THIS PAPER IS NOT TO BE REMOVED FROM THE EXAMINATION HALL

UNIVERSITY OF LONDON

CO3326 ZB

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 ($a \to 0$, $b \to 1$, ..., $z \to 25$), then pairs of these numbers, arranged in sequence as column vectors, are multiplied *modulo* 26 by this matrix:

$$\begin{bmatrix} 2 & 5 \\ 3 & 7 \end{bmatrix}$$

(a) What is the block size of this encryption scheme? Encrypt the word *aqua*. Use the result of the encryption to explain the advantage of a block cipher over simple substitution ciphers. Show all your working. [7]

(b) Suppose Charles is eavesdropping on the conversation and he intercepts the above matrix. Is this useful information? Explain why. [6]

(c) Suppose Charles intercepts, in addition to the matrix, the following ciphertext:

t r y v v j n n u s

Explain how he can decrypt it. Show all your working. [8]

(d) Explain how you would adjust this scheme to allow for the encryption of lowercase English text of any length. [4]

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 10101. 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 10101. 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? What is the maximum frequency of this LFSR? Which seed generates a maximum frequency stream? Give an example for a 5 bit sequence that cannot be found in any stream that this LFSR generates. [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 mention **implementation**, **key exchange**, and **known-message attack**. [5]

Question 3

(a) Alice and Bob share Data Encryption Standard (DES) keys K_1, K_2 and K_3, and Alice wants to send a message M, to Bob using 3DES. State the steps Alice takes to encrypt and send the message. State the steps Bob takes to decrypt it. [6]

(b) Suppose in the i-th round of a DES-type encryption a block is separated into left and right halves which are, respectively, $L_i = 1100$ and $R_i = 1001$, where a block size of 8 is assumed for simplicity. Suppose the key $K_i = 1010$ is to be combined with R_i using XOR. Explain how the Feistel structure employed by DES will generate the block input for the next round of DES, and specify this input. [5]

(c) What is the output size of SHA-1? With a **brute force search**, how many evaluations of SHA-1 must be carried out on average to find a collision? Explain your answer. [4]

(d) In the context of hash functions, which is a bigger security issue:

i. being able to find arbitrary collisions, or

ii. being able to find collision with a specific message?

Explain why. [4]

(e) A hash function for a string of alphanumeric characters is proposed as follows:

For $i = 1$ to 6 record the number of characters until the i-th character is repeated for the final time; record 0 if no repeat is found.

For example, the string $EXCESSIVE$ would give the hash value 800510.

i. Give the hash value computed for the string $SUCCESS$. [2]

ii. Find a preimage for the hash value 710502 (it does not have to be a word in English). [2]

iii. State one strength and one weakness of this hash function. [2]

Question 4

(a) Show that 3 is a generator for prime 17. [6]

(b) Bob wants to send Alice a message encrypted using the El Gamal cryptosystem. The message is $m = 5$. Alice's private key is $(p, g, a) = (17, 3, 6)$. Bob's private key is $(p, g, b) = (17, 3, 11)$. What is the ciphertext? Show all your working. [5]

(c) How does Alice decrypt the ciphertext she received from Bob? Show your working. [4]

(d) Explain how you would generate a large – 100 decimal digits or longer – prime and a corresponding generator for secure El Gamal encryption. [5]

(e) Is $g = 2$ a generator for prime $p = 107$? [5]

Question 5

(a) A PDF file is encrypted by Alice before being sent by email to Bob. Bob requires the password to open the file. Identify **THREE** methods by which Alice might send the password to Bob, briefly discussing the strengths and weaknesses of each method. [6]

(b) Use Fermat's little theorem with base 2 to show that 119 is not a prime number. [6]

(c) Alice has public RSA keys $(e, n) = (11, 91)$. Encrypt the message $m = 12$ to be sent to Alice. Show all your working. [4]

(d) Suppose Charles wants to break Alice's key. Explain step by step what Charles will do to obtain her private key. [5]

(e) Explain how Alice could encrypt and sign a message for Bob. [4]

END OF PAPER