UNIVERSITY OF COLOMBO, SRI LANKA
UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)
Academic Year 2005/2006 – 3rd Year Examination – Semester 5

IT5202: Security of Information Systems

Structured Question Paper with Model Answers
25th March 2006
(THREE HOURS)

To be completed by the candidate

BIT Examination Index No: .....

Important Instructions:

- The duration of the paper is **3 (Three) hours**.
- The medium of instruction and questions is English.
- This paper has **4 questions** and **11 pages**.
- **Answer all 4 questions**. All questions 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.
- **Non-programmable Calculators may be used.**

Questions Answered

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

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

Index No: ……...

1) Fill each blank using the most suitable word/phrase from the following list:

(1*25=25 marks)

(a) HTTP digest authentication
(b) SQL Injection
(c) Public key/public key
(d) Proxies/proxies
(e) Advanced Encryption Standard (AES)
(f) CRL
(g) Oakley
(h) SSL
(i) Honeypot
(j) Kerberos
(k) Sandbox/sandbox
(l) Smartcard/smartcard
(m) Private key/private key
(n) Authenticate/authenticate
(o) 3D Secure
(p) PGP
(q) Digital watermark/digital watermark
(r) DMZ
(s) Unconditional/unconditional
(t) Digital certificates/digital certificate
(u) Diffie-Hellman
(v) Firewall/firewall
(w) OCSP
(x) Authorization/authorization
(y) Trusted/trusted
(z) Java applets

(i) The RSA algorithm can be used to …… a person or an entity in the Internet.

(ii) ..... is a new technical standard developed by Visa and MasterCard to enhance the security of credit card transactions over the Internet.

(iii) ..... scheme is based on a simple challenge-response mechanism.

(iv) A/An ..... may be known by anybody and used to encrypt messages to provide confidentiality.

(v) ..... standard was developed by Phil Zimmermann for secure e-mail communication.

(vi) ..... takes advantage of insecure code on a system connected to the internet in order to pass commands directly to a database.

(vii) A/An ..... is a signal added to digital data that can be detected or extracted later to ascertain about the originality of data.

(viii) ..... are used by large Internet service providers to reduce network traffic and monitor their user activities.

(ix) Decryption algorithm of ..... is not identical to the encryption algorithm.

(x) The …… is a critical part of a firewall that is neither part of the untrusted network, nor part of the trusted network.

(xi) A/An ..... security implies that the cryptographic algorithm or protocol has no bound on the computational time from an adversary's view point.

(xii) A certificate authority revokes a certificate and notifies it by using a ..... .

(xiii) SSL protocol uses …… to authenticate a public-key.

(xiv, xv) ..... is a key exchange protocol based on the …… key exchange.

(xvi) ..... provides client authentication.

(xvii) ..... is an intruder information gathering technique.

(xviii) A/An ..... interconnects networks with differing trust levels.

(xix) ..... can provide more timely information regarding the revocation status of a certificate.

(xx) ..... is a trusted third-party authentication protocol designed for TCP/IP networks.

(xxi) Attribute Certificate (AC) is relevant for ..... purposes.

(xxii, xxiii) The …… model enables safeguarding of sensitive computer resources from the threats of mobile codes such as …… .

(xxiv) A/An …… provides tamper-proof storage for security application.

(xxv) Mandatory access control is one of the features of a ……operating system.

ANSWER IN THIS BOX

(i)	**n**	**(ii)**	**o**	**(iii)**	**a**
(iv)	**c**	**(v)**	**p**	**(vi)**	**b**
(vii)	**q**	**(viii)**	**d**	**(ix)**	**e**
(x)	**r**	**(xi)**	**s**	**(xii)**	**f**
(xiii)	**t**	**(xiv)**	**g**	**(xv)**	**u**
(xvi)	**h**	**(xvii)**	**i**	**(xviii)**	**v**
(xix)	**w**	**(xx)**	**j**	**(xxi)**	**x**
(xxii)	**k**	**(xxiii)**	**z**	**(xxiv)**	**l**
(xxv)	**y**				

(2) (a) Suppose there are 56 nodes in a computer network. How many DES keys would one need such that every pair of nodes can communicate in a safe way?

(3 marks)

ANSWER IN THIS BOX

n*(n-1)/2
n- number of nodes

55*56/2= 1540

(b) Suppose there are 80 nodes in a computer network. How many public keys do we need such that every pair of nodes can communicate in a safe way?

(3 marks)

ANSWER IN THIS BOX

80

(c) Briefly explain the three (3) basic security issues addressed by public key cryptographic systems.

(6 marks)

ANSWER IN THIS BOX

1. **Key distribution**
2. **Authentication**
3. **Number of keys required for group communication**

(Student should explain the above 3 points)

(d) Outline any three (3) essential features of a digital signature algorithm such as RSA.

(3 marks)

ANSWER IN THIS BOX

1. **Authentic**
2. **Not alterable**
3. **Not reusable**

(e) Suppose we want to use the RSA scheme for an encryption and have chosen the integer value 77 as the product of two (2) prime numbers p and q. For the private key d and public key e, we have the relation *e*d = 1 modulo (p-1) (q-1)*.

(i) What is the public key e for a private key with d = 43?

(ii) What is the cipher C for a message with M =5?

(10 marks)

ANSWER IN THIS BOX

(i) **Find 2 prime numbers p and q such that p*q=77**

Let p=11 and q=7

Select an integer d relatively prime to (p-1)(q-1)

*d=43; 43 is relatively prime to (p-1)(q-1) =10*6=60*

Select e such that e*d mod (p-1)*(q-1)=1

*e=7 since 7*43 mod 60 =301 mod 60 =1*

Public key e= 7

(ii) **$C=M^e \bmod n$**

M=5 so that $C=5^7 \bmod 77$; C=47

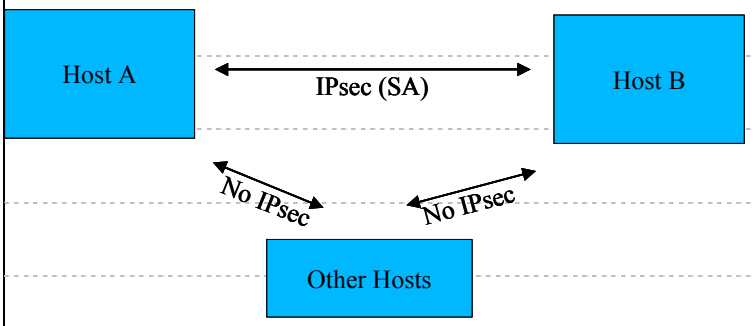
Cipher C = 47

(3) (a) Illustrate using diagrams, the three (3) distinct network configuration scenarios which uses the IPSec protocol.

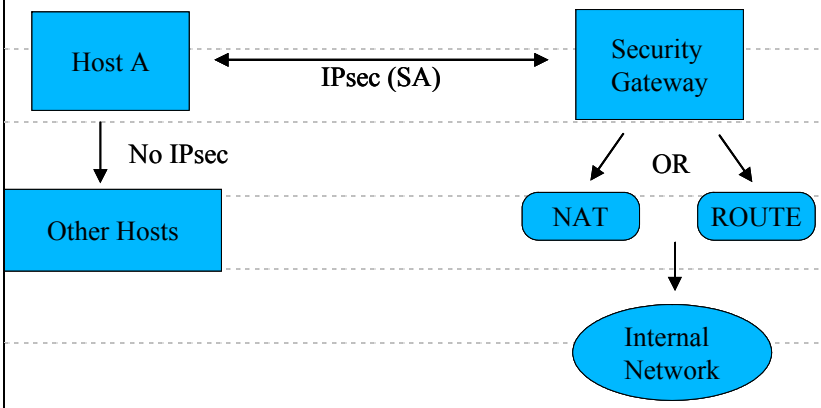
(6 marks)

ANSWER IN THIS BOX

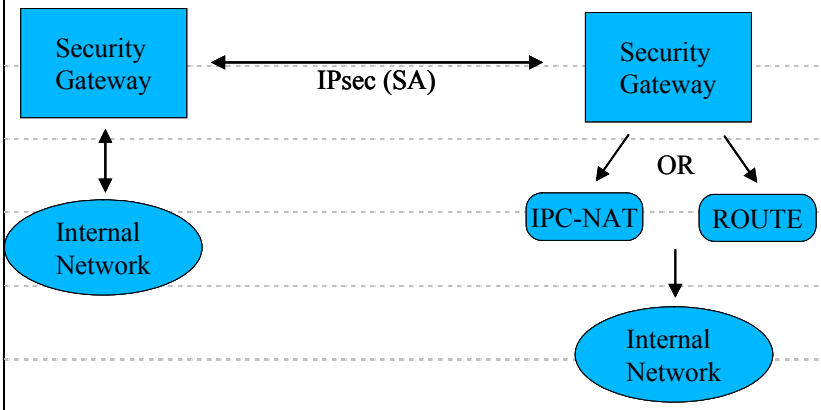
Host to host configuration



Host to security gateway configuration



Security gateway to security gateway configuration

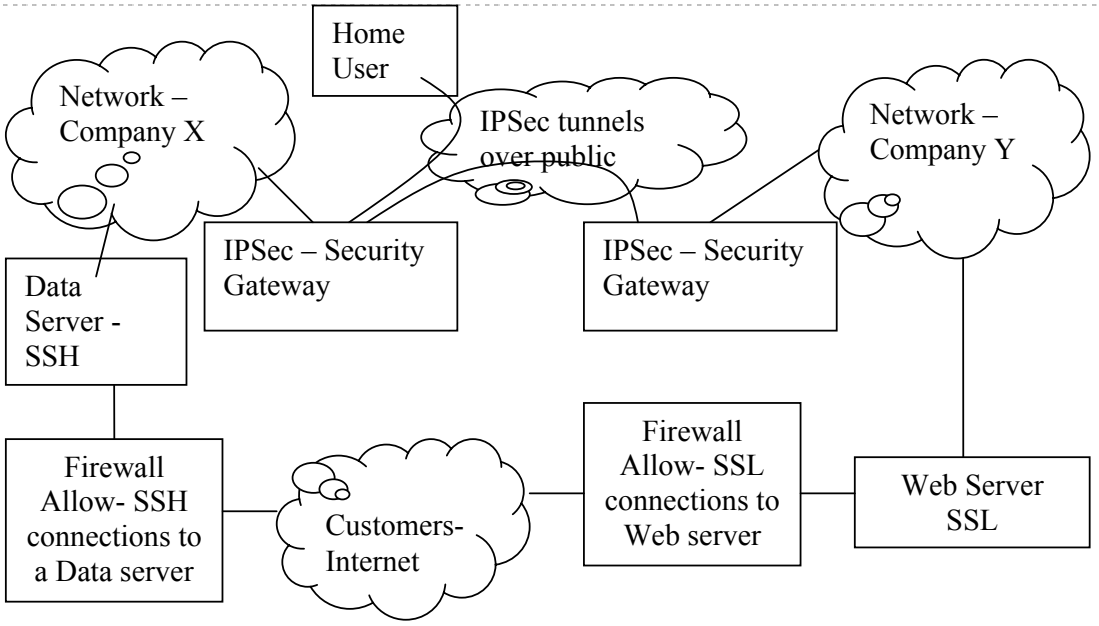


(b) Design a secure network system for two companies X and Y willing to share mutual information, according to the following security requirements.

- Every employee of company X should be able to securely access X's network from his home.
- Company X and company Y should be connected securely over the public network.
- Outside customers using Internet should be able to access a web server in company Y via a secure channel.
- A data server in company X should only be accessible to outside customers via an encrypted channel.

(9 marks)

ANSWER IN THIS BOX



Student should be able to draw a network diagram and describe the security setting at each entity. A sample design is given above.

(c) Briefly discuss any three (3) responsibilities of a system administrator with respect to maintaining network security.

(6 marks)

ANSWER IN THIS BOX

1. **Build a secure firewall for the network**
2. **Balance security issues against employees' ability to access websites for their work**
3. **Early installation of anti-virus, anti-adware and anti-spam systems**

(d) What are the four (4) basic types of firewalls?

(4 marks)

ANSWER IN THIS BOX

1. **Packet Filters**
2. **Stateful Packet Filters**
3. **Application Level Gateway**
4. **Circuit Level Gateway**

(4) (a) List any three (3) popular intruder information gathering techniques.

(3 marks)

ANSWER IN THIS BOX

1. **System logs**
2. **Firewall**
3. **Honeypots/Honeytokens**

(b) List any four (4) basic properties expected of a good security protocol.

(5 marks)

ANSWER IN THIS BOX

- **Everyone must know the steps in the protocol in advance**
- **Every one should be agreed to follow it**
- **Protocol should be clearly defined**
- **It must be complete.**
- **Not possible to do more or to learn more than what is specified in the protocol**

(c) Briefly explain what is meant by the "data inference problem" using your own example.

(5 marks)

ANSWER IN THIS BOX

Students should explain the problem by means of an example.

Following is an example:

Statement Avg(A1,A2,A3) and Avg(A1,A2), inferences the value of A3

A1, A2 and A3 **are data fields of a database**.

(d) List any three (3) popular anti-spamming techniques.

(3 marks)

ANSWER IN THIS BOX

1. **Blacklist/whitelist**
2. **Reverse DNS lookup**
3. **Rules-based filtering**

(e) CGI scripts are executable programs which run on the web server's host machine. How can the security of a CGI script be ensured?

(6 marks)

ANSWER IN THIS BOX

- **All user-supplied input should be checked before passing it through a command shell, an interpreter or any external program.**
- **File names should be examined carefully before opening them.**
- **All array boundaries should be checked.**

(f) List any three (3) popular digital payment systems over the Internet.

(3 marks)

ANSWER IN THIS BOX

1. **Credit card**
2. **Digital cash**
3. **Subscription**

****