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.

p	Consider an onling assword to access CIA (confidential)	s the bar ty, integ	k acc rity, a	ount ind a	and vaila	trans bilit	sfer 1 y) re	mon quir	ey oi emei	nline nts a	ssoc	ntio: iated	n exa	umple of the
	ystem. Also discuon the system	iss the le	evel of	t imp	orta	nce (low.	, me	dıum	ı, hıg	gh) o	t eac		quirement (12 marks)
(b) E	Briefly explain the	e two dif	ferent	t type	es of	pass	ive s	secu	rity a	ıttac]	ks.			(9 marks
(c) I	n relation to class	ical enci	yptio	n tec	hniq	ues,	expl	ain t	he fo	ollov	ving			
((i) Rail Fence C	Cipher												(4 marks)
((ii) One-Time Pa	ad												(4 marks)
((iii) Row Transp	osition C	Cipher	•										(4 marks)
ŀ	Encrypt the messa Key: 9 0 1 7 23 Plaintext: sendmo Key Plaintxt Cipherext	3 15 21	14 1		-								(10 1	marks)
i	Discuss the structual llustrate your ansets Explain the follow	wer.		Ciphe	er (ei	ncryj	otion	and	l dec	rypti	on).	Use	diag	ram to (11 marks)
((i) Diffusion an	d Confu	sion											(4 marks)
(ii) Steam Cipher and Block Cipher								(4 marks)						
((iii) Strict avalan	che crite	erion (SAC	() and	d Bit	inde	epen	denc	ce cri	terio	on (E	SIC)	(4 marks)

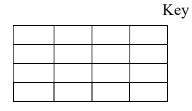
- **3. (a)** Explain the block Cipher Operation of CBC (Cipher Block Chaining). Use a diagram to illustrate your answer (9 marks)
 - (b) Explain the confidentiality and authentication using public-key cryptosystems. Use diagram to illustrate your answer. (12 marks)
 - (c) (i) Perform the AES initial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

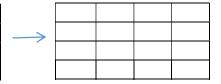


Output

(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)				
. ,		e a brief summary of what you have learned in relation to number theorethan 400 words.	ry with no (11 marks)				
(c)	De	scribe the five possible attacks on the RSA algorithm.	(10 marks)				