UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)
Academic Year 2007/2008 – 3rd Year Examination – Semester 5

IT5202: Security of Information Systems

Structured Question Paper
5th April 2008
(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 **13 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. ☒) 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) **State answer to each question as <u>true</u> or <u>false</u>, followed by a "<u>single sentence</u>" justification of your answer.**

(a) "Security through obscurity" refers to the practice of obscuring a user's password when the user types it in, so that no one else can see it on the screen.

(02 marks)

<u>ANSWER IN THIS BOX</u>

False

Security through obscurity refers to security that relies on secret information, design or implementation details to prevent attack.

(b) Suppose party A generates an RSA public and private key pair and publishes the public key. Then that is all A needs to be able to sends party B, a securely encrypted email.

(02 marks)

<u>ANSWER IN THIS BOX</u>

False

The public key should be certified by a certification authority.

(c) If Prof. D discovers an efficient algorithm for factoring very large numbers, it will make it possible to break RSA**.**

(02 marks)

<u>ANSWER IN THIS BOX</u>

True

The strength of the RSA algorithm depends on the factorization of extremely large prime products.

(d) Access control matrices can represent anything that is representable by access control lists.

(02 marks)

<u>ANSWER IN THIS BOX</u>

False

Access control lists can represent anything that is represented by Access control matrices.

(e) A firewall with a default deny policy is generally safer (from a security point of view) than a firewall with a default allow policy.

(02 marks)

ANSWER IN THIS BOX

True

A firewall with default deny policy opens mandatory communication ports.

(f) Key distribution problem is one of the major drawbacks of a symmetric key system.

(02 marks)

ANSWER IN THIS BOX

True

A symmetric key cannot transmit over the same network.

(g) The Vernam cipher is immune to most cryptanalytic attacks.

(02 marks)

ANSWER IN THIS BOX

True

The Vernam cipher's security key length is equivalent to plain text length.

(h) A Certificate Revocation List (CRL) can provide more timely information regarding the revocation status of a certificate**.**

(02 marks)

ANSWER IN THIS BOX

False

CRLs are published periodically.

(i) An attribute Certificate (AC) can be considered as relevant for authorization purposes.

(02 marks)

ANSWER IN THIS BOX

True

AC contains subject name and access attributes signed by a attribute authority.

(j) "Honeypots" are able to collect valuable information regarding remote web servers.

(02 marks)

ANSWER IN THIS BOX

False

Honeypots collect valuable information on remote intruders.

(k) Precautions to be taken against data corruption fall in to the category of data availability.

(02 marks)

ANSWER IN THIS BOX

False

Precautions against data corruption fall in to the category of data integrity.

(l) A Digital Signature Algorithm (DSA) can be used to encrypt electronic documents.

(02 marks)

ANSWER IN THIS BOX

False

DSA can only be used to sign electronic documents

(m) The Elliptic Curve (EC) cryptographic algorithm is a recent symmetric key cryptographic algorithm.

(01 mark)

ANSWER IN THIS BOX

False

Elliptic Curve (EC) cryptographic algorithm is a new asymmetric key cryptographic algorithm.

2) (a) The "one-time pad" is the most secure of all symmetric key cryptographic systems.

(i) Why is the "one-time pad" so secure?
(ii) Why is not the "one-time pad" used in all cryptographic systems?

(04 marks)

ANSWER IN THIS BOX

(i)

A random security key in one-time pad is used only once.

Encryption key length is equivalent to the data length.

(ii)

A generating the same random stream at the sender and recipient ends (synchronization) is still a difficult task.

(c) Explain why a good cryptographic encryption algorithm will necessarily have a large key size.

(03 marks)

ANSWER IN THIS BOX

All cryptanalytic algorithms are vulnerable to brute force attack, thus requiring a large key size.

(d) What is/are the respective key size/s for the DES, Triple-DES and AES algorithms?

(03 marks)

ANSWER IN THIS BOX

DES 56 bits

Triple DES 112 bits, 168 bits

AES 128 bits, 192 bits, 256 bits

(e) In certain modern applications, the AES symmetric cryptographic system is sometime used instead of the triple DES. State three (3) advantages of AES compared to Triple DES.

(04 marks)

ANSWER IN THIS BOX

Advantages:

AES has larger key sizes.

Decryption works faster than encryption.

Software implementation of AES works faster than software implementation of Triple DES.

AES has a larger block size and it overcomes the security problems related to the smaller block size algorithms such as Triple DES.

(f) Typically, a password should be relatively long enough to provide enhanced security. However, PINs (Personal Identification Numbers) used with ATM cards to draw money out of a cash machine have only four decimal digits. Why is it safe to have PINs of only four digits even though we would normally recommend that passwords be longer than this?

(05 marks)

ANSWER IN THIS BOX

ATM cards use two factor authentication (in addition to the PIN, a valid card must be presented at the ATM machine).

At the ATM machine an intruder can try the PIN only a maximum of 3 times.

(g) The customer details of a bank are held in a confidential manner. They are stored electronically and can only be accessed by authorized personnel by entering their user names and passwords. Describe what is meant by a "one-way function" and how a "one-way function" can be used to cryptographically protect the password file on the bank's computer system.

(06 marks)

ANSWER IN THIS BOX

One-way functions produce a unique code (hash) which represents the given data set.

The data set will not be able to be derived using the hash.

Hash code of the password should be calculated using a one-way function.

Hash code should be saved together with the user name in the password file.

At the verification, hash of the password should be calculated and compared against the hash code in the password file.

3) (a) Describe step-by-step, the key generation process for the RSA public key cryptographic system.

(06 marks)

ANSWER IN THIS BOX

1. Find 2 large prime numbers p and q (100 digits=512bits)

2. Calculate the product n=p*q (n is around 200 digits)

3. Select a large integer e relatively prime to (p-1)*(q-1)

Relatively prime means e has no factors in common with (p-1)*(q-1).

Easy way is to select another prime that is larger than both(p-1) and (q-1).

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

(b) Kamal has RSA public key (e=11, n=91) and RSA private key (d=59, n=91). Nimal has RSA public key (e=23, n=170) and RSA private key (d=7,n=170). Assuming the role of Nimal and showing all steps clearly, encrypt and decrypt the message M=20 be to sent to Kamal.

(07 marks)

ANSWER IN THIS BOX

Kamal	Nimal
Public key e=11, n=91	**Public key e=23, n=170**
Private key d=59, n=91	**Private key d=7, n=170**

Encryption

Nimal should encrypt the message (M=20) with public key of Kamal (e=11,n=91).

$C = M^e \bmod n$

$C= 20^{11} \bmod 91$

C=41

Continued…

Decryption

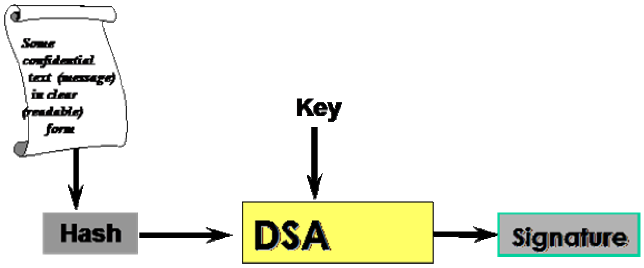
Kamal should decrypt the cipher message(C=41) with his private key (d=59, n=91).

$M = C^{d} \bmod n$
$M= 41^{59} \bmod 91$
$C=20$

(c) Write a protocol for deriving a digital signature, which makes use of a one-way hash function such as SHA-1 and a public key cryptographic system such as RSA.

(06 marks)

ANSWER IN THIS BOX



The student should explain the above diagram as follows:

1. The hash of a document should be calculated.
2. Then the hash should be encrypted using the private key.
3. Encrypted hash (digital signature) should be attached to the document together with the public key.

(d) Give one (1) advantage and one (1) disadvantage of using digital certificates in order to authenticate public keys.

(02 marks)

ANSWER IN THIS BOX

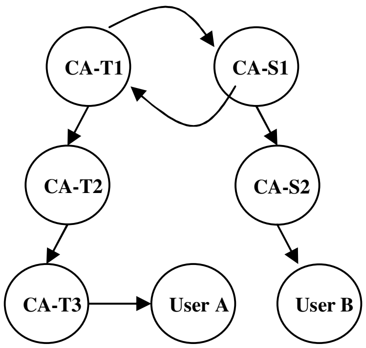
Using a digital certificates to authenticate public keys is a scalable solution.

If a digital certificate is certified by a trusted certification authority, public key in it can be accepted.

In order to obtain a digital certificate, a user should pay a considerable amount to the CA.

A user should trust the certification authority.

(e) User A receives the public key certificate of User B in the following cross-certified multiple PKI domains. What are the certificates which need to be verified by User A. Assume User A trusts only the certificate of CA-T1.



(04 marks)

ANSWER IN THIS BOX

CA-T1, CA-S1, CA-S2, User B

4) (a) Your manager sends you an e-mail containing a screen server while you are at work and suggests that you would love to have the screen server. What should you do? Briefly explain your answer.

(04 marks)

ANSWER IN THIS BOX

I would delete the e-mail because it has three big risks:

1. **Some screen savers contain viruses or other malicious programs and therefore in general, it is risky to put unknown or unsolicited programs or software on a computer.**
2. **Also, in some cases just clicking on a malicious link can infect a computer and unless one is sure that a link is safe, one should not click on it.**
3. **Finally, email addresses can be faked and therefore just because the email says it is from someone you know, you cannot be certain of this without checking.**

(b) Kamala did make sure that her yahoo account was no longer open in the browser window before leaving the computer laboratory. However, Nimal came in after she had used the same browser to re-access her e-mail account. He has started sending emails from it and had caused all sorts of problems. What do you think might have happened here?

(03 marks)

ANSWER IN THIS BOX

The first person probably did not properly log out of her account and therefore the new person could just go to history and access her account. Another possibility is that she did log out, but did not clear her web cache. (This is done through the browser menu to clear pages that the browser has saved for future use.)

(c) At present, many people filter their incoming email to remove (or quarantine) spam. This can be done by individual users on their own computers, or it can be done centrally by their employer or Internet Service provider (ISP), or both.

(i) State an advantage of enforcing it centrally?

(02 marks)

ANSWER IN THIS BOX

Centralized e-mail policy can be enforced.

System maintenance cost and time can be reduced.

(ii) State an advantage of enforcing it on end-user computers?

(02 marks)

ANSWER IN THIS BOX

Personalized spam policy can be enforced.

(iii) Does it make sense to enforce it in both places? Briefly explain your answer.

(04 marks)

ANSWER IN THIS BOX

It makes sense to do it in both places. The central computer can filter obvious spams and forward the doubtful e-mail to the personalized filter of the end user.

(d) E-mail is perhaps the most popular service on the Internet. However, as more people join the Internet, concerns over security are mounting. S/MIME tries to combat these concerns. State the four (4) basic security services that S/MIME provides.

(04 marks)

ANSWER IN THIS BOX

Authenticity

Confidentiality

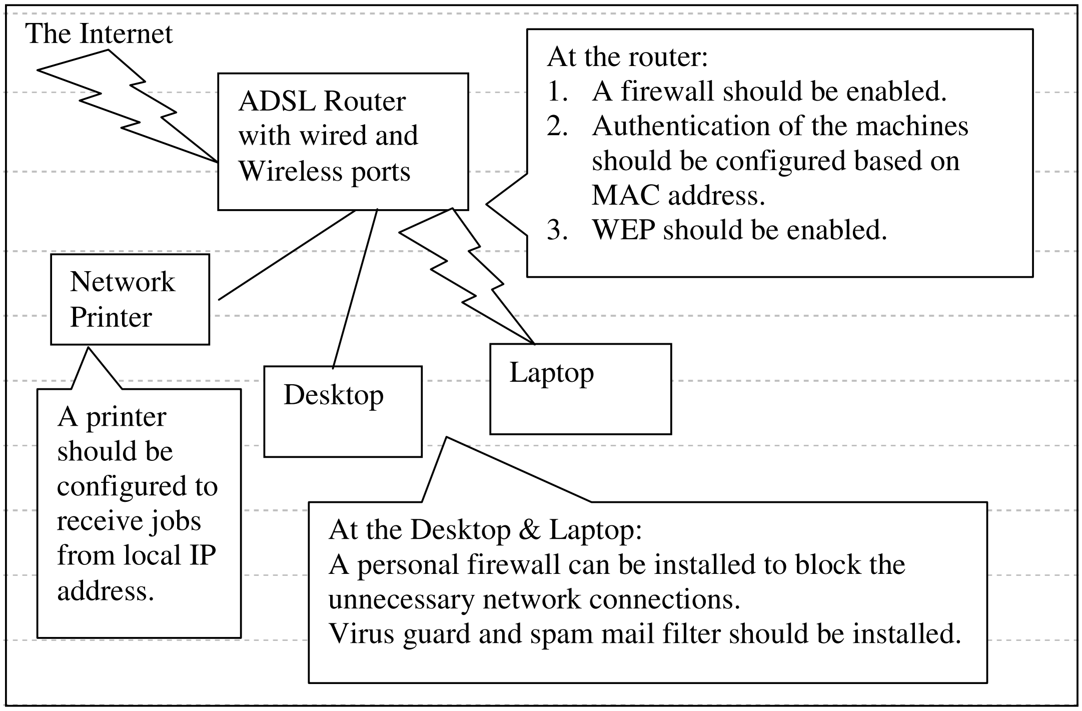
Integrity

Non-repudiation

(e) Sunil has just resigned from his old partnership and is setting up his own company so that he can spend more time with his family. He has set up a small home office and wants to connect it to his existing home Internet (ADSL) connection. He has a powerful desktop machine and a network printer which he will use for his work. He intends to buy a laptop and would like to have wireless access throughout the house. He has asked you to design a secure network infrastructure for this environment. Draw a diagram of the network and explain briefly your security design.

(06 marks)

ANSWER IN THIS BOX



At the router:

1. A firewall should be enabled.
2. Authentication of the machines should be configured based on MAC address.
3. WEP should be enabled.

A printer should be configured to receive jobs from local IP address.

At the Desktop & Laptop:
A personal firewall can be installed to block the unnecessary network connections.
Virus guard and spam mail filter should be installed.

****