UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)
Academic Year 2008/2009 – 3rd Year Examination – Semester 5

IT5203: Security of Information Systems

Structured Question Paper
16th May,2009
(TWO HOURS)

To be completed by the candidate

BIT Examination Index No: ....

Important Instructions:

- The duration of the paper is **2 (Two) hours**.
- The medium of instruction and questions is English.
- This paper has **4 questions** and **11 pages**.
- **Answer all 4 questions**. **Questions Do Not carry equal marks**
- **Write your answers** in English using the space provided **in this question paper**.
- Do not tear off any part of this answer book.
- Under no circumstances may this book, used or unused, be removed from the Examination Hall by a candidate.
- Note that questions appear on both sides of the paper.
  If a page is not printed, please inform the supervisor immediately.

Questions Answered

Indicate by a cross (×), (e.g. ☒) the numbers of the questions answered.

	Question numbers				
To be completed by the candidate by marking a cross (×).	1	2	3	4	
To be completed by the examiners:					

1) **Answer each question as true or false, and provide a single sentence justification for your answer.**

(a) The message length the Message Authentication Algorithm (MAC) depends on the plain text.

(02 marks)

ANSWER IN THIS BOX

False

Justification: Message length of Message Authentication Algorithm (MAC) is depend on the algorithm.

(b) Digital signatures employ hashing.

(02 marks)

ANSWER IN THIS BOX

True

Justification: Digital signature processes first, creates hash and then encrypts it with the private key.

(c) The HMAC Algorithm cannot use MD5 as hash function.

(02 marks)

ANSWER IN THIS BOX

False

Justification: HMAC can use any hash function

(d) HTTP protocol is considered as a secure communication protocol.

(02 marks)

ANSWER IN THIS BOX

False

Justification: HTTP protocol sends data in clear text format.

(e) The Quantum Cryptography(QC) algorithm can be used with a higher confidence compared to RSA.

(02 marks)

ANSWER IN THIS BOX

True

Justification: Strength of QC is not dependent on key size and thus has high confidence level.

(f) Euclidean algorithm exploits the fact that if x divides **a** and **b**, x also divides k-(a*b) for every k.

(02 marks)

ANSWER IN THIS BOX

False

Justification: Euclidean algorithm exploits the fact that if x divides a and b, x also divides a-(k*b) for every k.

(g) The greatest common divisor of two numbers a and b is the smallest integer that divides both a and b.

(02 marks)

ANSWER IN THIS BOX

False

Justification: The greatest common divisor of two numbers a and b is the largest integer that divides both a and b.

(h) The SSL protocol uses only symmetric key algorithms.

(02 marks)

ANSWER IN THIS BOX

False

Justification: One of the most important advantages of the SSL protocol is mixing the better of the two encryption key techniques, symmetric and asymmetric.

(i) Two numbers a and b are “relatively prime” if they have only prime divisors apart from 1.

(02 marks)

ANSWER IN THIS BOX

False

Justification: Two numbers a and b are relatively prime if they have no common divisors apart from 1.

(j) The level of security provided by good cryptographic protocol should depend on the secrecy of the algorithm.

(02 marks)

ANSWER IN THIS BOX

False

Justification: Security of a good cryptographic protocol should not depend on secrecy of the algorithm.

(k) A smart card provides the so called “two-factor authentication”.

(02 marks)

ANSWER IN THIS BOX

True

Justification: In the smart card system, a user is required to present the card and the enter the PIN so it that provides two factor authentication.

(l) A characteristic of diffusion states that the interceptor should not be able to predict how the change of a character in the plaintext will affect the ciphertext.

(02 marks)

ANSWER IN THIS BOX

False

Justification: The characteristics of diffusion state that the interceptor should not be able to predict how change of a character in the plaintext will affect the ciphertext.

(m) PGP is one of the widely used e-mail security standards.

(02 mark)

ANSWER IN THIS BOX

True

Justification: PGP and S/MIME are the e-mail security standards.

(n) A random security key in the "one-time pad" is the most secure symmetric key cryptographic system.

(02 mark)

ANSWER IN THIS BOX

True

Justification: A random security key in one-time pad is used only once and encryption key length is equivalent to the data length; thus it is the most secure symmetric key cryptographic system.

(0) Precautions taken against data corruption falls into the category of data integrity.

(02 mark)

ANSWER IN THIS BOX

True

Justification: Detecting an unauthorized modification is called data integrity.

2) (a) Write down the greatest common divisor of 1030 and 960.

(05 mark)

ANSWER IN THIS BOX

1030 = 1 x 960 + 70	**gcd(960,70)**
960 = 13 x70 + 50	**gcd(70, 50)**
70 = 1 x 50 + 20	**gcd(50,20)**
50 = 2 x 20 + 10	**gcd(20, 10)**
20 = 2 x 10 + 0	**gcd(10,0)**

(b) A 128 bit AES key is to be broken using the brute force method on a 1GHz computer. How long would it take to break the key in the best case and in the worst case situations? Assume that 1000 clock cycles are required to check a single AES key.

(05 mark)

ANSWER IN THIS BOX

time for test a AES key $=10^3 * 1/10^9$

number of DES keys $= 2^{128}$

Maximum time = (seconds) $2^{128} * 1/10^6$

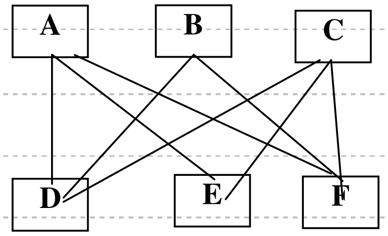
Minimum time = (seconds) $1/10^6$

(c) Suppose there are six nodes A, B, C, D, E and F in a network. How many keys are required such that each of A, B and C can communicate with each of the nodes D, E and F in a bidirectional secure way using the AES encryption algorithm?

(05 mark)

ANSWER IN THIS BOX

Nine (9) keys



(d) We now replace AES in section (c) with the RSA algorithm. How many public keys are required in this case where each of A, B and C can communicate with each of D,E and F in a bi-directional secure way?

(05 mark)

ANSWER IN THIS BOX

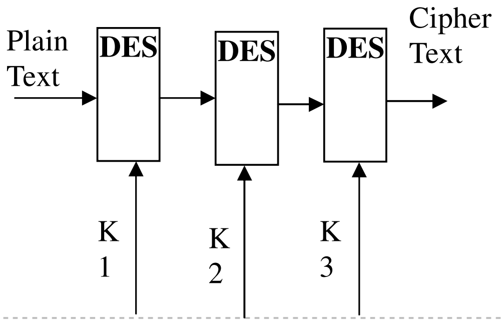
Each node must have a public key. So 6 public keys are required.

(e) One of the widely used schemes for encryption/decryption is the Data Encryption Standard (DES) and it's variances. Explain a simple scheme to enhance the strength of DES.

(05 mark)

ANSWER IN THIS BOX

Triple DES algorithm.



3) (a) In an implementation, the RSA public key system uses, p=11, q=13 and e =11 to encrypt a plain text m=7. What is the resulting cipher text C?

(05 mark)

ANSWER IN THIS BOX

Let p=11, q=13 and e=11
n=p*q=11*13=143

Encryption

$C=P^e$ mod n Let m=7 so that $C=7^{11}$ mod 143; C=106

(b) Suppose the RSA private key is d=5 and n=35. What is the corresponding plain text M for the intercepted cipher text c=10?

(05 mark)

ANSWER IN THIS BOX

Let p*q=n=35 and d=5

Decryption

$P=C^d$ mod n p=10^5 mod 35; p=5

(c) Who will vouch for the binding between the data items in a digital certificate?

(05 mark)

ANSWER IN THIS BOX

Certification Authority (CA)

(d) In exceptional situations, a user may have to revoke his digital certificate. List five (5) situations for such a need to revoke.

(05 mark)

ANSWER IN THIS BOX

Any five(5) from the below list:

- **Loss of the private key**
- **Corruption of the private key**
- **Private key has been stolen**
- **Change in the identification information**
- **Compromise of the CA's private key**
- **User has forgotten the password of the certificate database**
- **User changes the algorithms**
- **Loss of trustworthiness of the CA**

(e) List the necessary steps required for the setting up of an SSL web server.

(05 mark)

ANSWER IN THIS BOX

Create public & private key pair and install private key on the web server.

Generate certificate request including the public key.

Submit the certificate request to CA server.

Obtain the certificate and install it on the web server.

4) (a) List three (3) disadvantages of the IPSec protocol.

(03 marks)

ANSWER IN THIS BOX

- **cannot provide document level security**
- **data storage is not secure**
- **end user authentication is not possible**

(b) Suppose that one needs to prove that he/she, and not someone else, has sent a particular message to a colleague. Propose a method to achieve this, by assuming that he/she is using public key encryption.

(05 marks)

ANSWER IN THIS BOX

X=sender Y=recipient

- **X generates a public/private key pair**
- **X obtains digital certificate for the public key**
- **X generates a message**
- **X creates a hash of the message**
- **X encrypts the hash with the private key**
- **X sends message, encrypted hash together with the digital certificate to Y.**
- **Y compares new hash with the original hash.**

- **Y verifies the public key certificate**
- **Y obtains the public key of X from the certificate.**
- **Y decrypts the encrypted hash with the public key and obtains the original hash.**
- **Y creates a new hash of the message**

(c) Define the term "Trapdoor", and distinguish it from a computer virus.

(04 marks)

ANSWER IN THIS BOX

A trapdoor is a secret, undocumented entry point into a computer program. A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the owner.

(d) Define and compare the concepts of " packet filtering" and "application level firewalls".

(05 marks)

ANSWER IN THIS BOX

The packet filtering firewall looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing. Application level gateway applies security mechanisms to specific applications, such as HTP and FTP servers. This is very effective, but can impose a performance degradation

(e) A wireless network may have many vulnerabilities. State three (3) protocols/standards which could be used to limit the impact of these vulnerabilities on the system?

(03 marks)

ANSWER IN THIS BOX

Any three(3) from the list bellow:

- **Wired Equivalent Privacy (WEP)**
- **Wi-Fi Protected Access (WPA)**
- **Remote Authentication Dial In User Service (RADIUS)**
- **IEEE 802.11i**
- **IEEE 802.11x**

****