DUBLIN CITY UNIVERSITY

SEMESTER 1 EXAMINATIONS 2017/2018

MODULE: CA4005 - Cryptography and Security Protocols

PROGRAMME(S):

CASE	BSc in Computer Applications (Sft.Eng.)
CPSSD	BSc in ComputationalProblem Solv&SW Dev.
ECSAO	Study Abroad (Engineering and Computing)

YEAR OF STUDY: 4,O

EXAMINER(S):

Geoffrey Hamilton	(Ext:5017)
Dr. Hitesh Tewari	External
Prof. Brendan Tangney	External

TIME ALLOWED: 3 Hours

INSTRUCTIONS: Answer all questions.

PLEASE DO NOT TURN OVER THIS PAGE UNTIL INSTRUCTED TO DO SO.
The use of programmable or text storing calculators is expressly forbidden.

There are no additional requirements for this paper.

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

1(a) [4 Marks]

Compare and contrast *stream ciphers* and *block ciphers*.

1(b) [12 Marks]

Compare and contrast the block ciphers *Data Encryption Standard* (DES) and *Advanced Encryption Standard* (AES) with respect to the following (use diagrams if necessary):

- Encryption/decryption
- Block size
- Key size
- Number of rounds
- Robustness against attacks

1(c) [4 Marks]

Show how a block cipher can be used to implement a stream cipher.

[End Question 1]

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

2(a) [8 Marks]

Describe the *Merkle Damgård construction* which is often used in the implementation of hash functions (use diagrams if necessary). What properties are required for a hash function to be considered to be cryptographically secure and why?

2(b) [8 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.

2(c) [4 Marks]

If a MAC with secret key k were created from a MDC as $\text{MAC}_k(m) = \text{MDC}(k||m)$, show how you could make use of the Merkle Damgård construction to compute $\text{MAC}_k(m||m')$ without knowing k.

[End Question 2]

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

Consider a toy RSA example in which the public key is $(N = 55, e = 17)$.

3(a) [6 Marks]

Determine the value of the private key.

3(b) [7 Marks]

Describe how a digital signature can be implemented using RSA. Describe a technique which can be used to perform the mathematical operation used in this digital signature more efficiently using the prime factors of the modulus, and use this technique to generate the digital signature for the message digest value 35.

3(c) [7 Marks]

Describe how a digital signature can be verified using RSA. Give an efficient algorithm which can be used to perform both encryption and decryption in RSA, and use this algorithm in the verification of the digital signature value calculated above.

[End Question 3]

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

4(a) [10 Marks]

Describe the *Otway-Rees* protocol. Your answer should include the objectives of the protocol, the protocol steps, and an informal analysis of the security of the protocol.

4(b) [5 Marks]

Explain the use of nonces in the Otway-Rees protocol. Does the Otway-Rees protocol require synchronized clocks? Explain your answer.

4(c) [5 Marks]

What is a *type flaw attack*? Explain why the Otway-Rees protocol may be vulnerable to a type flaw attack.

[End Question 4]

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

5(a) [7 Marks]

Define what is meant by a *blind signature* and describe how this can be implemented using RSA. Explain how a blind signature scheme can be used to implement digital cash (this should include a description of the steps involved in a digital cash transaction).

5(b) [7 Marks]

Define the structure of the *blockchain* used in Bitcoin, and explain how this is used to implement digital cash (this should include a description of the steps involved in a digital cash transaction).

5(c) [6 Marks]

What are the main security objectives required of a digital cash scheme? Explain how these objectives are met by the digital cash schemes described in your answers for parts (a) and (b) of this question.

[End Question 5]

[END OF EXAM]