UNIVERSITI KUALA LUMPUR
MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL EXAMINATION
JANUARY 2016 SEMESTER

COURSE CODE	:	IKB10103
COURSE NAME	:	INFORMATION SECURITY
PROGRAMME NAME	:	BIT (Hons.) in Computer System Security Bachelor of Computer Engineering (Hons.)
DATE	:	28 MAY 2016
TIME	:	9.00 am – 11.30 am
DURATION	:	2 HOURS 30 MINUTES

INSTRUCTIONS TO CANDIDATES

1. Please CAREFULLY read the instructions given in the question paper.
2. This question paper has information printed on both sides of the paper.
3. This question paper consists of TWO (2) sections. Section A and B..
4. Answer ALL questions in section A .For section B, answer ONE (1) question from question 4 or question 5.
5. Please write your answers on the answer booklet provided..
6. Answer all questions in English language ONLY.

THERE ARE 9 PAGES OF QUESTIONS, INCLUDING THIS PAGE.

SECTION A (Total: 75 marks)

INSTRUCTION: Answer ALL questions.
Please use the answer booklet given.

Question 1

(a) An organization operating in the digital world today need layers of security to provide better protection of organization's assets. Other than personal security, briefly explain other layers of security and its scope.

(6 marks)

(b) The C.I.A. triangle has been considered the industry standard for computer security since the development of the mainframe. Consider an application that allows people to order goods over the Internet. Use C.I.A characteristic to answer following questions.

i. Explain threats this application might cause to purchaser.

(3 marks)

ii. Explain threats this application might cause to the merchant.

(3 marks)

iii. List **THREE (3)** vulnerabilities that could allow these threats to be actualized.

(3 marks)

(c) Public Key Infrastructure (PKI) is integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services enabling users to communicate securely. Discuss **FOUR (4)** ways on how PKI can protect information assets.

(8 marks)

(d) List **TWO (2)** general categories of threat.

(2 marks)

Question 2

(a) Malware, short for malicious software, also known as computer contaminant is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

i. Name **THREE (3)** types of Malware.

(3 marks)

ii. Provide **TWO (2)** differences between worm and viruses.

(4 marks)

iii. Explain how Trojan horse releases its payload.

(2 marks)

(b) Operating System (OS) must be protected from security breaches, such as runaway processes , memory-access violations, stack overflow violations, the launching of programs with excessive privileges, and many others. Explain **FIVE (5)** tips to secure the operating system.

(10 marks)

(c) There is some concern that the humans who are allowed access to a system be trustworthy, and that they cannot be forced into breaching security. However more and more attacks today are made via social engineering, which basically means fooling trustworthy people into accidentally breaching security.

i. Give **THREE (3)** techniques used in social engineering.

(3 marks)

ii. What is *Dumpster Diving*?

(3 marks)

Question 3

(a) Online marketplace eBay is forcing users to change their passwords after a cyber-attack compromised its systems. The US firm said a database had been hacked between late February and early March, and had contained encrypted passwords and other non-financial data. The company added that it had no evidence of there being unauthorised activity on its members' accounts. However, it said that changing the passwords was "best practice and will help enhance security for eBay users".
The California-based company has 128 million active users and accounted for $212bn (£126bn) worth of commerce on its various marketplaces and other services in 2013.It said it would be contacting users to alert them of the issue via email, its website, adverts and social media.

i. Based on your reading, briefly explain **FOUR (4)** reasons why hackers can easily hack the password that the users use.

(8 marks)

ii. There are many applications that are freely available to hack password. Based on the case study given, briefly explain the **TWO (2)** attacks that hackers use to hack the password.

(6 marks)

iii. You as an IT administrator need to enforce a policy of periodic password changes and encourage users to create harder-to-crack passwords. List **THREE (3)** guidelines on how to create strong password.

(6 marks)

(b) The Washington Mutual Bank Scam is one of the examples of dodge as it is used for financial institutions .In this scam, recorded by about.com, the customer of the bank receives an email that appears to be from the Washington Mutual Bank. The sender is recorded as Washington Mutual bank and the subject reads, Washington Mutual Security Alert. The content of the mail is well written and lacks grammar or spelling errors. First off, it apologizes for the inconvenience and goes on to explain that the bank has adopted a new method to transfer money due to past fraudulent activities. It mentions tha t by confirming and updating customers details by clicking on the

embedded URL, they will be able to continue doing their online banking business with them. This URL then brings up the fake Washington Mutual Bank site and supplies the attacker with any details filled in.

i. What is the type of crime that occurred for the above scenario.

(1 mark)

ii. Describe **TWO (2)** steps or actions should be taken for the above scenario

(4 marks)

SECTION B (Total: 25 marks)

INSTRUCTION: Answer ONE (1) of the TWO (2) questions.
Please use the answer booklet given.

Question 4

(a) A cookie theft vulnerability was reported in January 2005 in the Froogle (Google, Inc., Mountain View, California) comparison shopping service. Although the details reported are sketchy, it appears that malicious Java-Script in a URL points to Froogle. Once a user clicks that link, the JavaScript executes a redirect to a malicious Web site, which then steals the user's Google (Google, Inc., Mountain View, California) cookie. This stolen cookie apparently contained the username and password for the "Google Accounts" centralized log in service, information that is used by multiple Google services.

i. Name **ONE (1)** type of web vulnerability associate with the above scenario?

(2 marks)

ii. Explain how cookies action may lead to vulnerabilities for online shopping website.

(5 marks)

iii. Name **TWO (2)** common web application attacks.

(2 marks)

(b) Give **TWO (2)** differences between Asymmetric Encryption and Symmetric Encryption.

(4 marks)

(c) Name **ONE (1)** algorithm for asymmetric or public-key cryptography.

(2 marks)

(d) Cryptography from the Greek words kryptos, meaning “hidden”, and graphein, meaning “to write” is the process of making and using codes to secure the transmission of information.

i. By using Columnar Transposition, decode this ciphertext: **SRYTH NEFRR TEAMT IQSOS KEMEA ALEGM ULU** The keyword is **SECRET**.

(5 marks)

ii. By using The Vegeneres table given, decode: **EZFYAQIBLHFJNOGKU**. The key is **WORD**.

(5 marks)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 1-Vegeneres Table

Question 5

(a) Explain **THREE (3)** reasons why people might be reluctant to use biometrics for authentication.

(6 marks)

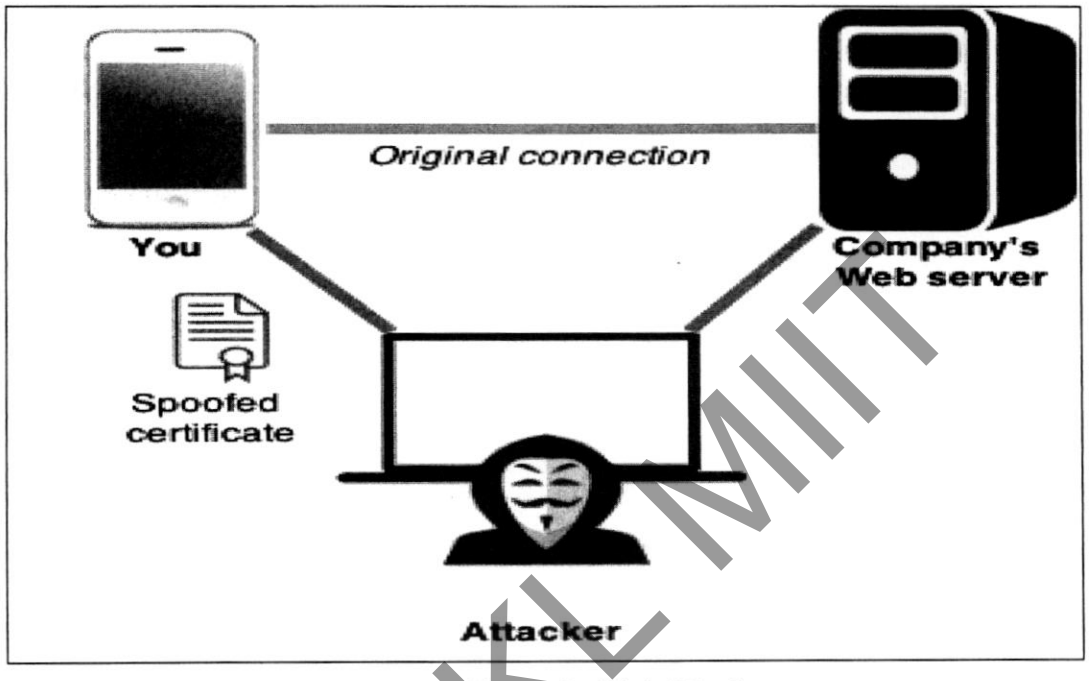

Figure 2 : Web Attack

(c) By referring to the above picture, assuming you are using public WIFI network at a coffee shop or at an airport. Many such networks do not require passwords, allowing bad guys to eavesdrop your communication. While you're browsing the Internet, you might encounter pop-up messages warning you of some computer issues. Believing these warnings, you click on them and fall into the trap set by attackers. They exploit this vulnerability to create fake certificates, fooling you to think that you're still communicating with trustable sources.

i. What is the type of classification attack related to the above case .

(1 mark)

ii. Name type of the network attack in the above case scenario.

(1 mark)

iii. Name **TWO (2)** techniques involved in the above attack.

(3 marks)

iv. Name **FOUR (4)** OSI layers potentially participate in the above attack.

(6 marks)

v. Explain **ONE (1)** threat might be facing by a company suffering for the above attack.

(2 marks)

(d) Justify **THREE (3)** reasons why one network's having two separate firewall, the first is a packet filtering gateway and the second is an application proxy. Explain **ONE (1)** reason why these separation is preferable

(6 marks)

END OF EXAMINATION PAPER