Programme Code: TU857, TU856, TU858
Module Code: CMPU 4007

TECHNOLOGICAL UNIVERSITY DUBLIN

Grangegorman

TU857- BSc. (Honours) Degree in Computer Science (Infrastructure)
TU856- BSc. (Honours) Degree in Computer Science
TU858- BSc. (Honours) Degree in Computer Science (International)
TU821- BSc. (Honours) Degree in Electrical & Electronic/ Computer & Communications Engineering

Year 3 & 4

SEMESTER 1 EXAMINATIONS 2023/24

CMPU 4007 Advanced Security 1

Internal Examiner(s): Dr. Aneel Rahim,
Dr. Paul Doyle

External Examiner(s): Sanita Tifentale – TU856, TU858
Dr. Charles Markham – TU857

Instructions To Candidates: ANSWER **THREE** QUESTIONS OUT OF **FOUR**.
ALL QUESTIONS CARRY EQUAL MARKS.
ONE (1) COMPLIMENTARY MARK WILL BE GIVEN.

Exam Duration: 2 hours

Special Instructions /Handouts/ Materials Required:

1. (a) Encrypt the plaintext "meet me after the toga party" using Rail Fence Cipher and the key depth is 2? (9 marks)

(b) 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 discuss the level of importance (low, medium, high) of each requirement on the system. (12 marks)

(c) In relation to classical encryption techniques, explain the following

(i) One Time Pad (4 marks)

(ii) Brute force Attack (4 marks)

(iii) Row Transposition Cipher (4 marks)

2. (a) Describe the encryption and decryption process of Feistel Cipher. Use diagram to illustrate your answer. (10 marks)

(b) Explain the Fermat's Theorem and Euler's Theorem. Use example to illustrate your answer. (12 marks)

(c) In relation to number theory, explain the following

(i) Divisibility (3 marks)

(ii) Modular Arithmetic (4 marks)

(iii) Euclidean Algorithm (4 marks)

3. (a) In relation to public key cryptography, explain what the Bob achieve in term of confidentiality and authentication in the following scenarios.

(i) Bob encrypt a message with Alice public key and send it to Alice. (4 marks)

(ii) Bob encrypt a message with his private key and send it to Alice. (4 marks)

(iii) Bob first encrypt with his private key and then with Alice public key and send it to Alice. (4 marks)

(b) Briefly discuss the ShiftRows and AddRoundKey function of AES algorithm. Use example to illustrate your answer. (12 marks)

(c) What requirements must a public-key cryptosystems fulfill to be a secure algorithm? (9 marks)

4. (a) Explain in your own words that what you have learned in relation to the True Random Number Generator (TRNG) and Pseudorandom Number Generator (PRNG). Do not write more than 400 words. (10 marks)

(b) Discuss the Double DES and explain the meet in the middle attack. (11 marks)

(c) Perform the DES initial permutation on the Plaintext: 02468aceeca86420. You can use the table 1(Plaintext in Binary) and table 2 (Initial Permutation (IP)). (12 marks)

Bit Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Plaintext	0	0	0	0	0	0	1	0	0	1	0	0	0	1	1	0	1	0	0	0	1	0	1	0	1	1	0	0	1	1	1	0

Bit Number	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
Plaintext	1	1	1	0	1	1	0	0	1	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	1	0	0	0	0	0

Table 1 Plaintext *in Binary*

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Table 2 Initial Permutation (IP)