THIS PAPER IS NOT TO BE REMOVED FROM THE EXAMINATION HALLS

UNIVERSITY OF LONDON **CO3326 ZB**

BSc Examination

COMPUTING AND INFORMATION SYSTEMS, CREATIVE COMPUTING AND COMBINED DEGREE SCHEME

Computer Security

Friday 4 May 2018: 10.00 – 12.15

Time allowed: 2 hours and 15 minutes

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

A software development company has three development projects $D1$, $D2$ and $D3$. Access to code for three employees Alice, Bob and Charles is specified as follows:

Alice:	$D1$: execute access; $D2$: read access; $D3$: no access;
Bob:	$D1$: read and execute access;
	$D2$: read and write access; $D3$: no access;
Charles:	$D1$: no access; $D2$: read, write and execute access;
	$D3$: execute and write access.

(a) Present this information in the form of an *access control matrix.* [3]

(b) Suppose that read access to one of the projects allows direct access to the code while execute access only allows compiled code to be run. Do you think that having read access without execute access is inconsistent in terms of system security? Briefly explain your answer. [5]

(c) Suppose that Alice is promoted to the same company status as Bob and therefore has identical access rights. Present this as an access control matrix showing the relationship of subjects (Alice, Bob and Charles) to objects (the projects) with appropriate grouping of subjects. [5]

(d) A 2 of 3 escrow is to be generated for the key value $K = 16$. Using the prime $p = 19$ (which is assumed to be public) and the four random numbers $a = 11$, $x_1 = 5$, $x_2 = 7$, $x_3 = 9$, generate the three key pieces. Show your working. [4]

(e) Show how the key pieces computed in *(d)* can be combined to reconstruct the key value $K = 16$: X_1 and X_2, X_1 and X_3. [8]

Question 2

Alice and Bob intend to communicate securely using the RSA cryptosystem. Bob constructs his public key $(e, n) = (7, 65)$. Alice sends him a message consisting of the single number $m = 38$ which she encrypts using Bob's public key.

(a) What is Bob's private key? Show your working. [5]

(b) Explain in detail how Alice encrypts the message m to obtain the ciphertext c. [6]

(c) Explain in detail how Bob decrypts the ciphertext c sent to him by Alice to recover the message m. [4]

(d) Complete the following table of modular inverses $x^{-1} \bmod 14$ ('–' means no inverse exists).

x	1	2	3	4	5	6	7	8	9	10	11	12	13
$x^{-1} \bmod 14$	1	–											

[4]

(e) Use Euclid's Algorithm to find the inverse of $240 \bmod 17$. [6]

Question 3

(a) Show that $38^{220} \bmod 221 = 1$. [4]

(b) State Fermat's Little Theorem (FLT) concerning powers modulo prime numbers. Considering that the equation in (a) satisfies FLT, does this prove that 221 is prime? Explain your answer and show your working. [6]

(c) Consider a room with n people. What is the smallest n, for which the probability of two people having the same birthday is greater than 50% (*i.e.* it is more likely than not)? Show your working. Note: this is also referred to as the *Birthday Paradox*. Why is this relevant to cryptography? [7]

(d) 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]

(e) Explain why being able to find arbitrary collisions *i.e.* two arbitrary messages that result in the same hash, is not an immediate security issue. What if an attack was discovered that could be used to find a collision with a specific message? [4]

Question 4

Consider a generalised Caesar cipher: the letters of an alphabet of size m are first mapped to the integers in the range 0 ... $m-1$. Then modular arithmetic is used to transform the integer that each plain-text letter corresponds to. The encryption function for a single letter is $\mathrm{E}(x) = (ax + b) \bmod m$, where m is the size of the alphabet and a and b are the keys – integers – of the cipher. Consider that our alphabet consists of the lower case letters of the English alphabet – hence $m = 26$ – and we know that the cipher is deterministically invertible.

(a) What is the decryption function? [5]

(b) What are the restrictions on a? Why? What are the possible values of a? [5]

(c) The following ciphertext has been encrypted with a generalised Caesar cipher using $a = 11$ and $b = 13$:

a z o j s n j t f s

Decrypt it. Show all your working. [7]

(d) Describe briefly the following key properties of a Block Cipher System and explain why they are important: *diffusion*, *confusion* and *completeness*. Why should a block cipher have a *large blocksize*? Why should a block cipher have a *large keysize*? [8]

Question 5

The rule

$$(n+1)\text{-th bit} = n\text{-th bit} \oplus (n-4)\text{-th bit},$$

for $n \geq 5$, is used to generate a keystream using an initial key K consisting of five bits. Two initial keys are:

$$K1 = 11100 \text{ and } K2 = 11010.$$

(a) Give the first 25 bits of the keystreams generated for the initial keys $K1$ and $K2$. Present your answers divided into consecutive blocks of five bits. After how many bits do the keystreams start to repeat? [5]

(b) Suppose a message is encrypted using the keystreams generated by keys $K1$ and $K2$. Explain briefly why the keystream produced by $K1$ is more vulnerable to attack than that produced by $K2$. Illustrate your answer by supposing that each alphabet letter of the message is represented by a 5-bit block in the plaintext, and that the message to be encrypted begins with the letter 'E'. [5]

(c) What is the maximum number of bits that a keystream generated by this rule may contain before the keystream begins to repeat? Give an example of a 5-bit key which achieves this maximum. Why is this key not a good choice for generating a keystream? [5]

(d) A combined keystream is produced by XOR-ing $K1$ and $K2$ to get $K1 \oplus K2$. Is this combined keystream safer against attack than $K2$ used on its own? Explain your answer. [5]

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

END OF PAPER