DUBLIN CITY UNIVERSITY

SEMESTER 1 EXAMINATIONS 2016/2017

MODULE: CA4005 - Cryptography and Security Protocols

PROGRAMME(S):

CASE - BSc in Computer Applications (Sft.Eng.)
CPSSD - BSc in ComputationalProblem SolvandSW Dev.
ECSAO - Study Abroad (Engineering and Computing)
ECSA - Study Abroad (Engineering and Computing)

YEAR OF STUDY: 4,O,X

EXAMINERS: Geoffrey Hamilton (Ph:5017)
Prof. David Bustard
Dr. Ian Pitt

TIME ALLOWED: 3 hours

INSTRUCTIONS: Answer all 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☐	*Dictionaries*	☐	*MCQ Only - Do not publish*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) [6 Marks]

What are the minimum recommended block size and key size which should be used for a block cipher? What attacks could be mounted against the block cipher if either of these sizes is less than recommended? What are the implications of this for DES?

1(b) [8 Marks]

Describe the *Feistel structure* which is used in many block ciphers in conjunction with a round function. Show how the effect of the Feistel structure can be reversed using the same round function. Using these answers, describe how encryption and decryption are performed in DES.

1(c) [6 Marks]

If a decision were taken to increase the security of DES by encrypting using the entire cipher twice, describe an attack which could be mounted against this modified cipher. How much more security would be provided by encrypting three times rather than two?

[End Question 1]

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

2(a) [6 Marks]

A cryptographically secure hash function should be *pre-image resistant* and *collision-free*. Define these properties and why they are important for hash functions.

2(b) [7 Marks]

Explain the *birthday paradox* by determining for k people the probability that one pair has a birthday in common. For a n-bit digest, how many messages would we need to hash on average before we find a collision? What would therefore be an appropriate digest size?

2(c) [7 Marks]

Describe how hash functions can be used to store passwords in conjunction with a *salt*, and how this makes them less susceptible to attack.

[End Question 2]

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

Consider a toy RSA example in which the public key is $(N = 33, e = 17)$.

3(a) [6 Marks]

Determine the value of the private key.

3(b) [7 Marks]

Describe how encryption is done in RSA. Give an efficient algorithm which can be used to implement this encryption, and use this algorithm to encrypt the message 27.

3(c) [7 Marks]

Describe how decryption is done in RSA. Describe a technique which can be used to implement this decryption more efficiently using the prime factors of the modulus, and use this technique to decrypt the ciphertext generated above.

[End Question 3]

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

4(a) [8 Marks]

Describe the Needham-Schroeder Public-Key (NSPK) protocol and Lowe's attack on the protocol.

4(b) [6 Marks]

Describe the Diffie-Hellman (DH) key agreement protocol and explain why it is subject to a man-in-the-middle attack.

4(c) [6 Marks]

Explain how the DH protocol can be "embedded" into the NSPK protocol and give the protocol steps of the resulting modified protocol that achieves entity-authentication and key-exchange. Is the resulting protocol subject to Lowe's attack or a man-in-the-middle attack? Justify your answers.

[End Question 4]

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

5(a) [7 Marks]

Describe SSL with particular reference to the protocols involved, how authenticity, confidentiality and integrity are achieved and the level of security provided.

5(b) [7 Marks]

Describe IPSec with particular reference to the protocols involved, how authenticity, confidentiality and integrity are achieved and the level of security provided.

5(c) [6 Marks]

Compare and contrast SSL and IPSEC with respect to the above.

[End Question 5]

[END OF EXAM]