THIS PAPER IS NOT TO BE REMOVED FROM THE EXAMINATION HALL

UNIVERSITY OF LONDON

CO3326 ZA

BSc EXAMINATION

COMPUTING AND INFORMATION SYSTEMS, CREATIVE COMPUTING and COMBINED DEGREE SCHEME

Computer security

Tuesday 7 May 2019: 10:00 – 12:15

Time allowed: 2 hours and 15 minutes

DO NOT TURN OVER UNTIL TOLD TO BEGIN

There are **FIVE** questions on this paper. Candidates should answer **THREE** questions. All questions carry equal marks, and full marks can be obtained for complete answers to a total of **THREE** questions. The marks for each part of a question are indicated at the end of the part in [.] brackets.

Only your first **THREE** answers, in the order that they appear in your answer book, will be marked.

There are 75 marks available on this paper.

A handheld calculator may be used when answering questions on this paper but it must not be pre-programmed or able to display graphics text or algebraic equations. The make and type of machine must be stated clearly on the front cover of the answer book.

Question 1

Alice and Bob would like to exchange encrypted messages. The message alphabet – for plaintexts as well as ciphertexts – consists of the 26 lower case letters from the English alphabet. The scheme they use goes as follows: the letters are first mapped to the $0...25$ interval ($a \rightarrow 0$, $b \rightarrow 1$, ..., $z \rightarrow 25$), then pairs of these numbers, arranged in sequence as column vectors, are multiplied *modulo* 26 by this matrix:

$$\begin{bmatrix} 3 & 4 \\ 4 & 5 \end{bmatrix}$$

(a) Demonstrate the encryption scheme on the following plaintext message:

understand

Show all your working. [6]

(b) What is the block size of this encryption scheme? With the aid of examples from the encryption above, explain the advantage of a block cipher over simple substitution ciphers. [5]

(c) Suppose Charles is eavesdropping on the conversation and he intercepts the above matrix. Explain how Charles could use this information to decrypt intercepted ciphertexts. Show all your working and provide a simple example. [9]

(d) Describe briefly the following key properties of a Block Cipher System and explain why they are important: **diffusion**, **confusion** and **completeness**. [5]

Question 2

Consider a 5-bit linear-feedback shift register (LFSR) with tap positions at bits 4 and 2.

(a) Demonstrate one step of this LFSR, with the aid of a schematic, starting from seed 11010. What is the corresponding equivalent recursive function that captures the functionality of this LFSR? [5]

(b) Give the first 30 bits of the keystreams generated for the seed 11010. Present your answer divided into consecutive blocks of five bits. After how many bits does the keystream start to repeat? [5]

(c) What is the frequency of the stream generated by seed 10010? How does it compare to the frequency of the stream generated by 11010, that you computed in (b)? Explain why. [5]

(d) Explain the following terms in the context of LFSRs: **feedback function**, **cycle**, and **maximal-length polynomial**. [5]

(e) What are the advantages and disadvantages of using a LFSR to implement a stream cipher? Your answer should cover **implementation**, **key exchange**, and **known-message attack**. [5]

Question 3

(a) Encrypted information is to be made accessible to ten company directors. Decryption requires a key K which has been divided into five pieces. Each director possesses one piece of the key and any three different key pieces are sufficient to reconstruct the key.

i. This protocol can be described as a t of n escrow: what are the values of t and n in this case? [2]

ii. Does this protocol allow any three directors to access the encrypted information by collaborating? Explain your answer. [2]

iii. It is later decided that any two directors should be able to collaborate to access the encrypted information. Describe how this may be achieved using the same escrow protocol if each director is given two different key pieces. [5]

(b) The prime number $p = 37$ is used as the modulus to generate three key pieces for a 2 of 3 key escrow scheme. Two of the key pieces are:

$$K_1 = (x_1 = 7, k_1 = 19)$$
$$K_2 = (x_2 = 26, k_2 = 3).$$

i. Find the value of the secret key K showing all your working. [7]

ii. Having the key K, find the random number a that generated the keys. Generate the third key piece given that $x_3 = 13$. [5]

(c) Explain how an n of n key escrow protocol works. [4]

Question 4

(a) State the **discrete logarithm problem** (DLP). In the context of El Gamal encryption, what does it mean that g is a *generator* for prime p? [4]

(b) Alice and Bob want to use the Diffie-Hellman key exchange protocol to generate a shared secret key. They have agreed to use prime number $p = 17$ with generator $g = 3$. Alice chooses the private key $a = 6$ and Bob chooses private key $b = 11$. What is the value of their shared secret key? Show all of your working. [5]

(c) Explain how you would generate a large – 100 decimal digits or longer – prime and a corresponding generator for secure El Gamal encryption. [6]

(d) Is $g = 2$ a generator for prime $p = 83$? [5]

(e) For each of the numbers 219, 221 and 223 prove that the number is prime or prove that it is composite. [5]

Question 5

(a) Give one strength and one weakness for each of the following passwords:

i. Isabella
ii. t7tE4%eK
iii. 2079197850.

[6]

(b) Give the key generation protocol for the RSA public key cryptosystem. [7]

(c) Alice has public RSA key $(e, n) = (13, 93)$. Encrypt the message $m = 7$ to be sent to Alice. Show all your working. [4]

(d) Show that $d = 37$ is the value of Alice's private key. [4]

(e) Explain how and why Alice and Bob might use RSA to exchange a key for use in a symmetric key cryptosystem. [4]

END OF PAPER