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)

WINTER EXAMINATIONS 2017/2018

ADVANCED SECURITY 1 [CMPU4007]

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

WEDNESDAY 10TH JANUARY 2.00 P.M. – 4.00 P.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 passive and active security attacks. (12 marks)

(b) Encrypt the plaintext "we are discovered save yourself" using Vigenère Cipher and key is the repeating keyword "**deceptive**" as long as the message length. (11 marks)

(c) List and briefly define categories of security services. (10 marks)

2. **(a)** Briefly define the Playfair cipher. (11 marks)

(b) What is the difference between a block cipher and a stream cipher? Use a diagram to illustrate your answer. (10 marks)

(c) Explain a Feistel Cipher design in detail. (12 marks)

3. **(a)** Explain the Euclidean Algorithm with the help of an example? (11 marks)

(b) In relation to number theory explain Euler's Theorem with help of example?

(10 marks)

(c) Briefly discuss the AES Encryption and Decryption with the help of diagram.

(12 marks)

4. **(a)** Describe the following Block Cipher Modes of Operation (12 marks)

I. Electronic Codebook (ECB)

II. Cipher Block Chaining (CBC)

III. Cipher Feedback (CFB)

(b) Explain the RSA algorithm with the help of an example. (12 marks)

(c) What are three broad categories of applications of public-key cryptosystems?

(9 marks)