UNIVERSITY OF LONDON   **291 0326 ZA**

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.

UL09/920

Question 1

(a) An on-line magazine can be accessed by subscribers who pay a small annual subscription fee. The magazine takes an on-line credit card payment for the subscription fee. Once the payment has been authorised, the subscriber is sent an e-mail to an e-mail address that they have provided. The e-mail contains a link to a website where subscribers can register by choosing a username and password. Once they have completed this initial registration process, subscribers can access the on-line magazine at any time for a period of one year, by providing their username and password.

    i A security system will typically provide one or more of the following features: confidentiality, integrity, availability, non-repudiation, authentication, access control and accountability

    Which of these security features should the magazine consider when designing their on line site? Which features are the most important and which are the least important?

[9]

    ii When subscribers register their new password they are asked to enter it two times to ensure that it is typed correctly and thus reduce the possibility of access control errors.

    Give **five** further examples of features that could be included in the design of the username/password log-in page in order to enhance the security of the website. The features that you suggest may relate to the interface or the system itself.

[5]

(b) A hacker has a dictionary of 10,000,000 words. He knows that passwords in a particular system are of the form *word_digit*, for example *banana7* or *carrot3*. The hacker writes a program to test all of the words in his dictionary by making them into the correct *word_digit* form.

    i How many passwords will the hacker have to test in order to try **all** of the possible passwords?

[2]

    ii How long will the hacker spend on average to find a password that is included in the keyspace he is testing if he can test 1,000 passwords per second?

[3]

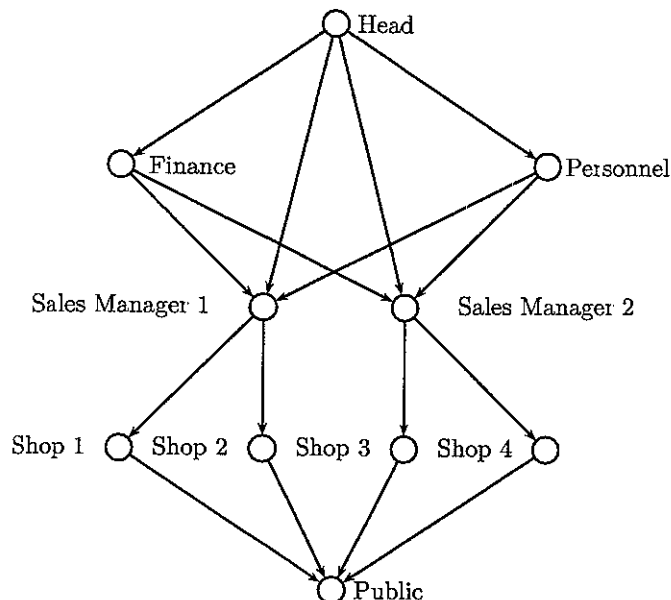(c) In your opinion, is it better for a company to insist that

    • passwords are 8 characters long and may contain any upper or lower case letter or digit;
    or
    • passwords are 7 characters long and must contain at least 2 digits

    Explain your answer

[6]

Question 2

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

(a) i. What are the properties of a lattice?

[4]

   ii. Explain why the graph above is not a lattice.

[2]

(b) i. A new security level, *Head of Sales*, is to be added such that *Head of Sales* is directly under *Finance, Head* and *Personnel* and *Sales Manager 1* and *2* are directly under *Head of Sales*. Copy the graph and add in the *Head of Sales* security level in the correct position

[2]

   ii. Is the graph drawn in part (b)i. a lattice?

[1]

   iii. Using equality symbols $>, \geq, =$ as appropriate, list all of the security levels in the (b)i. graph in hierarchical order starting with *Head*

[2]

(c) i. The shops are jewelery shops. A very valuable package of diamonds has to be transferred from Shop 1 to Shop 4. Design a protocol for the secure transfer of the diamonds.

[4]

   ii. Design a protocol for the secure transfer of **electronic information** between the Finance office and the Head office, assuming that these are in different physical locations. You may refer to existing cryptographic protocols, but should not assume the pre-existence of any cryptographic keys. Assume that eavesdropping can happen on the phone and data network and that the data network is also subject to interruption, interception and modification by an active attacker. Explain why each step of your suggested protocol is important.

[10]

Question 3

(a) Copy the following sentences about cryptography filling in the gaps using words from the list:

cipher	decipher	coding	decoding
the ciphertext	the plaintext	key space	key size
confidentiality	encryption	decryption	block size
the encryption key	the decryption key	the encryption algorithm	the decryption algorithm
a secure	an insecure	message space	statistical analysis
exhaustive search	dictionary search	intelligent search	substitution cipher

   i The purpose of . . is to transform a message, also called . . into an unreadable form called
. . . .

   ii. The sender Alice uses   chosen from . . and applies . . in order to produce . . .

   iii. Encrypted messages can be transmitted over . . channel whilst still maintaining . . . .

   iv The receiver Bob uses . . which corresponds to . . used by Alice in order to . . the . . and
retrieve the . . .

   v. It is important to have a large . . in order to prevent . . . .

[5]

(b) It is a desirable property that the encryption and decryption algorithms used in a cryptosystem
are the same.

   i Explain why this is a desirable property for a cryptosystem

[4]

   ii. Give an example of a *symmetric key cryptosystem* and an *asymmetric key cryptosystem*
which have this property

[2]

(c) 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.

(question continues on next page)

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 key COMPUTERS

i. Write the corresponding method for decryption of ciphertexts and hence decrypt the ciphertext **KMXNRRM** using the key **SECURITY**

[7]

ii. Discuss the security of this method of encryption considering the two cases:
- The message is shorter than the key;
- The message is longer than the key.

[7]

Question 4

70, 437, 29, 75, 32, 96, 35, 595, 60, 292

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 calculating a modular inverse.

(a) The public key that corresponds to the RSA private key $(n = 989, d = 425)$ given that p and q are 43 and 23 respectively

[5]

(b) The signature of the message $m = 12$ signed using the RSA private key $(n = 989, d = 425)$.

[4]

(c) The public key, e, that corresponds to the El Gamal private key $(p = 97, g = 5, d = 13)$.

[4]

(d) The plaintext which corresponds to the ciphertext $(r = 27, c = 93)$ when the ciphertext is decrypted using private El Gamal key $(p = 97, g = 5, d = 13)$.

[5]

(e) The total number of keys required for 35 people to communicate with each other using a symmetric key cryptosystem.

[2]

(f) The total number of keys required for 35 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 1200 bits, if the same package takes 1.5 seconds to calculate a modular exponentiation using number of size 300 bits.

[3]

Question 5

(a) Describe the Diffie-Hellman key exchange protocol. Your answer should include but is not limited to:
- Details of any parameters required and conditions that these parameter should satisfy.
- The steps that Alice and Bob should take in order to exchange a secret key K.
- The name of the one-way function that is used as the basis for the security of the protocol.
- An analysis of the security of the key exchange protocol assuming that the transmissions between Alice and Bob can be overheard but not modified or interrupted.

[10]

(b) A simple attack on the Diffie-Hellman protocol is for an interceptor Charles to replace the values sent between Alice and Bob with the value 1.

i. What is the value of the shared key K if this attack is successful?

[2]

ii. Suggest changes to the protocol which would prevent this attack from succeeding

[2]

(c) A more sophisticated attack is the man-in-the-middle attack. Charles chooses a secret value c for himself, intercepts the values sent from Alice to Bob and Bob to Alice, and performs the Diffie-Hellman protocol himself with each of them. Now Charles shares a secret key K_{AC} with Alice and a secret key K_{BC} with Bob. Alice and Bob both think that they are communicating securely with each other when in fact all of their messages can be decrypted, read, modified and forwarded by Charles. This attack is illustrated in the table below.

Alice	Charles	Bob
Chooses a	Chooses c	Chooses b
Computes x	Computes z	Computes y
Sends x to Bob	Intercepts x, replaces it with z and sends it to Bob	Sends y to Alice
	Intercepts y, replaces it with z and sends it to Alice	
Receives z from Charles (but thinks it is y from Bob)		Receives z from Charles (but thinks it is x from Alice
Computes K_{AC}	Computes K_{AC} Computes K_{BC}	Computes K_{BC}

Suppose Alice and Bob have agreed to use prime $p = 211$ and generator $g = 2$. Charles knows the values of p and g and chooses the value $c = 10$ for himself. Charles intercepts the values $x = 5$ sent from Alice to Bob and $y = 132$ sent from Bob to Alice.

i. What is the value of z that Charles should send to Alice and Bob in place of the ones he has intercepted?

[2]

ii. What is the value of the key K_{AC} that Charles shares with Alice?

[2]

iii. What is the value of the key K_{BC} that Charles shares with Bob?

[4]

iv. Suggest changes to the protocol which would prevent this attack from succeeding.

[3]

END OF EXAMINATION