UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)
Academic Year 2010/2011 – 3rd Year Examination – Semester 5

IT5203: Security of Information Systems

Structured Question Paper with Model Answers
12th March, 2011
(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**. (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 with at most one sentence.**

(a) Vernam cipher is immune to most cryptanalytic attacks.

(02 marks)

ANSWER IN THIS BOX

True

Justification: The Vernam cipher is immune to cryptanalytic attack because the available ciphertext does not display the pattern of the key.

(b) According to Shannon, the implementation of the encryption process should be as complex as possible.

(02 marks)

ANSWER IN THIS BOX

False

Justification: According to Shanan, the implementation of the encryption process should be as simple as possible. A complicated algorithm is prone to error or more likely to be programmed incorrectly.

(c) The columnar transposition and other transposition ciphers are examples of block ciphers.

(02 marks)

ANSWER IN THIS BOX

True

Justification: A block cipher encrypts a group of plaintext symbols as one block.

(d) The triple DES procedure is defined as C = E(k1, E(k2, D(k1,m))). That is, you encrypt with one key, decrypt with the second and encrypt again with the first key.

(02 marks)

ANSWER IN THIS BOX

False

Justification: The triple DES procedure is C = D(k3, E(k2, E(k1,m))). That is, you encrypt with one key, decrypt with the second and encrypt with a third.

(e) The AES algorithm as defined can use 56 or 128 bits keys.

(02 marks)

ANSWER IN THIS BOX

False

Justification: The AES algorithm as defined can use 128, 192 or 256 bit keys.

(f) A symmetric key system with six (6) users requires 15 keys and each user must track and remember a key for each other user with which he or she wants to communicate.

(02 marks)

ANSWER IN THIS BOX

True

Justification: A symmetric key system with n users requires n * (n - 1)/2 keys.

(g) A public key and a user's identity are bound together with a private key which is issued by an entity called a certificate authority.

(02 marks)

ANSWER IN THIS BOX

False

Justification: A public key and user's identity are bound together in a certificate which is then signed by someone called a certificate authority, certifying the accuracy of the binding.

(h) The Euclidean algorithm is a procedure for computing the Hash value of a message.

(02 marks)

ANSWER IN THIS BOX

False

Justification: The Euclidean algorithm is a procedure for computing the greatest common divisor of two numbers. This algorithm exploits the fact that if x divides a and b, x also divides a - (k * b) for every k.

(i) A logic bomb is a class of malicious code that "detonates" or goes off when a specified condition occurs.

(02 marks)

ANSWER IN THIS BOX

True

Justification: A logic bomb executes when a specified condition occurs.

(j) A virus spreads copies of itself as a stand-alone program, whereas a worm spreads copies of itself as a program that attaches to or embeds in other programs.

(02 marks)

ANSWER IN THIS BOX

False

Justification: The worm spreads copies of itself as a stand-alone program, whereas the virus spreads copies of itself as a program that attaches to or embeds in other programs.

(k) An access control matrix is a table in which each row represents a subject and each column represents an object.

(02 marks)

ANSWER IN THIS BOX

True

Justification: An access control matrix is a table in which each entry is the set of access rights for that subject to that object.

(l) A “security model” is a statement of the security we expect the system to enforce.

(02 marks)

ANSWER IN THIS BOX

False

Justification: A security policy is the statement of the security we expect the system to enforce.

(m) Web sites use cookies to avoid a customer having to log in on each visit to a site; these cookies may contain the user's ID and password.

(02 marks)

ANSWER IN THIS BOX

True

Justification: A cookie is a text file stored on the user's computer and passed by the user's browser to the web site when the user goes to that site. So it can be used to maintain the authentication sessions.

(n) "Integrity" refers to a way to infer or derive sensitive data from non-sensitive data.

(02 mark)

ANSWER IN THIS BOX

False

Justification: Inference is the way to infer or derive sensitive data from non-sensitive data.

(o) Lampson constructed a security model for preventing inappropriate modification of data.

(02 mark)

ANSWER IN THIS BOX

False

Justification: Biba constructed the model for preventing inappropriate modification of data.

(p) RSA algorithm can be used for signing and encryption.

(02 mark)

ANSWER IN THIS BOX

True

Justification: Digital Signature Algorithm(DSA) can be used only for signing but RSA can be used for signing and encryption.

(q) A packet filtering firewall maintains state information on each packet in the input stream.

(02 mark)

ANSWER IN THIS BOX

False

Justification: A stateful inspection firewall maintains state information from one packet to another in the input stream.

(r) An Intrusion Detection System (IDS) can be network based or host based.

(02 mark)

ANSWER IN THIS BOX

True

Justification: A network-based IDS is a stand-alone device attached to the network to monitor traffic throughout that network; a host-based IDS runs on a single workstation or client or host to protect that one host.

(s) The principal difference between Secure Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy(PGP) is the method of key exchange.

(02 mark)

ANSWER IN THIS BOX

True

Justification: PGP depends on each user's exchanging keys with all potential recipients and establishing a ring of trusted recipients; S/MIME uses hierarchically validated certificates, usually represented in X.509 format, for key exchange.

(t) The fundamental data structures of IPSec are the virtual private network header and the virtual private network payload.

(02 mark)

ANSWER IN THIS BOX

False

Justification: The fundamental data structures of IPSec are the AH (authentication header) and the ESP (encapsulated security payload).

2) (a) Determine the greatest common divisor of 123309 and 9315?

(05 mark)

ANSWER IN THIS BOX

123309 = 13 x 9315 + 2214	gcd(9315, 2214)
9315 = 4 x 2214 + 459	gcd(2214,459)
2214 = 4 x 459 +378	gcd(459,378)
459 = 1 x 378 +81	gcd(378,81)
378 = 4 x 81 + 54	gcd(81,54)
81 = 1 x 54 +27	gcd(54,27)
54=2*27+0	

gcd(123309, 9315) =27

(b) Identify pairs of relatively prime numbers from among the following list.
(18,17), (27, 81), (13,39), (8,3), (16, 21)

(05 mark)

ANSWER IN THIS BOX

(18, 17), (8,3), (16,21)

(c) Suppose we want to use the Diffie-Hellman Key Agreement protocol between two end points, A and B and have chosen the integer 3 as g and the integer 10 as the n. where g and n are as defined in the protocol. For the private key x and public key X, we have the relation

$X = g^x$ mod n.

If A generates the private key x=5 and B generates the private key y=6, what is the session key k between A and B?

(05 mark)

ANSWER IN THIS BOX

$X = g^x$ mod n.

$X= 3^5$ mod 10.

X= 243 mod 10

X=3

$k=g^{xy}$ mod n.

$k=3^{5*6}$mod 10.

k=9

OR

$k=X^y$ mod n. $=3^6$ mod 10.=9

(d) Nimal and Kamal use the RSA algorithm to communicate. Nimal's public key = (n, e) = (33, 3) and private key = (n, d) = (33, 7). Nimal received an encrypted message C=26. What is the corresponding plain text M?

(05 mark)

ANSWER IN THIS BOX

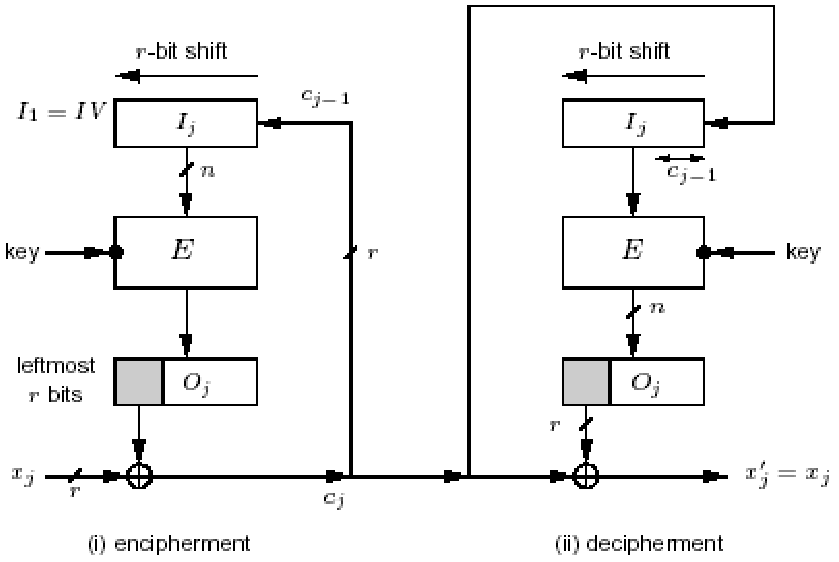
$M=C^d$ mod n *Let C=26 so that $M=26^7$ mod 33; C=5*

3) (a) Using a schematic diagram, describe a symmetric key block cipher encryption mode that can produce a stream cipher.

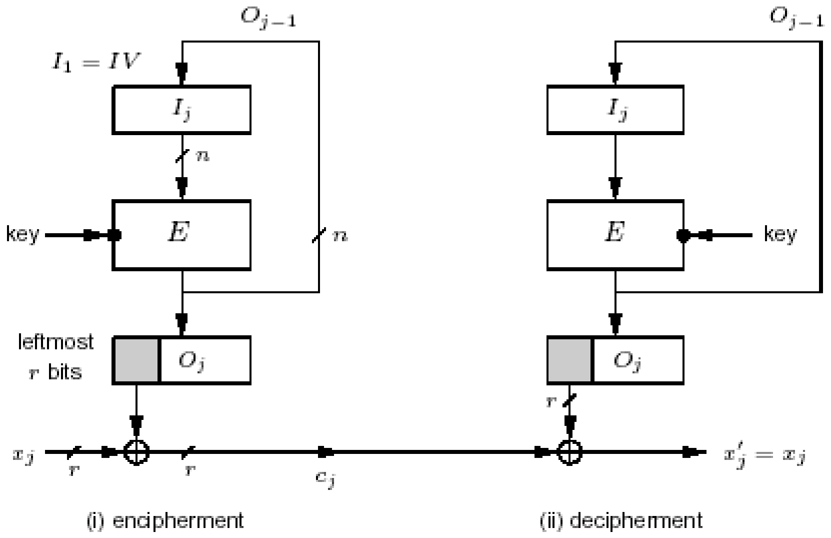
(06 mark)

ANSWER IN THIS BOX

As shown in the following figures, Cipher Feedback Mode (CFB) or Output Feedback (OFB) mode can produce a stream cipher. (***Student should explain CFB or OFB***)



Cipher Feedback Mode (CFB)



Output Feedback (OFB)

(b) Describe the two (2) problems associated with the one-time pad encryption method.

(04 mark)

ANSWER IN THIS BOX

.

The one-time pad method has two problems: the need for absolute synchronization between sender and receiver and the need for an unlimited number of keys. Although generating a large number of random keys is no problem, printing, distributing, storing and accounting for such keys are problems.

(c) Authentication mechanisms use three(3) basic principles to confirm a user's identity. Briefly describe these three(3) basic principles.

(06 mark)

ANSWER IN THIS BOX

1. Something the user knows. Passwords, PIN numbers, passphrases, a secret handshake, and mother's maiden name are examples of what a user may know.
2. Something the user has. Identity badges, physical keys, a driver's license, or a uniform are common examples of things people have that make them recognizable.
3. Something the user is. These authenticators, called biometrics, are based on a physical characteristic of the user, such as a fingerprint, the pattern of a person's voice, or a face (picture).

(d) List four (4) key features of a trusted operating system.

(04 mark)

ANSWER IN THIS BOX

Any four(4) from the following list:

1. user identification and authentication
2. mandatory access control
3. discretionary access control
4. object reuse protection
5. trusted path
6. audit logs
7. intrusion detection

4) (a) List five (5) fundamental user requirements for database security.

(05 marks)

ANSWER IN THIS BOX

Any five (5) from the following list:

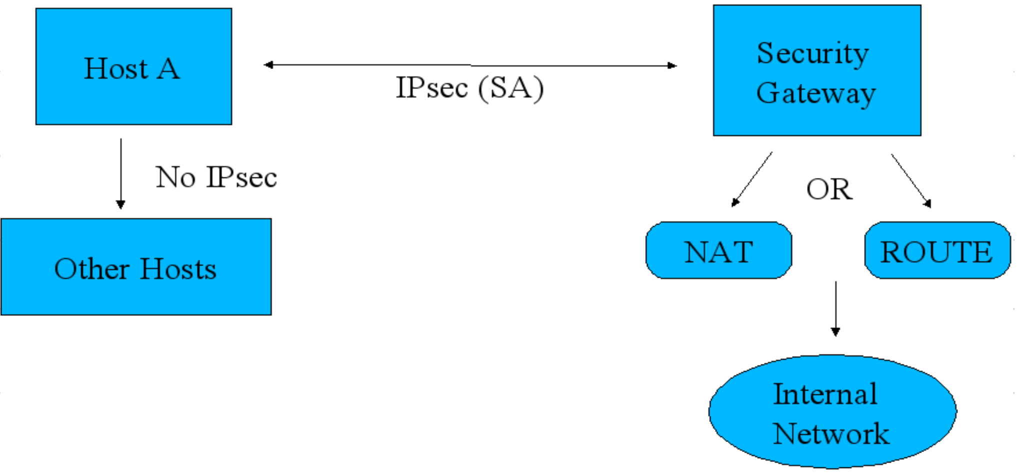
1. ***Physical database integrity:-*** The data of a database is immune to physical problems, such as power failures, and someone can reconstruct the database if it is destroyed through a catastrophe.
2. ***Logical database integrity:-*** The structure of the database is preserved. With logical integrity of a database, a modification to the value of one field does not affect other fields, for example.
3. ***Element integrity:-*** The data contained in each element is accurate.
4. ***Auditability:-*** It is possible to track who or what has accessed (or modified) the elements in the database.
5. ***Access control:-***A user is allowed to access only authorized data and different users can be restricted to different modes of access (such as read or write).
6. ***User authentication:-*** Every user is positively identified, both for the audit trail and for permission to access certain data.
7. ***Availability:-*** Users can access the database in general and all the data for which they are authorized.

(b) Briefly describe a typical "Host to Security Gateway" IPSec configuration method referring to an example.

(05 marks)

ANSWER IN THIS BOX

(***Student should explain the following digram by using a practical example such as as roaming user connectivity***)



(c) Compare and contrast the issues of copyright, patent and trade secrets which are intended to provide protection by law, to data and programs.

(05 marks)

ANSWER IN THIS BOX

	Copyright	**Patent**	**Trade Secret**
Protects	Expression of idea, not idea itself	Invention; the way something works	A secret competive advantage
Protected object made public	Yes; intention is to promote publication	Design filed at patent office	No
Requirement to distribute	Yes	No	No
Ease of filing	Very easy, do-it-yourself	Very complicated; specialist lawyer suggested	No filing
Duration	Life of human originator or 75 years for a company	19 years	Indefinite
Legal protection	Sue if copy sold	Sue if invention copied	Sue for improperly obtained secret

(d) Write down the steps that are necessary in order to create and execute a **signed** Java applet?

(05 marks)

ANSWER IN THIS BOX

1.Compile the applet

2.Create a JAR file

3.Generate Keys

4.Sign the JAR file

5.Export the Public Key Certificate

6.Import the Certificate as a Trusted Certificate

7.Create the policy file

8.Run the applet

****