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 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)

**(b)** Briefly explain the two different types of passive security attacks. (9 marks

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

**(i)** Rail Fence Cipher (4 marks)

**(ii)** One-Time Pad (4 marks)

**(iii)** Row Transposition Cipher (4 marks)

**2. (a)** Encrypt the message using Vigenère Cipher? (10 marks)

**Key:** 9 0 1 7 23 15 21 14 11 11 2 8 9
**Plaintext:** sendmoremoney

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key | | | | | | | | | | | | | |
| Plaintxt | | | | | | | | | | | | | |
| Cipherext | | | | | | | | | | | | | |

**(b)** Discuss the structure of Feistel Cipher (encryption and decryption). Use diagram to illustrate your answer. (11 marks)

**(c)** Explain the following items

**(i)** Diffusion and Confusion (4 marks)

**(ii)** Steam Cipher and Block Cipher (4 marks)

**(iii)** Strict avalanche criterion (SAC) and Bit independence criterion (BIC) (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 |

Plain Text

| | | | |
|---|---|---|---|
| DC | 9B | 97 | 38 |
| 90 | 49 | FE | 81 |
| 37 | DF | 72 | 15 |
| B0 | EF | 3F | A7 |

Key

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

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 |

→

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

**4. (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)

**(b)** Write a brief summary of what you have learned in relation to number theory with no more than 400 words. (11 marks)

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