AeU
asiaeuniversity

FINAL EXAMINATION
SEPTEMBER 2018 SEMESTER

SUBJECT CODE	:	CSC610
SUBJECT NAME	:	CRYPTOGRAPHY
LEVEL	:	MASTER'S DEGREE
TIME / DURATION	:	9.00 AM - 12.00 NOON (3 HOURS)
DATE	:	6 JANUARY 2019

INSTRUCTIONS TO CANDIDATES

1. Read the instructions given in the question paper CAREFULLY.
2. This question paper is 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 and Section B.
5. Write your answers in the answer booklet provided.
6. Answer all questions in English.

THERE ARE FOUR (4) PAGES OF QUESTIONS, EXCLUDING THIS PAGE.

SECTION A (Total: 40 marks)
INSTRUCTION: Answer ALL questions.
Please use the answer booklet provided.

Question 1

The protection of information security is essentially based on the CIA triad goals that are **confidentiality, integrity** and **availability**. Discuss how cryptography and encryption techniques allow us to address the issue of confidentiality, integrity and availability.

[10 marks]

Question 2

a) Briefly explain how Feistel cipher that was developed by an IBM Watson Research work.

(4 marks)

b) Digital Encryption Standard (DES) was developed in 1975 with support from the National Security Agency (NSA). It became an accepted standard in 1981 and was extensively utilized from there on. The crypto community later created the Triple DES (also known as 3DES). Explain the functions of DES and Triple DES.

(6 marks)

[Total: 10 marks]

Question 3

A message authentication code (MAC) is an authentication tag which results from applying an authentication system with a secret key to a message.

a) Differentiate between digital signatures and Message Authentication Code (MAC).

(6 marks)

b) Identify **FOUR (4)** types of MACs.

(4 marks)

[Total: 10 marks]

Question 4

A protocol is a sequence of steps, concerning two or more entities, designed to complete a task.

a) Provide **FOUR (4)** characteristics of protocols.

(4 marks)

b) With appropriate examples, explain **THREE (3)** types of active attacks against protocols.

(6 marks)

[Total: 10 marks]

SECTION B (Total: 60 marks)

INSTRUCTION: Answer ALL questions.

Please use the answer booklet provided.

Question 1

A digital code is attached to an electronically transmitted message that uniquely identifies the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be.

a) Provide **ONE (1)** example that shows the use of a digital certificate to confirm user's identity.

(4 marks)

b) Provide **FOUR (4)** characteristics of Digital Signatures.

(4 marks)

c) With an appropriate diagram, explain the process of digital signature and label your diagram accordingly.

(12 marks)

[Total: 20 marks]

Question 2

In present day of cryptography, people speak about the infeasibility of breaking the encryption system and computing information concerning exchanged messages. A cryptographic algorithm works in conjunction with a key which could be a word, digit or expression to encipher a plain-text. The security of the encrypted data is totally depends on the strength of the cryptographic algorithm and the secrecy of the key.

a) With appropriate examples or diagrams, describe the **accidental threats**, **passive attack** and **active attack** to cryptography.

(12 marks)

b) With an appropriate example, describe Caesar cipher attack and explain the strength of this algorithm.

(8 marks)

[Total: 20 marks]

Question 3

a) A poly-alphabetic substitution a cipher called Vigenere Cipher uses a 26x26 table with A to Z as the row heading and column heading as shown in Figure Q3. Using the Viginere cipher with **EXAM** as a keyword, encrypt plaintext **"SECURITY "** and **"CRYPTOGRAPHY"**.

(10 marks)

b) The Playfair cipher is a manual symmetric encryption technique invented by Charles Wheatstone in 1824. It employs a 5 by 5 square which is made up of the 25 letter of the alphabet. With the given secret key **"NETWORK SECURITY"**,

i. Sketch a 5 by 5 square playfair cipher key.

ii. Encrypt the plaintext **"YOUR SECRET"** and decrypt the ciphertext **"DZ BO VU VE GD IU ZK EY YS XV ZC"**.

(10 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 Q3

[Total: 20 marks]

END OF QUESTION PAPER