Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

SEMESTER 1 EXAMINATIONS 2020/2021

MODULE: CA4005 - Cryptography and Security Protocols

PROGRAMME(S):

CASE BSc in Computer Applications (Sft.Eng.)

YEAR OF STUDY: 4

EXAMINERS:

Geoffrey Hamilton	(Internal)
Dr. Hitesh Tewari	(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.
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☐	*Dictionaries*	☐	*MCQ Only - Do not publish*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]***

Consider a toy block cipher with a 4-bit block and an encryption algorithm that acts as follows:

Input	0000	0001	0010	0011	0100	0101	0110	0111
Output	1101	0111	1001	0000	1011	1111	0001	0010
Input	1000	1001	1010	1011	1100	1101	1110	1111
Output	1110	0011	1100	0101	0100	0110	1000	1010

1(a) [4 Marks]

Give the encryption of the plaintext 0110111000011010 using this block cipher when operating in ECB mode and justify your answer.

1(b) [8 Marks]

Give the encryption of the plaintext 0110111000011010 using this block cipher when operating in CBC mode with an IV of 1011 and justify your answer.

1(c) [8 Marks]

Give the encryption of the plaintext 0110111000011010 using this block cipher when operating in OFB mode with an IV of 1011 and justify your answer.

[End Question 1]

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

Consider a toy hash function implemented using the Merkle-Damgård construction with a 2-bit block, an IV of 10, and a compression function that acts as follows:

Message Block	00	00	00	00	01	01	01	01
Previous Value	00	01	10	11	00	01	10	11
Output	10	11	01	00	11	00	01	10
Message Block	10	10	10	10	11	11	11	11
Previous Value	00	01	10	11	00	01	10	11
Output	11	01	00	10	01	10	11	00

2(a) [4 Marks]

For this hash function, how many messages would you have to try on average before you found a collision?

2(b) [8 Marks]

Give the digest produced by the above hash function for the message 01100011 (you can assume that there is no extra block appended to the end of the message giving its length).

2(c) [8 Marks]

If a MAC with secret key k is implemented using the above hash function as MAC$_k(m)$ = $\mathcal{H}(k||m)$, and the value of this MAC is 01, what is the value of the MAC if the block 11 is appended to the end of the message m?

[End Question 2]

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

3(a) [6 Marks]

Determine whether 2 is a quadratic residue modulo 187.

3(b) [6 Marks]

Calculate the square roots of 2 modulo 71.

3(c) [8 Marks]

Find a primitive root of $\mathbb{Z}_{43}^*$

[End Question 3]

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

Consider a toy RSA example in which the public key is $(n = 35, e = 17)$.

4(a) [6 Marks]

Determine the value of the private key. Justify your answer using the extended Euclidean GCD algorithm.

4(b) [6 Marks]

Determine the result of encrypting the plaintext message 27. Justify your answer using one of the square-and-multiply variant algorithms.

4(c) [8 Marks]

Determine the result of decrypting the ciphertext 19. Justify your answer calculating the result modulo 5, and also modulo 7, and then combining these results using the Chinese Remainder Theorem.

[End Question 4]

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

Consider the following protocol that allows entities A and B to mutually authenticate each other using a shared secret key $K_{\langle A,B\rangle}$, where N_A and N_B are nonces and $\mathcal{H}$ is a known agreed hashing method.

1. $A \rightarrow B : A, N_A$
2. $B \rightarrow A : B, N_B, \mathcal{H}(\mathcal{N}_\mathcal{A}, \mathcal{K}_{\langle \mathcal{A},\mathcal{B}\rangle})$
3. $A \rightarrow B : \mathcal{H}(\mathcal{N}_\mathcal{B}, \mathcal{K}_{\langle \mathcal{A},\mathcal{B}\rangle})$

5(a) [4 Marks]

Explain how this protocol achieves mutual authentication of A and B.

5(b) [8 Marks]

Describe a reflection attack on this protocol.

5(c) [8 Marks]

Describe two techniques, that do not require the use of additional keys, for preventing the reflection attack described in your previous answer.

[End Question 5]

[END OF EXAM]