Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

SEMESTER 1 EXAMINATIONS 2022/2023

MODULE: CA4005 - Cryptography and Security Protocols

PROGRAMME(S):

CASE	B.Sc. in Computer Applications (Sft.Eng.)
ECSAO	Study Abroad (Engineering & Computing)
ECSA	Study Abroad (Engineering & Computing)

YEAR OF STUDY: 4,O,X

EXAMINER(S):

Geoffrey Hamilton	(Internal)	(Ext:5017)
Prof. Arend Rensink	(External)	External

TIME ALLOWED: 3 Hours

INSTRUCTIONS: Answer all 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.

There are no additional requirements for this paper.

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

1(a) [6 Marks]

Describe the general operation of *stream ciphers*, describing in particular how they perform encryption and decryption (using a diagram if necessary). What properties must the *keystream* have for the stream cipher to be considered secure?

1(b) [7 Marks]

Describe the *Cipher Block Chaining* (CBC) mode of operation for block ciphers. What is the role of the *Initialisation Vector* (IV)? What are the dangers if an IV is:

- altered by an attacker
- known to an attacker
- reused with the same key

1(c) [7 Marks]

Compare and contrast the *Output Feed Back* (OFB) and *Cipher Feed Back* (CFB) modes of operation for block ciphers with respect to the following:

- Encryption
- Decryption
- Error propagation

[End of 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 of Question 2]

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

3(a) [7 Marks]

Calculate $6/119 \pmod{191}$.

3(b) [6 Marks]

Calculate $\phi(24)$, where ϕ is the Euler Totient function. Use this to calculate $27^{615} \pmod{24}$.

3(c) [7 Marks]

Find a primitive root of $\mathbb{Z}_{17}^*$

[End of Question 3]

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

4(a) [6 Marks]

Compare and contrast the RSA cryptosystem with the Rabin cryptosystem.

4(b) [5 Marks]

Consider a toy Rabin cryptosystem in which the public key $N = 77$. Describe how encryption is done in the Rabin cryptosystem and use this to encrypt the message 29.

4(c) [9 Marks]

Describe how decryption is done in the Rabin cryptosystem using the prime factors of the modulus, and how this can be made faster by choosing these prime factors to satisfy specific properties. Use this decryption technique to find all possible decryptions for the ciphertext value 37 when the public key $N = 77$ as above. In practice, how would we determine which of the possible decryptions of a ciphertext is the correct one?

[End of 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 $K_{\langle A,B\rangle}$.

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

5(a) [4 Marks]

Explain the use of nonces in this protocol.

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 of Question 5]

[END OF EXAM]