UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)
Academic Year 2009/2010 – 3rd Year Examination – Semester 5

IT5203: Security of Information Systems

Structured Question Paper
27th March, 2010
(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 **12 pages**.
- **Answer all 4 questions.** (all questions **do not** carry equal marks)
- **Question 1** (40% marks) **and other questions** (20% 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.
- **Non-programmable Calculators may be used**

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 then justify your answers in at most one sentence.**

(a) A Digital Signature Algorithm (DSA) can be used for signing and encryption.

(02 marks)

ANSWER IN THIS BOX

False

Justification: Digital Signature Algorithm (DSA) can be used only for signing.

(b) Stream ciphers process messages in blocks, each of which is then encrypted or decrypted.

(02 marks)

ANSWER IN THIS BOX

False

Justification: Block ciphers process messages in blocks, each of which is then encrypted or decrypted.

(c) IPsec is one of the popular Virtual Private Network (VPN) technologies.

(02 marks)

ANSWER IN THIS BOX

True

Justification: In addition to IPSec, there are many other VPN protocols.

(d) The HTTPS protocol is able to provide a non-repudiation security service.

(02 marks)

ANSWER IN THIS BOX

False

Justification: The HTTPS protocol provides data integrity and confidentiality security services.

(e) Elliptic Curve Cryptography (ECC) algorithm has a higher confidence level when compared with RSA.

(02 marks)

ANSWER IN THIS BOX

True

Justification: ECC has high confidence level even though it has short key size.

(f) The characteristic of distributing information from a single plaintext letter over the entire ciphertext is called confusion.

(02 marks)

ANSWER IN THIS BOX

False

Justification: The characteristics of distributing the information from single plaintext letter over the entire ciphertext is called diffusion.

(g) If p is a prime number, for any number q<p, the greatest common divisor of p and q is equal to 0 (gcd(p,q)=0).

(02 marks)

ANSWER IN THIS BOX

False

Justification: If p is a prime number, for any number q<p, greatest common divisor is equal to 1 (gcd(p,q)=1).

(h) The Secure Electronic Transaction (SET) protocol uses only symmetric key algorithms.

(02 marks)

ANSWER IN THIS BOX

False

Justification: The Secure Electronic Transaction (SET) protocol uses symmetric key algorithms and asymmetric key algorithms.

(i) A public-key, which may be known by anybody, can be used to encrypt messages and verify signatures.

(02 marks)

ANSWER IN THIS BOX

True

Justification: A public-key can be used to encrypt messages and verify signatures. A private-key can be used to decrypt messages and create signatures.

(j) The security of an encryption scheme must depend on the secrecy of the key and the secrecy of the algorithms.

(02 marks)

ANSWER IN THIS BOX

False

Justification: The security of the encryption scheme must depend only on the secrecy of the key and not on the secrecy of the algorithms.

(k) A banking card (ATM card) provides two-factor authentication.

(02 marks)

ANSWER IN THIS BOX

True

Justification: In the ATM card system, user needs to present the card and enters the PIN so it provides two factor authentication.

(l) The size of enciphered text should be larger than the text of the original message.

(02 marks)

ANSWER IN THIS BOX

False

Justification: The size of enciphered text should be no larger than the text of the original message.

(m) S/MIME is one of the widely used e-mail security standards.

(02 marks)

ANSWER IN THIS BOX

True

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

(n) A firewall blocks only the incoming data that might contain a hacker attack.

(02 mark)

ANSWER IN THIS BOX

False

Justification: A firewall blocks incoming data that might contain a hacker attack; It hides internal addresses from Internet hackers; it screens outgoing traffic to limit Internet use and/or access to remote sites.

(o) Precautions against unauthorized modification fall in to the category of data integrity.

(02 mark)

ANSWER IN THIS BOX

True

Justification: Detecting an unauthorized modification is called data integrity.

(p) The tunnel mode of IPSec protocol encrypts the entire IP packet.

(02 mark)

ANSWER IN THIS BOX

True

Justification: The Transport mode of the IPSec encrypts data and the tunnel mode of IPSec protocol encrypts entire IP packet including the IP header.

(q) Computer viruses and other malicious software are often spread through email attachments.

(02 mark)

ANSWER IN THIS BOX

True

Justification: The most common method of virus spreading is email attachments.

(r) A Zombi is an anonymous, unsolicited junk email sent indiscriminately to huge numbers of recipients.

(02 mark)

ANSWER IN THIS BOX

False

Justification: Spam is anonymous, unsolicited junk email sent indiscriminately to huge numbers of recipients.

(s) IPSec is the first operating system evaluation criteria to gain wide acceptance.

(02 mark)

ANSWER IN THIS BOX

False

Justification: The Trusted Computer Security Evaluation Criteria (TCSEC) is the first operating system evaluation criteria to gain wide acceptance.

(t) An authority trusted by one or more users to create and sign attribute certificate is called the Certificate Authority.

(02 mark)

ANSWER IN THIS BOX

False

Justification: An authority trusted by one or more users to create and sign attribute certificate is called Attribute Authority.

2) (a) Determine the greatest common divisor of 1500 and 560.

(05 mark)

ANSWER IN THIS BOX

1500 = 2 x 560 + 380	gcd(560,380)
560 = 1 x380 + 180	gcd(380,180)
380 = 2 x 180 + 20	gcd(180,20)
180 = 9 x 20 + 0	gcd(20, 0)

The g.c.d. of 1500 and 560 is 20

(b) Identify pairs of relatively prime numbers from the following list.
(12,20), (30, 20), (13, 14), (8, 9), (19, 3)

(05 mark)

ANSWER IN THIS BOX

(13, 14), (8, 9), (19,3)

(c) What are/is the key size for the DES, IDEA and AES algorithms?

(05 mark)

ANSWER IN THIS BOX

DES: 56,

IDEA: 128,

AES: 128,192,256

(d) An RSA public key systems uses, p=17, q=7, e =5 and plain text m=7.
What is the cipher text C?

(05 mark)

ANSWER IN THIS BOX

Let p=17, q=7 and e=5

*n=p*q=17*7=119*

Encryption

$C=P^e$ mod n

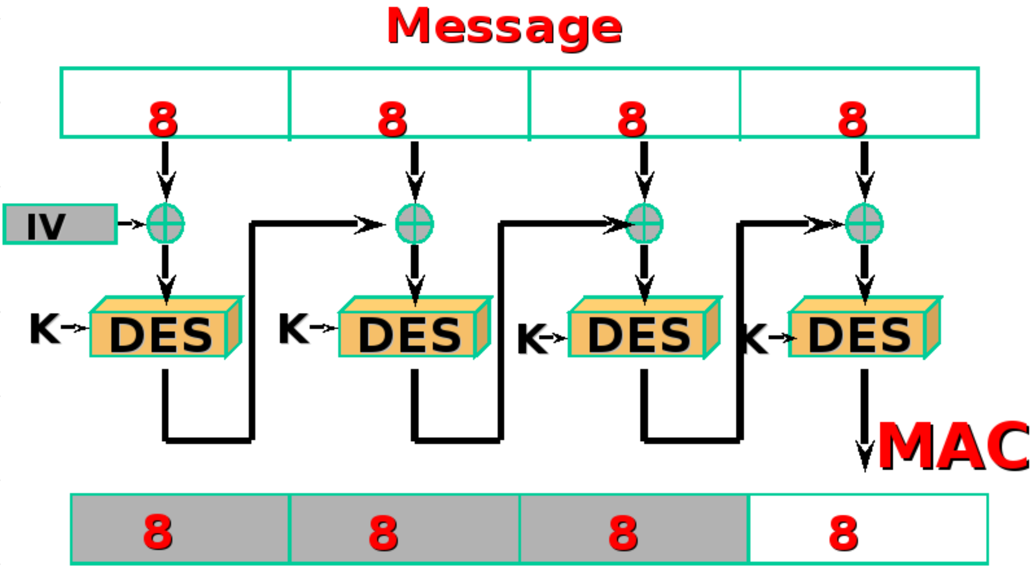
Let m=7 so that $C=7^5$ mod 119; C=28

3) (a) Using a block diagram, describe a symmetric key encryption mode that can generate the Message Authentication Code (MAC) code.

(06 mark)

ANSWER IN THIS BOX

As shown in the following figure, Cipher Block Chaining (CBC) mode can generate the MAC code.



(b) State an unconditionally secure key distribution method.

(02 mark)

ANSWER IN THIS BOX

The method is called BB84 which is based on Quantum Cryptography.

(c) Suppose we want to use the Diffie-Hellman Key Agreement protocol between two end points A and B, and have chosen the integer 2 as g and the integer 10 as the n. For the private key x and public key X, we have the relation $X = g^x \bmod n$. If A generates the private key x=4 and B generates the private key y=5, what is the session key k between A and B?

(06 mark)

ANSWER IN THIS BOX

$X = g^x$ mod n.
$X= 2^4$ mod 10
$X= 6$

$k=X^y$ mod n. $=6^5$ mod n.=6

OR

$k=g^{xy}$ mod n
$k=2^{4 *5}$mod 10

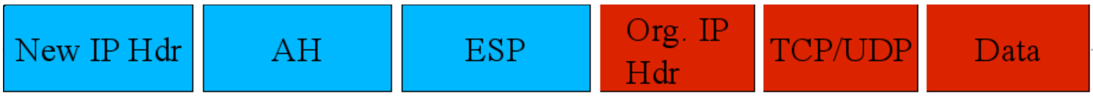
$k=6$

(d) Suppose one wants to authenticate and encrypt the IP packets (including the IP address) by using IPSec protocol. Explain the structure of a IPSec packet by using a suitable diagram.

(06 mark)

ANSWER IN THIS BOX

IPSec protocol should be configured in the tunneling mode by including the authentication (AH) and encapsulation(ESP) payload as shown in the following diagram.



4) (a) List two (2) good reasons to place security in the lower layers of the operating system.

(04 marks)

ANSWER IN THIS BOX

1. It may be possible to evaluate security to a higher level of assurance.
2. Putting security mechanisms into the core of the system reduces performance overheads caused by security.

(b) Describe an SQL injection attack through a Web application by using an example.

(06 marks)

ANSWER IN THIS BOX

Suppose application Java code contains the following SQL statement:

```
String query = "SELECT * FROM users_table " +
               " WHERE username = " +  " ‘ " + username + " ‘ " +
              " AND password = " + " ‘ " + password + " ‘ " ;
```

Suppose the programmer expects one row to be returned if success, no rows if failure.

Then attacker enters any username and password of: Aa ‘ OR ‘ ‘ = ‘. Therefore the final query becomes: SELECT * FROM users_table WHERE username = ‘anyname‘ AND password = ‘Aa‘ OR ‘ ‘ = ‘ ‘;

It returns all user rows. If the application checks for 0 vs more than 0 rows, attacker can successfully login to the system.

(c) List five (5) possible counter measures on a virus attack.

(05 marks)

ANSWER IN THIS BOX

Any five from the following list:

1. Update all software such as operating system, drivers, Internet browser and anti virus.
2. Install inbound and outbound firewall.
3. Encrypt important data.
4. Backup the data regularly.
5. Install third party registry editor, traffic monitoring software.
6. Disable autorun feature.
7. Use open source software and operating systems.

(d) List two (2) security restrictions imposed by the Java security manager on a Java Applet execution.

(02 marks)

ANSWER IN THIS BOX

Any two (2) from the below list:

1. Blocking the access of the local disk to read, write, delete or execute of any file
2. Blocking the access of non-standard libraries
3. Blocking the connections to arbitrary hosts

(e) A wireless network has several vulnerabilities. State three (3) such vulnerabilities.

(03 marks)

ANSWER IN THIS BOX

Any three (3) from the following list:

1. Unauthorized or “rogue” access points on trusted networks
2. Access to network by unauthorized clients (theft of service, "war driving")
3. Interception and monitoring of wireless traffic
4. Jamming is easy on unlicensed frequency.

****