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

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

(a) 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 secret key $a = 6$ and Bob chooses secret key $b = 11$. What is the value of their shared secret key? Show all of your working. [6]

(b) Name and describe a method of key management that involves using a trusted third party (TTP). [5]

(c) Describe the web of trust model used for key management in PGP, and which does not involve the use of a TTP. Give one advantage and one disadvantage of the web of trust model compared with the method that you have described in point *(b)*. [6]

(d) Describe the no-read up and no-write down rules enforced in the secure multi-user Bell-LaPadula model. [4]

(e) Explain why strict enforcement of the no-read up and no-write down rules could cause a problem for users of a system implementing the Bell-LaPadula model, and how Bell-LaPadula overcomes this problem. [4]

Question 2

(a) Use Fermats little theorem with base 2 to show that 93 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 $(e, n) = (13, 93)$. 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]

Question 3

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 ... $m-1$. Then modular arithmetic is used to transform the integer that each plain-text letter corresponds to. The encryption function for a single letter is $\mathsf{E}(x) = (ax + b) \bmod m$, 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 $a = 5$ and $b = 8$:

IHHWVCSWFRCP

Decrypt it. Show all your working. [7]

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

(e) A block cipher can be used in different modes. Three of these are Electronic Codebook Mode (ECB), Cipher Block Chaining Mode (CBC) and Output Feed-Back Mode (OFB). Briefly explain the differences between these three modes of operation. [6]

Question 4

(a) 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]

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

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

[7]

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

i. *fingerprint*

ii. *collision resistance*

iii. *second pre-image resistance*

iv. *determinism.*

[8]

(d) Suppose m is a positive integer. For the following two functions $H(m)$ give reasons why these are not suitable for use as cryptographically strong hash functions:

i. $H(m)$ is defined to be $m \bmod d$ where d is the first nonzero decimal digit of m (so, for example, if $m = 302$ then $H(m) = 302 \bmod 3 = 2$);

ii. $H(m)$ is defined to be the m-th prime number (so, for example, if $m = 4$ then $H(m) = 7$).

[4]

Question 5

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

(b) Consider the following elliptic curve E: $y^2 = x^3 + 2x + 2$ over the prime field F_{17} and point $P = (5, 1)$. Compute $2 \cdot P = P + P = (5, 1) + (5, 1) = (x_3, y_3)$. [7]

(c) Features that a good security system might provide include: confidentiality, integrity, availability, non-repudiation, authentication, access controls and accountability. For each, write a sentence explaining the purpose of the feature. [7]

(d) Answer the following questions related to hash functions and provide brief explanations for your answers:

i. Contrast MD-5 and SHA-1 in terms of efficiency, security and complexity.

ii. Can a Message Authentication Code (MAC) provide non-repudiation?

iii. Can a MAC provide authentication?

iv. Can hash functions be used in Output Feedback (OFB) mode? If so, what would be the advantage of this?

[8]

END OF PAPER