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

Date and Time: Thursday 4 May 2017 : 10.00 – 12.15

Duration: 2 hours 15 minutes

There are FIVE questions in 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 hand held 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

The *affine cipher* is a type of mono-alphabetic substitution 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 of the cipher. Consider that our alphabet consists of the 26 letters $m = 26$ 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 an affine cipher using $a = 3$ and $b = 1$:

KROBIKGAJLU

Decrypt it. Show all your working. [7]

(d) What is the relationship between the Affine cipher and the Caesar cipher? [2]

(e) How would you go about decrypting a ciphertext message that you intercepted, if you knew that it had been written in English and encrypted using a simple substitution cipher? Explain it with examples. When would you use an exhaustive search technique? [6]

Question 2

(a) Explain briefly in simple words the *Elliptic Curve Discrete Logarithm Problem (ECDLP)*. [3]

(b) Consider the following elliptic curve E: $y^2 = x^3 + 2x + 3$ over the prime field F_{19} and point $P = (1, 5)$. Compute $2 \cdot P = P + P = (1, 5) + (1, 5) = (x_3, y_3)$. [7]

(c) Give the four properties that a hash function should satisfy in order to be considered cryptographically strong, explaining the importance of each. [8]

(d) Consider the following scenario: a cloud storage provider *CloudS* charges you to store backups of your files. You intend to keep copies of your files on your own machine, so the copies stored with *CloudS* are just for backup, in case your local copies get damaged. *CloudS* would like to destroy your files because they take up a lot of space and are of no value to them. However they would like to continue to be paid for storing the files. You want to be able to perform some kind of check (as many times, and whenever *you* choose) to ensure that *CloudS* still has the complete versions of your files.

The files are too large for you to insist on seeing entire copies, instead you must use a protocol involving a hash function.

Design such a protocol and explain why your protocol ensures that *CloudS* cannot trick you believing that they still store your files when they actually do not. [7]

Question 3

(a) Use Fermats little theorem with base 2 to show that 91 is not a prime number. [6]

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

(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) Show that $d = 59$ is the value of Alice's private key. [4]

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

Question 4

(a) 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 given below. Find the value of the secret key K showing all your working.

$$K_1 = (x_1 = 11, k_1 = 31)$$
$$K_2 = (x_2 = 8, k_2 = 13)$$

[7]

(b) Explain how an n of n key escrow protocol works. Why is an n of n key escrow protocol rarely used in the real world? [6]

(c) The key size for DES is 56 bits. Explain how 3DES uses the DES algorithm with a 168-bit key. [4]

(d) Suppose in the i-th round of a DES-type encryption a block is separated into left and right halves which are, respectively, $L_i = 0110$ and $R_i = 1110$, where a block size of 8 is being assumed for simplicity. Suppose the key $K_i = 0101$ 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. [6]

(e) The key size for Rijndael can be either 128, 192 or 256 bits. Why does Rijndael allow different key sizes to be used? [2]

Question 5

(a) Alice and Bob intend to communicate securely using the El Gamal cryptosystem. Bob constructs his public key (p, g, y) where $p = 11$, $g = 6$ and $y = g^a \bmod p$, with $a = 4$ also forming the third part of his private key (p, g, a). Alice sends him a message consisting of the single number $m = 5$ which she encrypts using Bob's public key.

i. Show that $g = 6$ is a generator for the prime $p = 11$. [3]

ii. Explain in detail how Alice, choosing the random value $k = 3$, will encrypt the message m to obtain a ciphertext pair (r, c). [6]

iii. Explain in detail how Bob decrypts the ciphertext pair sent to him by Alice to recover the message m. [6]

(b) Describe the *Needham Schroeder* key management protocol, that involves key exchange using a trusted third party (TTP). [5]

(c) A **PGP** (Pretty Good Privacy) message, which has been encrypted and signed, includes the following additional data next to the payload:

- A signature component (timestamp + hash of the message and timestamp + first part of the message + key identifier of sender's public key),
- The session key component (encrypted session key + key identifier for the recipient's public key).

For both of these two components, explain why they are required. [5]

END OF PAPER