DUBLIN CITY UNIVERSITY

SEMESTER 1 EXAMINATIONS 2015/2016

MODULE: CA4005 - Cryptography and Security Protocols

PROGRAMME(S):

CASE - BSc in Computer Applications (Sft.Eng.)
ECSA - Study Abroad (Engineering and Computing)

YEAR OF STUDY: 4,X

EXAMINERS: Dr Geoff Hamilton (Ph:5017)
Dr. Ian Pitt

TIME ALLOWED: 3 hours

INSTRUCTIONS: Answer 5 questions. All questions carry equal marks.

PLEASE DO NOT TURN OVER THIS PAGE UNTIL INSTRUCTED TO DO SO

The use of programmable or text storing calculators is expressly forbidden.
Please note that where a candidate answers more than the required number of questions, the examiner will mark all questions attempted and then select the highest scoring ones.

Requirements for this paper (Please mark (X) as appropriate)

□ *Log Tables*	□ *Thermodynamic Tables*
□ *Graph Paper*	□ *Actuarial Tables*
□ *Dictionaries*	□ *MCQ Only - Do not publish*
□ *Statistical Tables*	□ *Attached Answer Sheet*

QUESTION 1 ***[Total marks: 20]***

1(a) [5 Marks]

Explain why padding schemes are necessary for block ciphers. Give two examples of appropriate padding schemes.

1(b) [8 Marks]

Compare and contrast the *Electronic Cook Book* (ECB) and *Ciphertext Block Chaining* (CBC) modes of operation for block ciphers with respect to the following (use diagrams if necessary):

- Encryption
- Decryption
- Error propagation
- Detection of alteration of ciphertext blocks

1(c) [7 Marks]

A block cipher has a block size of 64 bits. For both ECB mode and CBC mode, answer the following:

- After encrypting how many blocks would you expect to observe that two of the ciphertext blocks are identical?
- What information would the observation of identical ciphertext blocks reveal to an attacker?

[End Question 1]

QUESTION 2 ***[Total marks: 20]***

2(a) [5 Marks]

Describe the structure of an X.509 *PKI certificate*, explaining the purpose of each field.

2(b) [10 Marks]

Explain the concept of a *certificate path*. Describe an algorithm which can be used to validate a certificate path and extract a user's public key. Given a root CA (A), an intermediate CA (B) and a user (C), give an example of a certificate path used to certify C's public key, and the steps which would be followed to validate this path and extract the key.

2(c) [5 Marks]

Explain the concept of a *certificate revocation list*, and why these are necessary. For the example in part (b), what CRLs are needed to validate C's certificate?

[End Question 2]

QUESTION 3 ***[Total marks: 20]***

3(a) [7 Marks]

Describe in detail how the RSA cryptosystem works. Your description should include how public and private key pairs are generated, how encryption and decryption are performed, and the hard problem that the security of RSA rests upon.

3(b) [6 Marks]

Describe an efficient algorithm which can be used to implement encryption and decryption in RSA. Show how encryption can be implemented more efficiently by using an appropriate value for the encryption exponent. Show how decryption can be implemented more efficiently using the prime factors of the modulus.

3(c) [7 Marks]

Suppose we have three RSA users with the same encryption exponent $e = 3$ but different public moduli N_1, N_2 and N_3. If the same message is encrypted using the public key of each of these users and sent to them, show how an attacker can use the values of these ciphertexts to recover the original message. If the values of these public moduli are $N_1 = 33$, $N_2 = 35$ and $N_3 = 39$ and the attacker sees the corresponding ciphertexts $c_1 = 31$, $c_2 = 29$ and $c_3 = 25$, determine the value of the original message. What lessons can be learned from this in improving the security of RSA?

[End Question 3]

QUESTION 4 ***[Total marks: 20]***

4(a) [8 Marks]

Describe in detail how *Diffie-Hellman* (DH) key exchange works. Give an example with suitable small values.

4(b) [7 Marks]

Show how DH key exchange is subject to a man-in-the-middle attack.

4(c) [5 Marks]

Describe in detail two ways in which the man-in-the middle attack on DH can be avoided.

[End Question 4]

QUESTION 5 ***[Total marks: 20]***

5(a) [5 Marks]

Explain the difference between *entity authentication* and *message origin authentication*. Which form of authentication can be provided in a secure e-mail system? Explain your answer.

5(b) [7 Marks]

Explain how a combination of symmetric and asymmetric ciphers can be used to implement secure e-mail. Your answer should explain the use of *message keys* and *tokens*.

5(c) [8 Marks]

Describe PGP and how this can be used to implement a secure e-mail system.

[End Question 5]

[END OF EXAM]