THIS PAPER IS NOT TO BE REMOVED FROM THE EXAMINATION HALLS

UNIVERSITY OF LONDON **CO3326 ZA**

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

Consider a generalised Caesar cipher: the letters of an alphabet of size m are first mapped to the integers in the range $0 \ldots m-1$. 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) Why is this a generalised Caesar cipher? [2]

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

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

(d) The following ciphertext has been encrypted with a generalised Caesar cipher using $a = 7$ and $b = 15$:

l t v z o p s t j c

Decrypt it. Show all your working. [7]

(e) What is a block cipher? What is the purpose of *diffusion* and *confusion* in the design of block ciphers? [6]

Question 2

Alice and Bob intend to communicate securely using the RSA cryptosystem. Bob constructs his public key (e, n) using the two primes $p = 5$ and $q = 13$ and the value $e = 7$. Alice sends him a message consisting of the single number $m = 38$ which she encrypts using Bob's public key.

(a) What are the values in Bob's public and private keys? [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) Write out a table of modular inverses modulo 11, *i.e.* $(x - 1) \bmod 11$. [4]

(e) Use Euclid's Algorithm to find the inverse of $25 \bmod 302$. [6]

Question 3

(a) State Fermat's Little Theorem concerning powers modulo prime numbers and explain how it can be used for primality check. [5]

(b) Use Fermat's Little Theorem with base 4 to show that 121 is not a prime number. [5]

(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) In the context of cryptographic hash functions, briefly explain the following notions:

i. *fingerprint*

ii. *collision resistance*

iii. *second pre-image resistance*

iv. *determinism*.

[8]

Question 4

In a secure system based on the Bell-LaPadula model, four subjects and three objects are distinguished, with given security levels as shown:

Subject	Level
S1	2
S2	1
S3	3
S4	2

Object	Level
O1	1
O2	2
O3	3

The actions which the subjects may perform on the objects are specified in the following access table:

	S1	S2	S3	S4
O1	r	rwx	rx	rw
O2	rx	rx	rx	rw
O3	r	–	rwx	–

(a) What does the entry rwx mean? Explain what *no read-up* and *no write-down* mean in this context, and why they are important. [3]

(b) Why might the *no write-down* policy make interaction difficult between S1 and S2, and how does the Bell-LaPadula model allow for this difficulty? [4]

(c) Identify **THREE** cases in which the access table violates the rules of Bell-LaPadula and explain why they constitute violations. [6]

(d) A 2 of 3 escrow is to be generated for the key value $K = 14$. Using the prime $p = 17$ (which is assumed to be public) and the four random numbers $a = 7$, $x_1 = 4$, $x_2 = 5$, $x_3 = 9$, 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 $K = 14$: X_1 and X_2, X_1 and X_3. [8]

Question 5

Alice and Bianca intend to communicate securely by exchanging a secret key using the El Gamal cryptosystem. Conrad, who is eavesdropping on their exchange, intercepts the following values:

$$p = 283$$
$$g = 12$$
$$A = 77$$
$$B = 46.$$

He assumes that (p, g, A) is Alice's public key and (p, g, B) is Bianca's public key.

(a) State the condition that must be satisfied for g to be a *generator* for prime $p = 283$. Write a function in pseudocode that tests whether g is a generator for p. [5]

(b) Assume you are Conrad. Break Alice's and Bianca's keys. Show all your working. [6]

(c) Show how Alice and Bianca compute the shared key using the private keys they generated, which have been broken by Conrad in point (b). [4]

(d) Explain briefly the concepts: *one-way function*, *one-way hash function* and *trapdoor one-way function*. [6]

(e) Describe briefly how a one-way hash function may be used for message authentication. [2]

(f) Explain why a stream cipher fails to protect message integrity. [2]

END OF PAPER