



**6G7Z1009 : INTRODUCTION TO COMPUTER FORENSICS AND SECURITY**

**Duration : 3 hours**

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. In the context of EnCase digital forensics, please answer the following questions:

- (a) What is a physical file size? [2]
- (b) What is the area between the end of a file's logical size and the file's physical size called? [2]
- (c) How many copies of the FAT does each FAT32 volume maintain in its default configuration? [2]
- (d) How does EnCase verify that the evidence file contains an exact copy of the suspect's hard drive? [2]
- (e) What is a hardware write blocker and what it's used for? [4]
- (f) What is **UNICODE**? [3]
- (g) Within the EnCase Environment, what does the File Signatures function do? [2]
- (h) Give **THREE** examples of compound files EnCase can open in hierarchical format? [3]
- (i) Within EnCase evidence file structure; list **THREE** pieces of information can be found in the acquisition information section? [3]
- (j) What does EnCase do when a deleted file's starting cluster number is assigned to another file? [2]

2. Figure **Q2.1** shows a basic FAT directory entry structure and its hexadecimal and ASCII data associated from a Windows OS based machine which uses Intel processor, find out the following:

**FIGURE Q2.1:** Basic FAT directory entry structure and it Hex and ASCII data associated.

Count	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
HEX	E5	69	64	64	65	6e	31	32	54	58	54	20	18	84	82	70	9F	2D	9F	2D	00	00	F1	71	9F	2D	16	02	80	00	00	00
ASCII	i	d	d	d	e	n	1	2	T	X	T				p	-	-	-	-				q	-	-							
	Status	File Name							Extension			Attributes	Reserved	Created		Date	Accessed	Unused	Written		Time	Date	Starting Cluster	File Size								

(a) What is the file name, including the extension? [2]

(b) Briefly explain what the starting cluster section contains and how it is used? [4]

(c) What is the status of the file; and how did you identify it? [2]

(d) What is the logical file size and how did you identify it? [5]

(e) When was the file created; including date and time; show your calculations? [12]

3. (a) Briefly explain how contiguous allocation differs from linked allocation in terms of performance, disk space management, file sizes management, random access of blocks? [8]

(b) What is the 7-bit ASCII; within the 7-bit ASCII table: how many codes addressed; what types of codes represented and what types of characters? [9]

(c) Windows XP operating system does produce system data and artefacts that can be used as digital evidence. Describe **FOUR** types of the generated data and artefacts. [8]

### SECTION B Questions (4 - 6):

4. (a) Explain what is meant by a public key algorithm and explain the difference between Diffie-Hellman and RSA. [7]

b) The acronym CIA (confidentiality, integrity and availability) is often used as a basis of classifying computing and network security services. List three other security services. Explain the meaning of the terms: confidentiality, integrity and availability and the three 'additional' services and discuss 6 situations where each of them would be individually implemented [18]

5. a) Explain the block cipher and give an example that uses the block cipher method. [7]

b) Describe one-time pad and explain why it is secure [7]

c) Use symmetric ciphers to encrypt message "promised" and decrypt message "FOG". [11]

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:

Encryption  $E_{(k)} : i \mapsto i + k \text{ mod } 26$

Decryption  $D_{(k)} : i \mapsto i - k \text{ mod } 26$

$i$  represents the messages (plaintext or cipher),  $k$  represents a symmetric key. In this case  $k=20$

6. a) In the context of X.509 PKI, explain what is meant by Certificate Authority (CA) and the basic tasks of CA [4]
- b) Explain Digital signature and Digital certificate, describes issues with Digital signature. [4]
- c) Explain Message authentication and Message Authentication Code, and why message authentication is necessary [6]
- d) With the aid of a diagram, state and explain what Kerberos is, how Kerberos works, and it's pros and cons [11]

**END**