Queen Mary
University of London

B. Sc. Examination by course unit

MTH6115 Cryptography SPECIMEN EXAM

Duration: 2 hours

Date and time:

Apart from this page, you are not permitted to read the contents of this question paper until instructed to do so by an invigilator.

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 4 questions answered will be counted.

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

Complete all rough workings in the answer book and cross through any work which is not to be assessed.

Candidates should note that the Examination and Assessment Regulations state that possession of unauthorized materials by any candidate who is under examination conditions is an assessment offence. Please check your pockets now for any notes that you may have forgotten that are in your possession. If you have any, then please raise your hand and give them to an invigilator now.

Exam papers must not be removed from the examination room.

Examiner(s): Bill Jackson

Question 1 (a) Explain the terms *plaintext*, *ciphertext*, and *key*, and illustrate them in an example. [6]

(b) State *Kerckhoff's Principle* for cryptography. Why is it reasonable to assume that it holds? [4]

(c) Decrypt the following, which has been encrypted with a Caesar cipher: [9]

```
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? [6]

Question 2 (a) Explain how a substitution cipher works. [5]

(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. [5]

(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.] [7]

(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? [5]

Question 3 (a) What is an n-bit binary shift register? Explain briefly how it may be described by a polynomial with coefficients in $\mathbb{Z}_2$. [5]

(b) Draw a diagram of the binary shift register corresponding to the polynomial $x^5 + x + 1$. [4]

(c) Calculate the next 5 bits of the sequence produced by this shift register following 01011. [4]

(d) Define the terms *irreducible* and *primitive* as applied to polynomials (or shift registers). [5]

(e) Determine (with proof) whether $x^5 + x + 1$ is (i) irreducible, (ii) primitive. [7]

Question 4 (a) Define the term *Latin square* over an alphabet A. [2]

(b) Explain how a Latin square can be used in conjunction with a random word over A to create a stream cipher. [6]

(c) State and prove Shannon's theorem for such a cipher. [10]

(d) Does Shannon's theorem hold if the stream cipher uses a substitution table which is not a Latin square? (Justify your answer.) [7]

Question 5 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. [25]

Question 6 (a) If p is a prime, what is a primitive root modulo p? Find a primitive root modulo 17. [5]

(b) Explain the *discrete logarithm problem*, and why it is thought to be hard. [6]

(c) Explain carefully the operation of the El-Gamal public-key cryptosystem. [10]

(d) Why is it important for the random exponent (or key) chosen by Alice to be truly random? [4]

End of Paper