DUBLIN CITY UNIVERSITY

AUGUST/REPEAT 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) [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 *Counter* (CTR) modes of operation for block ciphers with respect to the following (use diagrams if necessary):

- Encryption/decryption
- Error propagation
- Hiding of patterns and repetitions in plaintext
- Amenability to processing blocks in parallel
- Detection of insertion of ciphertext blocks by attacker

1(c) [7 Marks]

A block cipher has a block size of 64 bits. For both ECB mode and CTR 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) [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) [8 Marks]

Describe how hash functions can be used help in performing 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) [6 Marks]

Describe how hash functions can be used to generate a symmetric key from a passphrase in conjunction with a *salt*. How does the salt help to thwart an attacker trying to perform a *dictionary attack* to find the key? How can the key generation be done in such a way to further thwart an attacker trying to perform a dictionary attack?

[End Question 2]

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

3(a) [6 Marks]

Define the *RSA problem* which must be solved in order to break RSA. Show that this problem is no harder than the integer factorisation problem.

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) [8 Marks]

Suppose we have two RSA users with the same public modulus N but different encryption exponents e_1 and e_2. If the same message is encrypted using the public key of each of these users and sent to them as the corresponding ciphertexts c_1 and c_2, show how an attacker can use the values of these ciphertexts to recover the original message. If the value of the public modulus $N = 18923$, the encryption exponents are $e_1 = 11$ and $e_2 = 5$, and the attacker sees the corresponding ciphertexts $c_1 = 1514$ and $c_2 = 8189$, determine the value of the original message.

[End Question 3]

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

4(a) [8 Marks]

Describe the *Needham-Shroeder Secret-Key (NSSK)* 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) [6 Marks]

Give an outline of the steps of the *Kerberos* protocol.

4(c) [6 Marks]

Compare and contrast the NSSK and Kerberos protocols with respect to the following:

- The objectives of the protocol.
- The different mechanisms by which these objectives are achieved.
- The need for synchronised clocks.
- The lifetime of sessions keys: is it possible to re-use session keys on different connections between the participants?

[End Question 4]

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

5(a) [7 Marks]

Distinguish between a *SSL session* and a *SSL connection*. Which phases in IPSEC do these roughly correspond to?

5(b) [7 Marks]

Describe the steps involved in establishing a SSL session. Compare and contrast this with the steps involved in achieving a similar goal in IPSEC.

5(c) [6 Marks]

Describe the steps involved in establishing a SSL connection. Compare and contrast this with the steps involved in achieving a similar goal in IPSEC.

[End Question 5]

[END OF EXAM]