W211C/408C, W228/408C

DUBLIN INSTITUTE OF TECHNOLOGY

DT211C BSc. (Honours) Degree in Computer Science (Infrastructure)

Year 4

DT228 BSc. (Honours) Degree in Computer Science

Year 4

WINTER EXAMINATIONS 2016/2017

ADVANCED SECURITY 1 [CMPU4007]

MR HUGH PEARSE
DR. DEIRDRE LILLIS
MR. THOMAS NOLAN – DT211
MR. KEVIN FOLEY – DT228

WEDNESDAY 11TH JANUARY 4.00 P.M. – 6.00 P.M.

TWO HOURS

ANSWER **THREE** QUESTIONS OUT OF **FOUR**.

ALL QUESTIONS CARRY EQUAL MARKS. ONE (1) COMPLIMENTARY MARK WILL BE GIVEN.

1. (a) The following cipher text was obtained encrypted using ceasar cipher and the key 13.

Gur Hygvzngr Qevivat Znpuvar

Decrypt the ciphertext.

(11 marks)

(b) A round function can be found in most iterated block ciphers, explain its use and purpose.

(11 marks)

(c) Explain linear and differential cryptanalysis.

(11 marks)

2. (a) Explain the completeness effect.

(11 marks)

(b) Explain pre-image resistance in relation to hash functions.

(11 marks)

(c) A MAC is said to achieve integrity and authenticity. Explain why a hash function is not used with a secret key to achieve authenticity.

(11 marks)

3. (a) Alice wants to send a large video file to Bob securely. Alice will use encryption and file compression to send the file, which order should she apply the operations and why?

(11 marks)

(b) Explain the purpose of re-seeding a pseudo-random number generator.

(11 marks)

(c) Explain the difference between the one-time pad cipher and most modern stream ciphers.

(11 marks)

4. (a) Explain what is the diffie-hellman protocol, why it is used and how it works.

(11 marks)

(b) Explain how RSA encryption works.

(11 marks)

(c) Discuss the reasons that the concept of "security through obscurity" is generally considered a bad principle to rely on. Provide at most two real-world examples of where you have seen this principle being used.

(11 marks)