DUBLIN CITY UNIVERSITY

AUGUST/RESIT 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☐	*Dictionaries*	☐	*MCQ Only - Do not publish*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]

Block ciphers are usually designed to provide *confusion* and *diffusion*. Explain what is meant by each of these properties, and give examples of the features of block ciphers which are used to provide them.

1(b) [10 Marks]

Describe the *Advanced Encryption Standard* (AES) with reference to the following (use diagrams if necessary):

- Encryption algorithm
- Decryption algorithm
- Block size
- Key size
- Number of rounds
- Robustness against attacks

Describe how AES provides confusion and diffusion.

1(c) [5 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 AES?

[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]

Describe how hash functions can be used to implement digital signatures. Explain why it is important in this context that a hash function has a digest size of at least 160 bits. Describe a simple fraud that could be perpetrated using digital signatures if the hash function digest size were only 64 bits.

2(c) [7 Marks]

Describe how hash functions can be used for message authentication. How do *Message Authentication Codes* (MACs) differ from *Manipulation Detection Codes* (MDCs)? Describe how a MAC can be constructed from a block cipher, and how a MAC can be constructed from a MDC.

[End Question 2]

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

Consider a toy ElGamal example with prime modulus $p = 23$, generator $g = 4$ and private key $a = 10$.

3(a) [5 Marks]

Determine the public key value h.

3(b) [7 Marks]

Describe how encryption is done in ElGamal and encrypt the message $m = 19$ with the ephemeral key $k = 2$.

3(c) [8 Marks]

Describe how decryption is done in ElGamal and use this to decrypt the ciphertext $(18||19)$.

[End Question 3]

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

Consider the following protocol that allows entities A and B to mutually authenticate each other and to establish a shared session key.

1. $A \rightarrow B : A, N_A$
2. $B \rightarrow S : B, N_B, \{A, N_A\}_{K_{B,S}}$
3. $S \rightarrow A : N_B, \{B, N_A, K_{A,B}\}_{K_{A,S}}, \{A, B, N_B, K_{A,B}\}_{K_{B,S}}$
4. $A \rightarrow B : \{A, B, N_B, K_{A,B}\}_{K_{B,S}}, \{N_B\}_{K_{A,B}}$

4(a) [6 Marks]

Explain the role played by S and the use of the keys $K_{A,S}$, $K_{B,S}$ and $K_{A,B}$ in this protocol.

4(b) [8 Marks]

Explain how the nonces N_A and N_B ensure the freshness of the session key, and their role in the mutual authentication of A and B.

4(c) [6 Marks]

Consider the protocol obtained by replacing step 4 with the following step:

$4'.\ A \rightarrow B : \{A, B, N_B, K_{A,B}\}_{K_{B,S}}$

Does this new protocol still achieve mutual authentication? Explain your answer.

[End Question 4]

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

5(a) [7 Marks]

Describe the WEP protocol, including in particular how messages are encrypted and decrypted, and whether the values involved are public or private.

5(b) [7 Marks]

Describe how message integrity is implemented in WEP. Explain using an example how an attacker can modify messages without detection. How could message integrity have been implemented to prevent this attack?

5(c) [6 Marks]

WEP uses a 24-bit IV. If this IV were generated randomly for each packet, after how many packets would you expect the same IV to be generated? What information could this re-occurrence reveal to an attacker?

[End Question 5]

[END OF EXAM]