UNIVERSITY OF LONDON 291 0326W

FOR EXTERNAL STUDENTS - WESTERN

B.Sc. EXAMINATION 2005

COMPUTING AND INFORMATION SYSTEMS

CIS326 Computer Security

Duration: 2 hours 15 minutes

Date and time: Tuesday, 24 May 2005 : 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.

Electronic calculators must not be programmed prior to the examination. Calculators which display graphics, text or algebraic equations are not allowed.

UL05/490

Answer any three of the following five questions. There are 25 marks for each question.

1. a) Name and briefly explain six features that should be provided by a good security system. [6]

   b) A password system is used to prevent unauthorized access to a computer system. Describe how a hacker may try to obtain a valid user's password by performing a *spoofing attack.* [2]

   c) What measures can be taken to prevent or discover a spoofing attack: [2]
      i) by the system
      ii) by the user

   d) i) A password in a particular system can be made up of any of 100 different keyboard characters. What is the size of the keyspace for this system if passwords are 6 characters long? [1]

      ii) The system requires users to change their passwords once every six months, and insists on a minimum password length of n characters. Assuming that an automated password cracker can check 10,000 passwords per minute, what is the least possible value of n that can be used in order to prevent a successful exhaustive search attack? [4]

   e) A team of three security personnel maintains the password system. The passwords are stored in a file, which can be accessed only by using a secret key K. Describe how the three security personnel could use a key escrow scheme to safe guard against the loss of the key K. [5]

   f) A 2 of 3 key escrow scheme has been used to protect a key K. The three key holders have keys $(k_1 = 2, x_1 = 7)$, $(k_2 = 5, x_2 = 3)$ and $(k_3 = 14, x_3 = 10)$ respectively. The prime number used in the scheme is 19. Showing all of your working, find the value of the key K. [5]

2. A commercially available symmetric key cryptosystem, called XYZ, has blocks of size b bits and keys of size k bits.

   a) Why does the value of b need to be large? With modern algorithms what would you estimate to be the smallest value of b that could guarantee security? [2]

   b) How could XYZ be modified to a new symmetric key cryptosystem called double-XYZ, so that the blocksize is still b but the keysize is $2k$. Explain the suggested encryption and decryption algorithms for double-XYZ. [6]

   c) Given that it takes 10 seconds to encrypt one block using XYZ; 0.01 seconds to transmit one block of ciphertext using XYZ; and 100 hours to do an exhaustive key search for the XYZ key; approximately how long would it take: [6]

      i) To encrypt one block using double-XYZ?
      ii) To transmit one block of ciphertext using double-XYZ?
      iii) For a cryptanalyst to do an exhaustive key search for a double-XYZ key?

   d) If Alice and Bob are using a symmetric key cryptosystem to communicate, they will both need to know the key. Describe three different methods that Alice could use to securely exchange a key with Bob. [11]

3. a) Describe the El Gamel public key cryptosystem. Your answer should include [10]

   i. The generation of public and private keys
   ii. The encryption algorithm
   iii. The decryption algorithm
   iv. A justification for the security of the algorithm

   b) Bob has private El Gamel key *(p=29, g=2, a=19)*. What is the value of Bob's public key? [2]

   c) Alice has encrypted a message using Bob's public key. The ciphertext that Alice sends to Bob is *(r=24,c=6)*. Showing all your working, use Bob's private key to recover the message. You may use the algorithm for modular exponentiation given below if you wish. [4]

To compute x^n *mod m*

Initialise *y=1;*
u=x mod m;
Repeat
If *n* is odd then *y:=(y*u) mod m;*
n:=n div 2;
*u:=(u*u) mod m;*
Until *n=0;*
Output *y*;

   d) Show that the algorithm for modular exponentiation given above is of time complexity $O(b^3)$ where *b* is the size of the parameters *x,n* and *m*. Hence show that although the El Gamel algorithms for encryption and decryption are different, they both take approximately the same amount of time to execute. [6]

   e) A particular implementation of the modular exponentiation algorithm takes 0.5 seconds to perform one exponentiation where the numbers input are of size 100 bits. How long would it take for the same implementation to perform one exponentiation if the numbers input were of size 200 bits? [3]

4. a) Suppose that a mathematician found a method that could be used to factorise a large composite number efficiently. Given a composite number *n* the method could quickly find *p* and *q* such that *p*q = n*. Explain why the security of the RSA public key cryptosystem would be compromised. [4]

   b) Bob has a public RSA key *(n = 253, e = 7)*. He sends Alice a message *m* and the digital signature *s* of the message. Bob calculates the signature by computing $s = m^d \bmod n$ where *d* is Bob's private key. The message that Alice receives is *(m = 107, s = 26)*. Should Alice accept the message as genuine or not? You must give a justification for your answer. [8]

   c) Name the four properties that a cryptographic hash function should possess and explain why each of these is important. [6]

   d) Explain how a hash function can be used in conjunction with RSA to produce digital signatures. [6]

   e) What is the advantage of using a hash function when producing a digital signature? [1]

5. Pretty Good Privacy (PGP) provides security for electronic mail systems.

a) Describe how PGP provides simultaneously confidentiality, authentication and compression. [14]

Your answer should describe how a user compresses, digitally signs and encrypts a message and how the receiver determines the original message and proves that it is genuine. It is not necessary to give specific details about particular hash functions, symmetric cryptosystems or public key cryptosystems, but you should indicate what protocols you are assuming are available to each of the participants.

b) Name two advantages that the compression stage brings to PGP. [2]

c) Explain why there is sometimes a difficulty in sending encrypted text by electronic mail and describe how PGP overcomes this difficulty. [6]

d) Why is it essential to have a good method of generating pseudorandom numbers for both PGP and many other cryptographic applications? [3]

END OF EXAMINATION