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) Consider an online password to access CIA (confidentialit system. Also discus on the system	the bank y, integri	account ity, and a	t and t vailal	trans bility	fer 1 y) re	non quir	ey oi emei	nline nts a	. Me	ntion ated	n exa with th rec	mple of the
(b) Briefly explain the	two diffe	erent typ	es of 1	pass	ive s	secui	rity a	ıttacl	KS.			(9 marks
(c) In relation to classi	cal encry	ption tec	chniqu	ies,	expl	ain t	he fo	ollov	ving			
(i) Rail Fence Ci	pher											(4 marks)
(ii) One-Time Pa	d											(4 marks)
(iii) Row Transpo	sition Ci	pher										(4 marks)
2. (a) Encrypt the messa. Key: 9 0 1 7 23 Plaintext: sendmon	15 21	14 11 1		ner?							(10 1	narks)
Plaintxt												
Cipherext												
Cipilcicxt												
 (b) Discuss the structural illustrate your answer. (c) Explain the following (i) Diffusion and (ii) Steam Cipher. (iii) Strict avalance 	ver. Ing items Confusi and Blo	on ck Ciphe	er									ram to (11 marks) (4 marks) (4 marks) (4 marks)

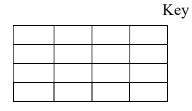
- **3. (a)** Explain the block Cipher Operation of CBC (Cipher Block Chaining). Use a diagram to illustrate your answer (9 marks)
 - (b) Explain the confidentiality and authentication using public-key cryptosystems. Use diagram to illustrate your answer. (12 marks)
 - (c) (i) Perform the AES initial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

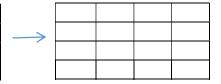


Output

(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)			