FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

DEPARTMENT OF INFORMATION AND MEDIA TECHNOLOGY

SECOND SEMESTER 2015/2016 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:	3

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) List any four (4) subdivisions of number theory except computational number theory. (4 marks)

(b) (i)What is computational number theory? (2 marks)

(ii) Explain the importance of computational number theory to computer security. (6 marks)

(c) (i) Which class of complexity will you categorize ***travelling sales man*** problem? (2 marks)

(ii) Explain any two (2) ways to optimize travelling sales man problem. (6 marks)

Question 2

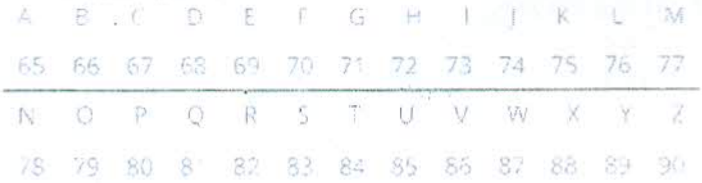
(a) (i) State the general Euclidean algorithm. (3 marks)

(ii) Briefly describe audio scrambling. (4 marks)

(iii) List the four (4) audio scrambling techniques. (4 marks)

(b) (i) Describe the three (3) basic steps to decrypt RSA cipher text. (3 marks)

(ii) Encrypt the plaintext **RAM** with RSA token (89, 5, 6) and using the ASCII table below. (6 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

Question 3

(a) Explain iterated block cipher. (2 marks)

(b) Explain the following concepts; (8 marks)

i. Threshold scheme ii. Unicity distance

(c) You are hired as media security expert to improve cryptosystem of news management system. The management system known as FutInfoBase contains classified news contents and it is currently running on a legacy system. The computing resources of the legacy system could only allow Data Encryption Standard (DES) to be implemented on FutInfoBase when it was developed. The system administrator of FutInfoBase realized that DES is highly susceptible to present security threats. However, the administrator could not replace DES with any advanced cryptosystems due to some constraints.

(i) What can you do to enhance the DES as security expert so that FutInfoBase will continue to run on the legacy system? (6 marks)

(ii) Which attributes will you use to measure the complexity of your enhanced DES? (4 marks)

Best of luck.