13.01.20

09.30 - 11.30am

CMPU 4007 Advanced Security 1

Basement 1, Kevin Street

Programme Code: DT211C, DT228, DT282
Module Code: CMPU 4007
CRN: 22531, 22421, 31084

TECHNOLOGICAL UNIVERSITY DUBLIN

KEVIN STREET 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 2019/20

Advanced Security 1

Dr. Aneel Rahim
Dr. Deirdre Lillis
Dr. David Malone – DT211C
Mr. Patrick Clarke – DT228/282

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)** Explain the basic model of Network Security. Use a diagram to illustrate your answer.

(12 marks)

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

(c) Briefly explain the four different types of active security attacks. (10 marks)

2. **(a)** Encrypt the plaintext "attack postponed until two am xyz" using Row Transposition Cipher and the key is 4312567? (12 marks)

(b) Explain the Feistel Cipher encryption and decryption with the help of a diagram.

(12 marks)

(c) In relation to DES (Data Encryption Standard) algorithms explain the following

i. Avalanche effect (9 marks)

ii. Timing attacks

iii. Number of Rounds

3. (a) Explain the Extended Euclidean Algorithm with the help of an example. (12 marks)

(b) Explain the block Cipher Operation of Electronic Codebook Mode (ECB) and Counter Mode (CTR). Use a diagram to illustrate your answer. (12 marks)

(c) In relation to number theory explain the following (9 marks)

i. Division Algorithm

ii. Chinese Remainder Theorem

iii. Euler's totient function

4. (a) Discuss the six ingredients of public-key encryption scheme. (12 marks)

(b) Explain the concept of RSA encryption/decryption. Use example to illustrate your answer. (9 marks)

(c) See the next page.

(c)

i. Perform the AES SubBytes Transformation on matrix below with the help of S-box. (6 marks)

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

→

ii. Perform the AES shift Row Transformation on matrix below. (6 marks)

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

→

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