UNIVERSITY OF LONDON

291 0326 ZA

FOR EXTERNAL STUDENTS - WESTERN

B.Sc. Examination 2008

COMPUTING AND INFORMATION SYSTEMS

CIS326 Computer Security

Duration: 2 hours 15 minutes

Date and Time: Friday 16 May 2008 : 2.30 – 4.45 pm

Answer any **three** of the following five questions.

Full marks will be awarded for complete answers to a total of three questions. Each question carries 25 marks. The marks for each part of a question 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, text or algebraic equations. The make and type of machine must be stated clearly on the front cover of the answer book.

THIS EXAMINATION PAPER MUST NOT BE REMOVED FROM THE EXAMINATION ROOM

1. The charity *CryptoAid* is run by six committee members. On the committee there is the chairman, treasurer, secretary and three other committee members. The committee meets every three months to discuss how money for the charity should be raised and spent. The committee tries to make decisions by majority vote amongst themselves with no member of the committee having a greater weight than any of the others. *CryptoAid* has a bank account and the treasurer keeps the accounts. The treasurer presents a copy of the accounts to all of the committee members at each meeting. The treasurer, chairman and secretary are all authorised signatories for the bank account. Any one of the signatories can get statements or pay money into the bank account. To withdraw money from the bank account, any two of the signatories must sign a cheque.

   (a) Identify the *subjects* and *objects* in the scenario described above.

   [4]

   (b) Describe a *protection ring* access control structure and explain why a protection ring is not a suitable structure to model the subjects identified in the CryptoAid scenario.

   [4]

   (c) At a particular committee meeting, it is decided that a committee member called Frank should become a fourth authorized signatory for the CryptoAid bank account. Write a protocol for adding Frank onto the list of authorised signatories held by the bank. The aim of the protocol is to ensure that it is impossible for anyone to become a signatory for the bank account without the proper authorisation and verification.

   [8]

   (d) Now there are four authorised signatories and any two of them have to sign a cheque to withdraw money from the bank account. This is a basic 2 of 4 key escrow scheme. Why is this scheme arguably less secure than a key escrow scheme based on a mathematical formula?

   [1]

   (e) The CryptoAid committee want to increase security and so decide to implement a 2 of 4 key escrow scheme based on the solution of simultaneous equations mod a prime number. Explain how the keys for each key holder are generated.

   [4]

   (f) Given that the keys held by the treasurer and chairman are ($x_1 = 7, k_1 = 14, p = 17$) and ($x_2 = 3, k_2 = 11, p = 17$) respectively, find the shared key K.

   [4]

2. (a) i. Describe the key generation protocol for the RSA public key cryptosystem.

[7]

ii. Suppose that an algorithm is found that can efficiently factorise a large number. Explain how a cryptanalyst could use this algorithm to break the RSA cryptosystem.

[3]

(b) Following is a simple method for blocking and encoding upper case letters for encryption.

- Group letters into blocks of two starting at the leftmost letter. Add a space character at the rightmost side if necessary to make an even number of characters.
- Encode letters using $A = 1$, $B = 2$, ..., $Z = 26$, space $= 0$.
- Convert each block of two characters into a single decimal number by multiplying the value of the first character by 27 and then adding the value of the second character.

Thus the word STARS is partially encoded as follows:

characters	S	T	A	R	S *space*
character values	19	20	1	18	
block value	19(27)+20 =533				

i. Copy and complete the table above. Then using the RSA public keys ($n = 799, e = 3$) encrypt the word STARS.

[5]

ii. Suppose we want to include both lower case and upper case characters in our messages. Suggest changes that have to be made to the key and encoding method that would enable this. (Keep two characters per block).

[4]

iii. Instead of changing the key, it is suggested that messages are encrypted character by character. Under this scheme, the word stars is encrypted to (39,657,507,490,39). Decrypt the word (39,657,507,490,657) and hence or otherwise explain why encrypting character by character is a bad idea.

[6]

3. The Needham-Schroeder Protocol can be described symbolically as follows:

A $\rightarrow$ S: A,B

S $\rightarrow$ A: $e_{K_{AS}}(B, K_{AB}, e_{K_{BS}}(A, K_{AB}))$ A decrypts

A $\rightarrow$ B: $e_{K_{BS}}(A, K_{AB})$ B decrypts

(a) Explain each step of the protocol in words.

[7]

(b) Adapt the protocol given above so that it prevents another person replaying a message. Explain how the modifications you have made work.

[6]

(c) Alice and Bob are using the Needham-Schroeder Protocol to communicate with each other. A cryptanalyst Charles has access to all of the communications between Alice and Bob.
Explain why this is not a security problem.

[4]

Charles now gets hold of Bob's key K_{BS}. What can Charles do now? What should Bob do when he discovers that his key has been compromised?

[8]

4. (a) Consider the following three mappings where x is a binary number of arbitrary length.

$f(x) = x \oplus$ the current air temperature in degrees Centigrade

$g(x) = x \bmod 2^{64}$ (i.e. the least significant 64 bits of x)

$h(x)$=SHA-1(x)

i. Of the above, which is a cryptographic hash function, which is a hash function, and which is not a proper function?

[3]

ii. Why is the hash function identified in part (i) unsuitable for use in a cryptographic protocol?

[4]

iii. Describe the SHA-1 protocol.

[6]

(b) KeepitSafe Ltd has designed two vaults with electronic locks. The vaults open only after the correct decimal code has been entered. Version A is a low cost model which expects an 8-digit code. After all eight digits have been entered, it will either open or will signal that the code was wrong and remain locked. Version B is a far more secure version which expects a 32-digit code.

i. Explain why some companies may prefer to use version A even though version B is many times more secure.

[4]

To overcome the problems associated with version B, KeepitSafe introduce a modification. Version B2 still expects a 32-digit code but after every 4-digits, B2 either confirms that the code has been entered correctly so far, or it asks for the previous four digits again.

ii. Compare the security of the three versions A, B and B2. You may assume that a hacker can provide numbers (regardless of length) at a rate of 1000 per second.

[8]

5. (a) Write a paragraph describing the main differences between public key and symmetric key cryptosystems. Explain the advantages and disadvantages of each.

[6]

(b) Alice, Bob and Charles are using a public key and symmetric key cryptosystem to communicate with each other. Following is the protocol they are using to send a signed, encrypted message.

- Alice wants to send Bob message m
- Alice generates a random session key K and encrypts the message using the symmetric key cryptosystem with key K to obtain $c = encrypt_K(m)$.
- Alice generates a signature for her message by encrypting c using her private key. Thus $sig = encrypt_{A_{priv}}(c)$.
- Alice uses Bob's public key to encrypt the session key K to obtain $k' = encrypt_{B_{pub}}(K)$.
- Alice sends (c, sig, k') to Bob.

Complete the protocol by writing the steps that Bob must take to read and authenticate the message.

[4]

(c) Consider the following scenario. Alice describes a money making invention in a message m and signs it for Bob as described in the protocol above. Charles intercepts the message.

Show how Charles can replace Alice's signature with his own before sending the message to Bob. How will Bob interpret the message?

[10]

(d) Re-write the protocol given in part b) so that the message is signed first and then encrypted. Does this new protocol prevent Charles from stealing Alice's idea?

[5]

END OF EXAMINATION