DUBLIN INSTITUTE OF TECHNOLOGY

DT211C/4 BSc. (Honours) Degree in Computer Science (Infrastructure)

DT228/4 BSc. (Honours) Degree in Computer Science

DT282/4 BSc. (Honours) Degree in Computer Science (International)

DT8900/1 International Pre-Masters for MSc in Computing

WINTER EXAMINATIONS 2018/2019

ADVANCED SECURITY 1 [CMPU4007]

DR. ANEEL RAHIM
DR. DEIRDRE LILLIS
DR. DAVID MALONE – DT211C
MR. PATRICK CLARKE – DT228/DT282

MONDAY 14TH JANUARY 9.30 A.M. – 11.30 A.M.

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) List and briefly define categories of security mechanisms. (12 marks)

(b) Briefly define the Row Transposition Cipher with the help of examples. (11 marks)

(c) What is the difference between passive and active security attacks? (10 marks)

2. (a) What are two problems with the one-time pad? (6 marks)

(b) Encrypt the plaintext "meet me after the toga party" using Rail Fence Cipher and the key depth is 2. (10 marks)

(c) Explain a Feistel Cipher design features in detail. (10 marks)

(d) What is the difference between diffusion and confusion? (7 marks)

3. (a) Explain Euler's and Fermat's Theorems with help of example. (12 marks)

(b) Explain the Miller-Rabin Algorithm with the help of example. (9 marks)

(c) Explain any two Block Cipher Modes of Operation. Use a diagram to illustrate your answer. (12 marks)

4. (a) What are the roles of the public and private key in Public-Key Cryptosystems? Use a diagram to illustrate your answer. (12 marks)

(b) Describe five possible attacks on the RSA algorithm. (10 marks)

(c) Perform the AES SubBytes Transformation on matrix below with the help of S-box. (11 marks)

EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

→

Table 5.2 AES S-Boxes

		y														
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

(a) S-box