B. Sc. Examination 2005

MAS 335 Cryptography

Duration: 2 hours

Date and time: 6 May 2005, 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) Explain the difference between cryptography, steganography, and cryptanalysis. [3]

(b) Explain the terms *plaintext*, *ciphertext*, and *key*, and illustrate them in an example. [5]

(c) Decrypt the following, which has been encrypted with a Caesar cipher: [7]

```
YFND LTYN FFUN FLCU RNFF UTYL TBTY LTBZ
WRNF FUTY LTBT FLCU TYLT BNFF U
```

(d) Why is it important for a cipher to have a large number of potential keys? [5]

Question 2 (20 marks) Explain how the RSA public-key cryptosystem works. Your explanation should include a discussion of which problems are 'easy' and which are 'hard', and why, and the significance of this for security and for practical implementations.

Question 3 (20 marks)

(a) Explain how a substitution cipher works. [3]

(b) Illustrate by encrypting the text

```
Eve has found the key
```

with the substitution

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
T H E Q U I C K B R O W N F X J M P S V L A Z Y D G
```

[3]

(c) Explain briefly how a substitution cipher can be broken. [4]

(d) Alice and Bob wish to use the same substitution for both encryption and decryption. What property must the substitution have, considered as a permutation of the alphabet?

How many such substitutions are there of a 26-letter alphabet, assuming no letter is encrypted as itself? [You may leave your answer in factorised form, rather than multiplying it out.] [6]

(e) If Eve knows that the same substitution is used for both encryption and decryption, does it make her job of breaking the cipher any easier? Why? [4]

Question 4 (20 marks)

(a) Define the term *Latin square* over an alphabet A. [2]

(b) Prove that $n \times n$ Latin squares exist for every positive integer n. [5]

(c) Explain how a Latin square can be used in conjunction with a random string over A to create a stream cipher. [4]

(d) State precisely Shannon's theorem for such a cipher. [3]

(e) What two main problems can occur if the substitution table for a stream cipher is not a Latin square? (Give details.) [6]

Question 5 (20 marks)

(a) What is an n-bit binary shift register? Explain briefly how it may be described by a polynomial with coefficients in $\mathbb{Z}/(2)$. [4]

(b) Draw a diagram of the binary shift register corresponding to the polynomial $x^5 + x + 1$. [3]

(c) Calculate the next 5 bits of the sequence produced by this shift register following 01011. [3]

(d) Define the terms *irreducible* and *primitive* as applied to polynomials (or shift registers). [4]

(e) Determine (with proof) whether $x^5 + x + 1$ is (i) irreducible, (ii) primitive. [6]

Question 6 (20 marks)

(a) If p is a prime, what is a primitive root modulo p? Find a primitive root modulo 17. [4]

(b) Explain the *discrete logarithm problem*, and why it is thought to be hard. [5]

(c) Explain carefully the operation of the El-Gamal public-key cryptosystem. [8]

(d) Why is it important for the random exponent (or key) chosen by Alice to be truly random? [3]

 END OF EXAMINATION