FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

DEPARTMENT OF INFORMATION AND MEDIA TECHNOLOGY

SECOND SEMESTER 2016/2017 EXAMINATION

COURSE CODE:	IMT 526
COURSE TITLE:	COMPUTER SECURITY TECHNIQUES
CREDIT UNITS:	2
TIME ALLOWED:	2 HOURS
COURSE LECTURER(S):	DR. ISHAQ O. OYEFOLAHAN AND MR. S.O. GANIYU
NUMBER OF QUESTIONS:	3
NUMBER OF PAGES:	2

INSTRUCTIONS

- Answer all questions
- Do **not** use red pen
- Please use a clear handwriting
- This exam is closed book, closed notes, closed laptop and closed cell phone
- Please use non-programmable calculators only

Question 1

(a) Discuss the following cryptographic concepts:

(i) monoalphabetic cipher; (4 marks)

(ii) polyalphabetic cipher; and (4 marks)

(iii) one-time pad. (4 marks)

(b) Write short note on Euclidean algorithm. (4 marks)

(c) Explain the importance of unicity distance to cryptographer. (4 marks)

Question 2

(a) i. Briefly describe cryptanalysis. (4)

ii. State the three (3) cryptanalysis methods. (3)

iii. Why is perfect secrecy impractical in information security? (4 marks)

(b) i. List the factors that determine the complexity of encryption algorithm. (4 marks)

ii. Why is complexity theory necessary in encryption process? (5 marks)

Question 3

(a) i. Explain audio scrambling. (4 marks)

ii. As a prospective media security professional, explain why subscribers to paid television services (e.g. StarTimes and GOtv) require decoder to view their channels. (5 marks)

(b) i. Briefly describe the mathematical procedures employed in Data Encryption Standard. (3 marks)

(ii) Use **RSA** token defined by (253, 5, 8) to encrypt each character of the word **STUDY** to its numeric values. The ASCII code is provided in Table 1. (8 marks)

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

Table 1: ASCII

Best of luck.