Programme Code: TU857, TU856, TU858

Module Code: CMPU 4007 CRN: 22531, 22421, 31084

TECHNOLOGICAL UNIVERSITY DUBLIN

CITY CAMPUS

BSc. (Honours) Degree in Computer Science (Infrastructure)

BSc. (Honours) Degree in Computer Science

BSc. (Honours) Degree in Computer Science (International)

Year 4

SEMESTER 1 EXAMINATIONS 2021/22

Advanced Security 1

Internal Examiner: Dr. Aneel Rahim

Dr. Paul Doyle

External Examiner: Sanita Tifentale – TU856

Mr. Pauline Martin – TU857 Pamela O'Brien – TU858

Two Hours

INSTRUCTIONS TO CANDIDATES

Answer THREE questions out of FOUR.

ALL QUESTIONS CARRY EQUAL MARKS.

ONE (1) COMPLIMENTARY MARK WILL BE GIVEN.

1. (a)	1. (a) Consider an online banking system in which users provide an account number and password to access the bank account and transfer money online. Mention example of CIA (confidentiality, integrity, and availability) requirements associated with the											
	system. Also discussion the system	ss the level	of imp	ortan	ce (lov	v, me	dium	, hig	h) of	f each	_	uirement 12 marks)
											`	,
(b)	Briefly explain the	two different	ent type	es of p	assive	secu	rity a	ittack	KS.		((9 marks
(c)	In relation to classi	cal encrypt	ion tec	hniqu	es, ex	olain 1	the fo	ollow	ing			
	(i) Rail Fence Ci	ipher										(4 marks)
	(ii) One-Time Pa	d										(4 marks)
	(iii) Row Transpo	sition Ciph	er									(4 marks)
2. (a) Encrypt the message using Vigenère Cipher? (10 marks) Key: 9 0 1 7 23 15 21 14 11 11 2 8 9 Plaintext: sendmoremoney							narks)					
	Key											
	Plaintxt											
	Cipherext											
	Discuss the structurillustrate your answ Explain the following	ver.	l Cipho	er (end	eryptic	on and	l deci	rypti	on).	Use d	_	am to (11 marks)
	(i) Diffusion and	l Confusion	ı									(4 marks)
(ii) Steam Cipher and Block Cipher								(4 marks)				
	(iii) Strict avalanche criterion (SAC) and Bit independence criterion (BIC)						C)	(4 marks)				

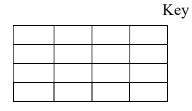
- **3. (a)** Explain the block Cipher Operation of CBC (Cipher Block Chaining). Use a diagram to illustrate your answer (9 marks)
 - (b) Explain the confidentiality and authentication using public-key cryptosystems. Use diagram to illustrate your answer. (12 marks)
 - (c) (i) Perform the AES initial AddRoundKey Transformation on the matrix.

(6 marks)

B9	94	57	75
E4	8E	16	51
47	20	9A	3F
C5	D6	F5	3B

DC	9B	97	38
90	49	FE	81
37	DF	72	15
B0	EF	3F	A7

Plain Text

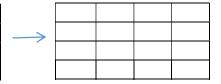


Output

(ii) Perform AES Shift Row Transformation on the matrix below.

(6 marks)

65	0F	C0	4D
74	C7	E8	D0
70	FF	E8	2A
75	3F	CA	9C



i. (a)	in relation to pseudorandom number generators, explain the following:					
	(i)	True Random Number Generator (TRNG)	(4 marks			
	(ii)	Pseudorandom Number Generator (PRNG)	(4 marks)			
	(iii)	Blum Blum Shub (BBS) Generator	(4 marks)			
(b) Write a brief summary of what you have learned in relation to number theoremore than 400 words.						
(c)	De	scribe the five possible attacks on the RSA algorithm.	(10 marks)			