL TDQC UHUD GTJQ OGHF UIT
```

[8]

(c) Why would it be better to use a random permutation instead of an affine permutation to encrypt a message? [3]

(d) Alice wants to encrypt a message using a substitution cipher, and thinks that she will make the cipher more secure by making sure that no letter is encrypted as itself. Is she right? Why? [3]

Question 2 (20 marks)

(a) Explain the difference between coding theory and cryptography. Are there any practical circumstances in which you might want to use both at once? [4]

(b) Encrypt the message 'this exam is too easy' with a Vigenère cipher, with the key 'hard'. [4]

(c) Is there any point in encrypting a message with a Vigenère cipher, and then encrypting the ciphertext again with another Vigenère cipher? Explain. [4]

(d) Explain briefly how you would break a Vigenère cipher, including how to find the length of the key. [4]

(e) Explain briefly how frequency analysis can be used to break a substitution cipher. [4]

Question 3 (20 marks)

(a) Define the term *Latin square* over an alphabet A. Explain how a Latin square can be used in conjunction with a random string over A to create a stream cipher. [6]

(b) State Shannon's Theorem for such a stream cipher. [3]

(c) Describe an n-bit binary shift register and explain how it can be used to produce a pseudo-random binary sequence. [4]

(d) Explain how to reconstruct the shift register, and hence the complete binary sequence, from any $2n$ consecutive bits of the sequence. Why does this make a shift register unsuitable as a replacement for a one-time pad? [7]

Question 4 (20 marks)

(a) Define Euler's phi-function $\phi(n)$, and show that if p is prime then $\phi(p^a) = p^{a-1}(p-1)$. State without proof a general formula for $\phi(n)$. Prove that if $\gcd(x,n) = 1$ then $x^{\phi(n)} \equiv 1 \bmod n$. Where does your proof break down if $\gcd(x,n) \neq 1$? [8]

(b) Explain briefly the operation of the RSA cryptosystem. [8]

(c) Show how RSA with modulus N can be broken if $\phi(N)$ is known. Illustrate by factorising 9167, given that it is a product of two primes and $\phi(9167) = 8976$. (The marks are for the method, not the factorisation.) [4]

Question 5 (20 marks)

(a) Explain the terms *plaintext*, *ciphertext*, and *key*, and illustrate them with an example. [4]

(b) Why is it important for a cipher to have a large number of potential keys? [2]

(c) Explain the concept of a *digital signature*. Give an instance of a situation in which it might be used in practice. Describe in detail an implementation of digital signatures, using a public-key cryptosystem of your choice. [10]

(d) Show how to compute $x^a \pmod b$ with at most $2\log_2 a$ multiplications and reductions modulo b. Illustrate by calculating $2^{101} \pmod{85}$ without a calculator. (Show your working.) [4]

Question 6 (20 marks)

(a) Explain Diffie–Hellman key exchange. On what hard problem does its security depend? [10]

(b) What is the knapsack problem? Explain the Merkle–Hellman public-key cryptosystem based on this problem. [10]

 END OF EXAMINATION