UNIVERSITY OF LONDON 291 0326 ZB

FOR EXTERNAL STUDENTS - EASTERN

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. Following is a protocol used for the preparation and marking of examination papers.

   - Candidates are entered for the examination.
   - Lead examiner and second examiner are appointed by the University exams office.
   - Lead examiner writes the examination paper and solutions and posts these to the second examiner.
   - Second examiner checks the examination paper and solutions, marks corrections on these, and posts them back to the lead examiner.
   - Lead examiner makes corrections as appropriate and posts final copies of examination paper and solutions to the University exams office.
   - University exams office prints the examination paper and distributes it by post to the examination centers.
   - Candidates sit the examination at their appointed examination center and then leave their scripts and examination paper at the examination center.
   - Examination scripts are distributed, half each, to the lead examiner and second examiner for first marking.
   - Lead examiner and second examiner exchange first marked scripts for second marking.
   - Scripts are given a final mark after second marking and returned to the University exams office.
   - Final marks are entered on the University database by the University exams office.

(question continues on next page)

question 1 continued

(a) The *subjects* in this protocol are the candidates, the lead examiner, the second examiner, the University exams office and the examination centers. One of the *objects* in the protocol is the examination paper. Identify **two** other objects.

[2]

(b) Suggest suitable permissions from the list {write, read, alter, limited access read} for each of the subjects on each of the objects. Your answer may be in the form of an access control table if you wish.

[6]

(c) Draw a *protection ring* to illustrate the access control rights of the subjects with regards to the examination paper.

[3]

(d) Which of the access control permissions are enforced by the protocol, and which are dependent upon the trustworthiness of the subjects?

[7]

(e) As it stands there are no integrity checks on either the examination papers or the final marks awarded. Suggest steps that could be added to the protocol to ensure that integrity is maintained.

[7]

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 HELLO is partially encoded as follows:

characters	H	E	L	L	O	*space*
character values	8	5	12	12		
block value	8(27)+5 =221					

i. Copy and complete the table above. Then using the RSA public keys ($n = 901, e = 3$) encrypt the word HELLO.

[5]

ii. Suppose we want to include both lower case and upper case characters in our messages. Suggest changes to the key and encoding method which 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 hello is encrypted to (561,58,812,812,445). Decrypt the word (561,445,812,58) 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 → S: A,B

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

A → 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 from 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 Alice's key K_{AS}. What can Charles do now? What should Alice do when she discovers that her key has been compromised?

[8]

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

$f(x) = x \ mod \ 2^{32}$ (i.e. the least significant 32 bits of x)

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

$h(x) = x \oplus$ number of seconds since 1st January 2000

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]

(question continues on next page)

question 4 continued

(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 a 6-digit code. After all six 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 40-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 40-digit code but after every 5-digits, B2 either confirms that the code has been entered correctly so far, or it asks for the previous five 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) Describe the PGP protocol for encrypting a signed message.

[7]

(b) Alice, Bob and Charles are using PGP to communicate. Consider the following scenario:

- Alice writes a message, signs it, then encrypts the message for Bob.
- Bob receives the message and decrypts it. Bob now has a message with Alice's signature on it, which can be kept. The message says "I love you".
- Bob does not share Alice's feelings and decides to play an embarrassing trick on her.
- Bob encrypts the message, already signed by Alice, using Charles' public key and sends this to Charles.

How will Charles interpret the message? Will he be able to tell that he has been misled?

[4]

What message should Alice have sent in order to avoid this embarrassment?

[2]

(question continues on next page)

question 5 continued

(c) Describe how Alice would look up Bob's public key using the X509 protocol.

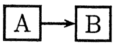
[4]

(d) An alternative key management system is to use the *web of trust.* This model allows users to sign each others public key. Keys are published together with all of the signatures they have obtained. Alice should only sign Bob's key if she has personally verified his identity and is sure that his key is correct.

i. What are the advantages and disadvantages of the *web of trust* model compared with X509?

[3]

The following notation is used to indicate that Alice (A) has signed Bob's (B) key.



ii. Consider the diagrams, Figure 1 and Figure 2, which show two different pathways between keyholders A and E via other keyholders B, C and D. In which case should Alice be more confident of E's identity? Explain your answer.

[5]

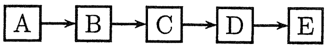


Figure 1

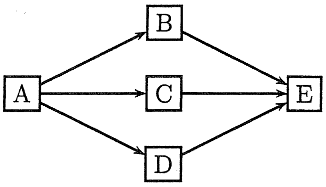


Figure 2

END OF EXAMINATION