Programme Code: TU857, TU856, TU858
Shared with: TU821
Module Code: CMPU 4007
CRN: 22531, 22421, 31084, 36352

# TECHNOLOGICAL UNIVERSITY DUBLIN

**CITY CAMPUS - 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 2024/25

## CMPU 4007 Advanced Security 1

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

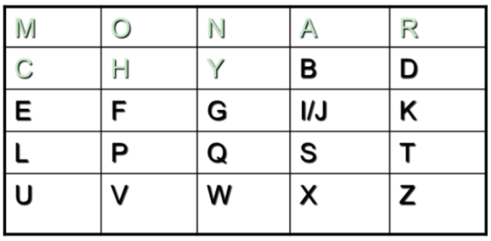
**External Examiner(s):** Dr. Jamal Abdul Nasir – TU857
Dr. Colm O'Riordan– TU856, TU858

***Exam Duration:*** **2 hours**

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

**1. (a)** Using the Figure 1: Playfair Key matrix. (12 marks)

Encrypt the message “AR MU HS EA”.



| | | | | |
|---|---|---|---|---|
| M | O | N | A | R |
| C | H | Y | B | D |
| E | F | G | I/J | K |
| L | P | Q | S | T |
| U | V | W | X | Z |

*Figure 1: Playfair Key Matrix*

**(b)** Using the Vigenère cipher, encrypt the word “explanation” using the key *leg*. (12 marks)

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

**(i)** Steganography (3 marks)

**(ii)** Rotor Machines (3 marks)

**(iii)** Two difficulties of One-Time Pad (3 marks)

**2. (a)** Write a summary (no more than 400 words) of Advanced Encryption Standard (AES). In your answer, discuss the AES Encryption Process and AES Transformation Functions. (12 marks)

**(b)** In Public Key Cryptography, what are the roles of the public and private key. Use a diagram to illustrate your answer. (12 marks)

**(c)** Discuss the encryption and decryption process of RSA. Use example to illustrate your answer. (9 marks)

**3. (a)** What are three broad categories of applications of public-key cryptosystems? (9 marks)

**(b)** Write a summary (no more than 400 words) of Number Theory. In your answer, discuss the Euclidean algorithm, Fermat's Theorem and Miller-Rabin Algorithm. (12 marks)

**(c)** The structure of Feistel Cipher is shown in the Figure 2. Write the missing labels in the encryption and decryption process of Feistel Cipher. (12 marks)

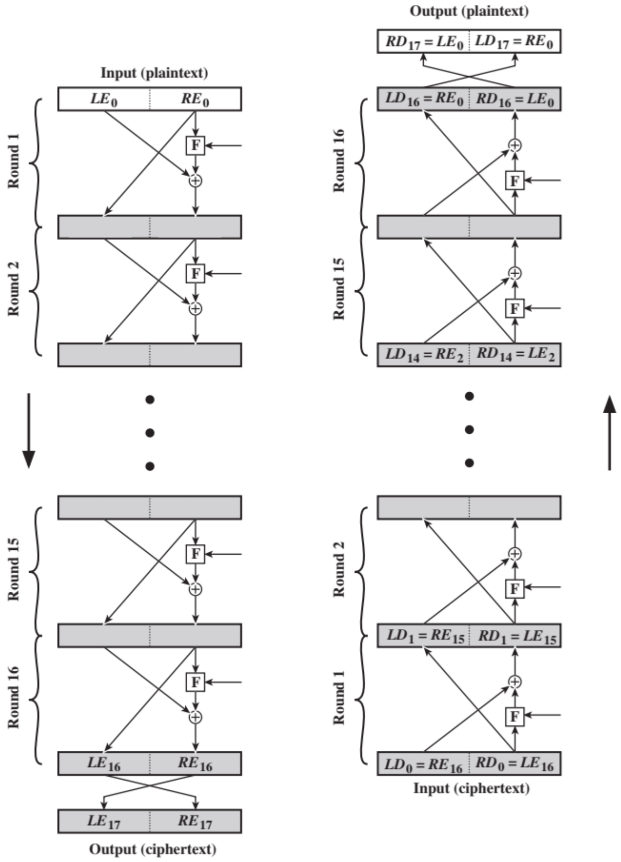


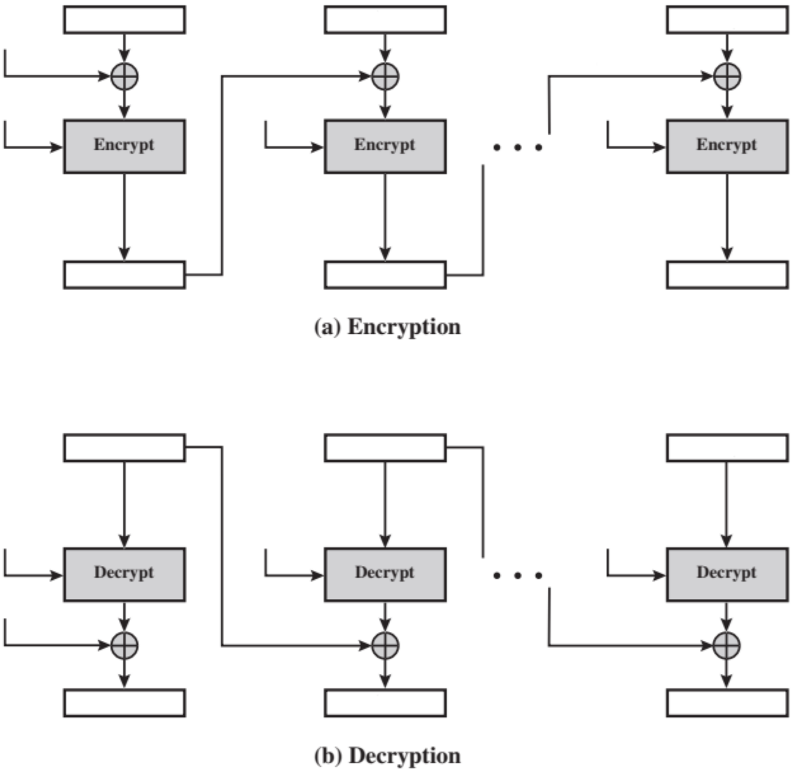
*Figure 2: Feistel Encryption and Decryption (16 rounds)*

**4. (a)** List and briefly define categories of security mechanisms. (10 marks)

**(b)** In relation to Pseudorandom Number Generation, discuss the Blum Blum Shub (BBS) Generator. Use a diagram to illustrate your answer (11 marks)

**(c)** Cipher block chaining(CBC) is the general-purpose stream-oriented transmission and it overcome the security deficiencies of Electronic Codebook (ECB). Label the Figure 3 of Cipher block chaining(CBC). (12 marks)

See the next page.



(a) Encryption

(b) Decryption

*Figure 3: Cipher Block Chaining (CBC) Mode*