FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

DEPARTMENT OF INFORMATION AND MEDIA TECHNOLOGY

SECOND SEMESTER 2017/2018 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 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) Write the formal definition of Shannon theory of perfect secrecy. (4 marks)

(b) What is the next number in the sequences below? (2 marks each)

(i) 6; 28; 496;

(ii) 3; 7; 11; 15;

(iii) (3,4,5); (5,12,13); (7,24,25);

(c) Use **RSA** token defined by (253, 5, 8) to decrypt each character of the word **ICTA** 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

(d) Explain one-way cipher and list three (3) of such ciphers that are yet to be broken. (6 marks)

Question 2

(a)Why is complexity theory important in the field of cryptography? (5 marks)

(c) Explain one-time pad.(5 marks)

(b)Give detail explanation of threshold scheme. (10 marks)

Question 3

(a) (i) Use Euclidean Algorithm to find the gcd of 1292240050 and 79430316. (7 marks)

ii. Describe the contribution of Egyptian to early cryptography. (3 marks)

(b)You are hired to work with a team of media professionals overseeing online discussion between your organisation and a foreign business partner. The discussion involves exchange of vital and strategic information between the two parties through video conferencing. Address the underlisted concerns about the discussion as a team member with average knowledge of media security.

(i) What are the possible dangers that your organisation could be exposed to during the period of the discussion? Support your explanation with at least three (3) points. (6 marks)

(ii) List four (4) methods to avoid the possible dangers in identified in (i) above. (4 marks)

Best of luck!