UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)
Academic Year 2006/2007 – 3rd Year Examination – Semester 5

IT5202: Security of Information Systems

Structured Question Paper
24th March 2007
(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 **14 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.

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:

(a) data integrity
(b) virus
(c) sign
(d) inference attacks
(e) CRL
(f) cryptanalytic
(g) SSL
(h) Honeypots
(i) Kerberos
(j) SQL injection
(k) RSA
(l) application-level gateway
(m) block cipher
(n) confusion
(o) 3D Secure
(p) PGP
(q) digital watermark
(r) credit card transactions
(s) public key
(t) attribute certificate
(u) Diffie-Hellman
(v) Bell-La Padula confidentiality model
(w) trusted
(x) HMAC
(y) AES
(z) Role Based Access Control

(i) The DSA algorithm can be used to …… electronic documents.

(ii) 3D Secure is a new technical standard developed by Visa and MasterCard to enhance the security of …….. over the Internet.

(iii) The digital certificate identifies the owner of the …… .

(iv) The …… key agreement protocol allows one to establish a secret key over an insecure network.

(v) The …… authentication system keeps a database of client's secret keys.

(vi)…….. uses a secret key to authenticate messages.

(vii) …….. has a 128 bit block length.

(viii) ……. is an asymmetric key encryption algorithm.

(ix) ……..collect valuable information on intruders.

(x) …….. is one of the widely used e-mail security standards.

(xi)A/An ……..…….. needs separate proxies for each network service.

(xii) A/An …….. can be either resident or transient.

(xiii) Precautions taken against data corruption fall in to the category of …….. .

(xiv) Random data perturbation is a possible precaution that can be taken against …….. .

(xv) …….. is to take advantage of insecure code on a system connected to the Internet in order to pass commands directly to a database.

(xvi) ……..…….. control appears to be a viable alternative to traditional discretionary and mandatory access controls.

(xvii) A/An ……..……..associates a holder with access attributes.

(xviii) A/An …….. is an encryption scheme which breaks up the plaintext messages into strings of a fixed length block over an alphabet and encrypts one block at a time.

(xix) The …….. provides mechanisms to obtain certificate revocation information.

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

(xxi) The…….. protocol uses a digital certificate to authenticate a public-key.

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

(xxiii) ……..……..……..is a formal description of the allowable paths of information flow in a secure computer system.

(xxiv) The Vernam cipher is immune to most …….. attacks.

(xxv) The characteristics of …….. state that, the interceptor should not be able to predict how a change of a character in the plaintext will affect the ciphertext.

(25 marks)

ANSWER IN THIS BOX

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

(2) (a) State five (5) drawbacks of authentication mechanisms which are based on the notion of "something you know"?

(5 marks)

ANSWER IN THIS BOX

1. **The necessity to create a shared secret for virtually every resource**
2. **Systems administrators can obtain or change shared secrets**
3. **Requiring users to know numerous shared secrets**
4. **Requiring shared secrets to be stored at servers and sent over the public network**
5. **Shared secrets are vulnerable to attacks such as dictionary attack.**

(b) Express in symbolic notation, the operation of the *Caesar* cipher. Decrypt the following ciphered text which is known to have been encrypted with a Caesar cipher:

HDVB TXHVWLRQ

(3 marks)

ANSWER IN THIS BOX

Caesar Cipher : $C_i = E(P_i) = P_i + 3$

Ciper Text : HDVB TXHVWLRQ

Plain Text : EASY QUESTION

(c) State eight (8) characteristics of a good encryption algorithm.

(4 marks)

ANSWER IN THIS BOX

1. **The size of the encrypted message should not be larger than the original message.**
2. **Errors should not propagate to the other encrypted/decrypted blocks in the message.**
3. **Simple implementation**
4. **Confusion**
5. **Diffusion**
6. **Works on any kind of plain text**
7. **Strong enough to face a brute force attack**
8. **Clearly defined and published**

(d) Briefly name and describe three (3) workstation security safeguards for which you may be responsible as a system administrator.

(6 marks)

ANSWER IN THIS BOX

1. **User ID, Password**
2. **Log-off programs**
3. **Lock-up office or work area (doors, windows)**

(Student should explain the above 3 points)

Continued …

(e) State three (3) advantages of the RSA algorithm over the AES algorithm.

(3 marks)

ANSWER IN THIS BOX

1. **Can use to provide several security services such as authentication, integrity and non-repudiation**
2. **Has strong key size**
3. **Can distribute keys over open network**

(f) List four (4) security services supported by the Kerberos protocol?

(4 marks)

ANSWER IN THIS BOX

1. **User Authentication**
2. **Two-Party Authentication**
3. **Key Distribution**
4. **Authentication of data origin and content**

(3) (a) What is the main difference between HASH and MAC?

(3 marks)

ANSWER IN THIS BOX

MAC uses a key but HASH dose not need a key.

(b) Use the Euclidean algorithm to determine the greatest common divisor of 104 and 66?

(3 marks)

ANSWER IN THIS BOX

104 = 1 x 66 + 38	**gcd(66,38)**
66 = 1 x 38 + 28	**gcd(38, 28)**
38 = 1 x 28 +10	**gcd(28, 10)**
28 = 2 x 10 +8	**gcd(10, 8)**
10 = 1 x 8 + 2	**gcd(8, 2)**
8 = 4 x 2 + 0	**gcd(2,0)**

(c) List five (5) possible digital certificate types.

(5 marks)

ANSWER IN THIS BOX

1. **Digital signature**
2. **Key Encryption**
3. **Object signing**
4. **Certificate signing**
5. **CRL signing**

(d) State two (2) major drawbacks of Online Certificate Status Protocol (OCSP)?

(4 marks)

ANSWER IN THIS BOX

The OCSP is slightly ambiguous on the meaning of 'unknown'. It may mean that the subject certificate itself is unknown, or that the revocation status of the certificate is unknown.

OCSP, while aimed at providing timely certificate-status checking, may be prone to the same impediments of Certificate Revocation List (CRL)-namely the time lag between revoking a certificate and its publishing.

OCSP is more prone to replay attacks.

(e) Briefly explain the steps required to obtain a public key certificate from a certificate authority.

(6 marks)

ANSWER IN THIS BOX

1. **Use a Web browser to access the desired certificate authority (CA).**
2. **Complete a Web form requesting certification of your public key by the authority.**
3. **Electronically submit the complet form to the CA.**
4. **It simultaneously generates a private and public key pair, stores the private key as a strongly encrypted file on a security token and sends the public key to the CA.**

Continued …

5. **Physically present at a Local Registration Authority (LRA) and provide identity verification documents such as birth certificate**
6. **Upon identity verification, the CA issues the public key certficate and sends an e-mail message with a URL for downloading the certificate.**

(f) 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) A 256 bit AES key is required to be broken using the brute force method on a 2GHz 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.

(5 marks)

ANSWER IN THIS BOX

time for test a AES key $=10^3 * 2/10^9$

number of AES keys $= 2^{256}$

Maximum time = (seconds) $2^{256} * 2/10^6$

Minimum time = (seconds) $2/10^6$

(b) Your are working in a software company and your project supervisor is a very busy person. He asks you to log into the mail server using his user-ID and password to retrieve some reports. What should your response be?

(4 marks)

ANSWER IN THIS BOX

User IDs and passwords must not be shared.

If pressured further, report the situation to management or to Security Audit Department.

(c) Suppose you are a registered BIT student and you receive the following e-mail. What should your response be?

```
From: nihal@uscs.cmb.ac.lk
Subject: ACTION: ID Audit
Date: January 24, 2006 9:07:02 AM
To: jeeva@ucsc.cmb.ac.lk, kim@ucsc.cmb.ac.lk, and 933 more

Dear BIT Students,

It's time once again to Audit everyone's University ID Card.
Please let me know exactly your Name and ID number. As always with
ID card audits, simply reply to this message with the ID number
and name. If you have any questions regarding this Audit, please
contact Ms. Shanthi at 611.

Best,
Nihal/UCSC
```

(5 marks)

ANSWER IN THIS BOX

I should definitely think twice before replying to the email. If I know the person who sent it, and I know that he is authorized and responsible for collecting this information, I should still verify that the "reply to" address is correct and that my reply email is addressed to the right person. (Emails can be re-directed, so it is always a good idea to double-check the address that replies are going to.)

Continued …

If I don not know the person who sent the email, or are not sure of his role in this matter, you need to check the request before sending the information.

The contact information provided in the email may be a trick so that I should look up the phone number or email address of the person and verify the information independently.

(d) A company XYZ would like to install a Java applet in the company Web server in USA to access the company database server situated in Sri Lanka. Explain the steps in implementing such a Java applet.

(6 marks)

ANSWER IN THIS BOX

Signed Java applet should be implemented.

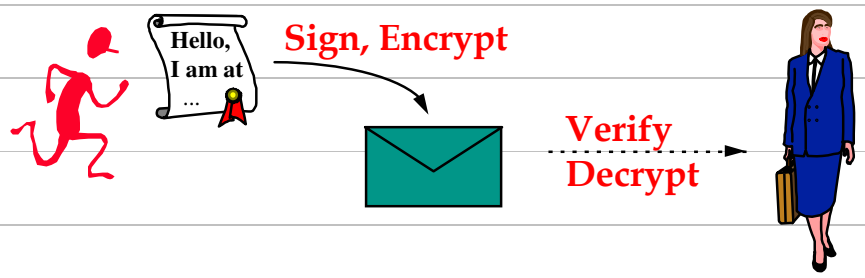
Steps:

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**

(e) Explain a mechanism that can provide all the properties of information integrity, authenticity and confidentiality of emails.

(5 marks)

ANSWER IN THIS BOX



Student should be able to describe the concept of sign/encrypt and decrypt/verify as shown in the above diagram.

*****