THE MANCHESTER METROPOLITAN UNIVERSITY

FACULTY OF SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING, MATHEMANTICS AND DIGITAL TECHNOLOGY

ACADEMIC YEAR 2016-2017:

MIDSEMESTER SESSION

Examination for
MSc Cyber Security

UNIT 6G7Z1009: Introduction to Computer Forensics and Security

Duration: 3 hour(s)

Instructions to Candidates

Please answer **FOUR** questions (**Two** questions each from both **Section A** and **Section B**)

Each question carries 25 marks.

Students are permitted to use their own calculators subject to the standard Faculty conditions.

Section A Questions (1 - 3):

1. (a) You are a digital forensic investigator in a forensic team. The team has been asked to go to a suspect scene. Briefly describe the five steps of the forensic computing process you are going to conduct. [11]

(b) During the computer forensics data acquisitions: state two data formats could be used and two hashing algorithms are commonly used? [4]

(b) What is a hardware write blocker and what is it used for? [4]

(c) List two major advantages of using automated forensics tools in report writing? [6]

2. In FAT file system; answer the following questions:

(a) List three pieces of information could be found in the volume boot record? [3]

(b) What is FAT1 and what its role? [2]

(c) How many copies of FAT does each FAT32 volume maintain in its default configuration? [2]

(d) What is the size of each directory entry in a FAT file System in Bytes length? [2]

(e) List four types of information a file's directory entry in a FAT file system store about itself? [4]

(f) What are the three things that occur when a file is created in a FAT32 file system? [6]

(g) What is meant by file logical size; file physical size and what is the area between the end of a file's logical size and file's physical size called? [6]

Continued

3. (a) Consider the scenario where a file must be written to disk; the file size is 2560 bytes. If the disk block size is 512 bytes, a pointer to a disk block occupies 4 bytes, and an index block is 1 disk block in size. How many disk blocks this file is going to take when the file system is allocated with:

(i) Contiguous allocation
(ii) Linked allocation
(iii) Indexed allocation

Fully explain your answer and include all calculation details

[10]

(b) Explain the key features of the NTFS file system. Your answer should include information concerning: the master file table, character sets, resident and nonresident attributes, and $Bitmap. [9]

(c) Highlight the forensic importance of each of the following files in the Windows XP Operating System:

(i) FileName.LNK;

(ii) FileName.SPL;

(iii) Thumbs.DB;

[6]

Section B Questions (4 - 6):

4. a) Explain the functions of a security policy and system should provide?

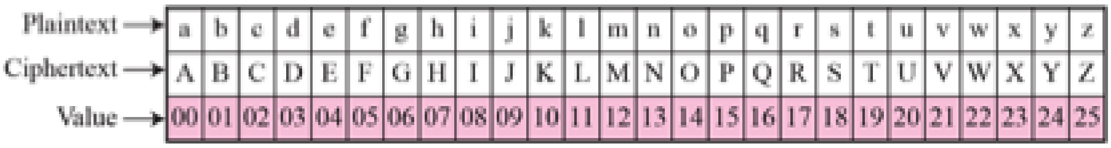
[20]

b) Define security attacks and the type of attacks [5]

5. a) Explain computational security, provable security and unconditional security [9]

b) Use symmetric ciphers to encrypt message “welcomtru” and decrypt message “XYZANBJ”. [16]

The representation of characters in modulo 26 is described as follows:



Plaintext →	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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The mathematical equations for encryption and decryption can be described as follows:

Continued

$$\text{Encryption } E_{(k)} : i \rightarrow i + k \bmod 26$$

$$\text{Decryption } D_{(k)} : i \rightarrow i - k \bmod 26$$

i represents the messages (plaintext or cipher), k represents a symmetric key. In this case k=16

6. a) Explain what Zero-knowledge proof system is ? Give an example of any cryptographic algorithm that is a zero-knowledge proof system and explain why? [10]

b) i) Explain how Needham Schroeder Protocol operates and use the diagram to assist your analysis [10]

ii) Explain the vulnerability in Needham-Schroeder protocol and how to overcome it? [5]

END OF QUESTIONS

Continued