THIS PAPER IS NOT TO BE REMOVED FROM THE EXAMINATION HALLS

UNIVERSITY OF LONDON **291 0326 ZB**

BSc Examination
for External Students

COMPUTING AND INFORMATION SYSTEMS AND CREATIVE COMPUTING

Computer Security

Dateline: Wednesday 13 May 2009 : 2.30 – 4.45 pm

Duration: 2 hours 15 minutes

Candidates should answer any **THREE** of the following five questions

Full marks will be awarded for complete answers to **THREE** questions. Each question carries 25 marks. The marks for each part of a questions are indicated at the end of the part in [ ] brackets. 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, texts or algebraic equations. The make and type of machine must be stated clearly on the front cover of the answer book.

Question 1

(a) A security system will typically provide one or more of the following features:

- confidentiality,
- non-repudiation,
- availability.

i. For each of the three features listed above, give an example of a situation where the listed feature is more important than the others. Justify your answers.

[6]

ii. State **three** further features that may be offered by a security system

[3]

(b) A bank has approximately 10,000 employees. In order to use the bank computer system, each employee has a unique username and a password. New employees are issued with their username which is made up of their first and last name and a randomly generated password

If a new employee has the same name as an existing employee, the username has a digit appended to distinguish the employees. Thus if there are three people working for the bank called John Smith, their usernames would be John Smith, John.Smith2 and John Smith3 respectively.

At their first log-in, employees must enter their username and initial password. They are then forced to immediately change the password by entering a password of their own choice two times.

Explain why:

i It is important that each employee has a unique username.

[2]

ii New employees are issued with an initial password.

[2]

iii Employees are forced to change their initial password immediately on their first log-in

[2]

iv Employees have to enter their new password twice.

[1]

(c) The system can insist on each employee having a unique username. One of the system administrators thinks that unique passwords should also be used. He suggests that if an employee tries to set a password which is already in use in the system, then the system should inform the user and ask them to choose a different password.

i. Explain why this method of notifying the employee is a potential security issue.

[3]

ii. If passwords are not unique, how could an attacker who got hold of the encrypted password file exploit this to his advantage?

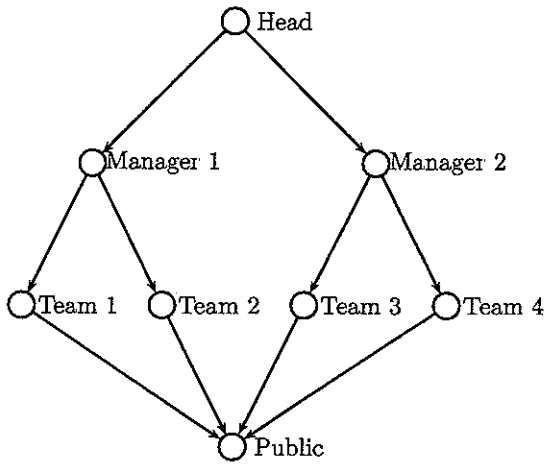
[3]

iii Explain how password salting could be used to ensure that an attacker will not be able to tell by looking at the encrypted password file that two passwords are the same.

[3]

Question 2

Below is a lattice graph showing the security levels of the staff in a large organisation.



(a) What are the properties of a lattice? You may refer to the given diagram to illustrate your answer.

[4]

(b) What is the *least upper bound* and the *greatest lower bound* for *Manager 1* and *Team 3*?

[2]

(c) i. A new security level, *Finance*, is to be added such that *Finance* is directly under *Head* and *Team* is directly under *Finance* for all four *Team* vertices. Copy the figure and add in the *Finance* security level in the appropriate position.

[2]

ii. Find in the resulting graph a pair of vertices which do not have a least upper bound.

[1]

iii. Explain why this could be a problem in terms of accountability.

[2]

(d) *Team 1* and *Team 4* are in different physical locations. Eavesdropping can happen on the telephone and data network between *Team 1* and *Team 4*. The data network is also subject to interruption, interception and modification by an active attacker.

i. Design a protocol for the secure transfer of **paper information** between *Team 1* and *Team 4* ensuring confidentiality and detection of any interruption.

[4]

ii. Design a protocol for the secure transfer of **electronic information** between *Team 1* and *Team 4*. You may refer to existing cryptographic protocols, but should not assume the pre-existence of any cryptographic keys. Explain why each step of your suggested protocol is important.

[10]

Question 3

(a) What is the purpose of encryption?

[2]

(b) What is meant by *perfect secrecy*?

[2]

(c) Explain how a *one-time pad* be used to achieve perfect secrecy.

[5]

Following is a simple method for the encryption of upper case letters.

- As in table 1, each letter A,B,C,...,Z is associated with a number 1,2,3,...,26. The space character is associated with number 0.

Character	space	A	B	C	D	E	F	G	H	I	J	K	L	M
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Character		N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Number		14	15	16	17	18	19	20	21	22	23	24	25	26

Table 1: Encoding for upper case letters

- A message (the plaintext) is a stream of upper case letters and spaces.
- A key is a stream of upper case letters and spaces. The key may be random or it may be a word or phrase.
- The message is encrypted by adding, character by character starting with the leftmost character, the value of the message character and the value of the key character modulo 27, and then converting the resulting value back into a upper case letter (or space).
- If the message is longer than the key, the key is repeated as many times as necessary in order to encrypt the entire message.

For example, the *message* **THE DOOR IS OPEN** encrypted with the *key* **COMPUTERS** results in the *ciphertext* **WWRPYHTISLGMDJYS**. This is illustrated in table 2.

plaintext	T	H	E		D	O	O	R		I	S		O	P	E	N
key	C	O	M	P	U	T	E	R	S	C	O	M	P	U	T	E
ciphertext	W	W	R	P	Y	H	T	I	S	L	G	M	D	J	Y	S

Table 2: Encryption using ECB mode

(d) Write the corresponding method for decryption of ciphertexts and hence decrypt the ciphertext **EFUEJ** using the key **SECURITY**.

[6]

(question continues on next page)

The encryption shown in table 2 is an example of a simple block cipher in *electronic codebook mode* or ECB. The blocks (in this case single characters) are each encrypted independently of the other blocks. To use the block cipher in *cipherblock chaining mode* or CBC, the value of the previous ciphertext block is added to the next message block as well as the key value. This mode of operation is used to encrypt the message in table 3. As before, all additions are modulo 27. The CBC key is initially set to *space* and subsequently is equal to the previous ciphertext value.

plaintext	T	H	E		D	O	O	R		I	S		O	P	E	N
key	C	O	M	P	U	T	E	R	S	C	O	M	P	U	T	E
CBC key		W	S	J	Z	X	E	Y	G	Z	K	R	D	H	R	P
ciphertext	W	S	J	Z	X	E	Y	G	Z	K	R	D	H	R	P	H

Table 3: Encryption using CBC mode

(e) Discuss the security of the two different modes considering the two cases:

- The message is shorter than the key;
- The message is longer than the key

[10]

Question 4

125, 190, 145, 87, 175, 64, 40, 25, 157, 78

From the list of numbers given above, select the number which matches each of (a) to (g). Full marks will not be awarded unless you show your working. Note that in some cases you may have to use trial and error in order to find the correct solution without having to find a modular inverse.

(a) The public key that corresponds to the RSA private key ($n = 989, d = 325$) given that p and q are 43 and 23 respectively.

[5]

(b) The signature of the message $m = 30$ signed using the RSA private key ($n = 989, d = 325$).

[4]

(c) The public key, e, that corresponds to the El Gamal private key ($p = 97, g = 5, d = 12$).

[4]

(d) The plaintext which corresponds to the ciphertext ($r = 53, c = 71$) when the ciphertext is decrypted using private El Gamal key ($p = 97, g = 5, d = 12$)

[5]

(e) The total number of keys required for 20 people to communicate with each other using a symmetric key cryptosystem.

[2]

(f) The total number of keys required for 20 people to communicate with each other using an asymmetric cryptosystem.

[2]

(g) The approximate number of seconds it will take to calculate a modular exponentiation using numbers of size 1000 bits, if the same package takes 1.4 seconds to calculate a modular exponentiation using numbers of size 200 bits.

[3]

Question 5

(a) State the discrete logarithm problem and give suitable parameter sizes, and any other conditions on the parameters, that are required in order to make the discrete logarithm problem a cryptographically secure one-way function.

[5]

Following is the Diffie-Hellman key exchange protocol used by Alice and Bob to exchange a secret key k. They have already agreed upon the values of p and g.

	Alice	Bob
1.	generates a	generates b
2.	computes $x = g^a \bmod p$	computes $y = g^b \bmod p$
3.	send x to Bob	send y to Alice
4.	computes $k = y^a \bmod p$	computes $k = x^b \bmod p$

(b) Explain why the Diffie-Hellman protocol is secure even if an eavesdropper learns the values of p, g, x and y. State any assumptions that you have made about the parameters.

[4]

(c) Alice and Bob have agreed to use parameter values $p = 211$ and $g = 2$. Bob has generated key $b = 79$ and receives the value $x = 9$ from Alice. Showing all your working, calculate the value of the key that Alice and Bob will share.

[6]

(d) An attacker, Charles, intercepts the values of x and y sent between Alice and Bob and replaces both of these with the value 1 before forwarding them to their intended recipients. How does this attack help Charles to decipher messages sent by Alice and Bob using their secret shared key k?

[3]

(e) To counter the attack described in part (d), Alice and Bob add a step into the Diffie-Hellman protocol to ensure that the value of y or x that they respectively receive is not equal to 1. Explain how Charles can still manipulate the protocol to his advantage by performing a man-in-the-middle attack.

[7]

END OF EXAMINATION