Course: Master of Science in Cybersecurity, Privacy and Trust
Module: COMP C5205 Modern Cryptography
Exam: Summer 2023
Lecturer: Dr. Martin Harrigan

Instructions:

- Answer any four questions.
- You have 2.5 hours to complete the exam.
- The exam is worth 50% of your final grade.

Question 1 **(20 marks)**

(a) The one-time pad takes a plaintext, P, and a key, K, as input. What are the two requirements for the key, K? Are there any requirements for P?

(6 marks)

(b) Suppose $P = \texttt{11110000}$ and $K = \texttt{11000011}$. Use the one-time pad encryption process to produce the corresponding ciphertext. Use the decryption process to recover the plaintext.

(6 marks)

(c) Draw a diagram that illustrates the Counter Mode (CTR) of operation for block ciphers when decrypting ciphertext. Your diagram should show the flow of data from the ciphertext blocks to the decryption processes to the plaintext blocks.

(8 marks)

Question 2 **(20 marks)**

(a) During the Diffie-Hellman (DH) protocol, Alice and Bob interact over an insecure channel. The interaction involves several numbers:

1. Alice and Bob agree on a base number g and a prime number p.
2. Alice chooses a number a and sends the number A to Bob where $A = g^a \mod p$.
3. Bob chooses a number b and sends the number B to Alice where $B = g^b \mod p$.

Eve observes all communication over the channel. For each number (g, p, a, b, A and B), indicate whether each of the participants (Alice, Bob and Eve) has knowledge of the number at the end of the interaction by completing the table below. For example, the first line indicates that Alice, Bob and Eve all have knowledge of g at the end of the interaction.

	Alice	Bob	Eve
g	✓	✓	✓
p			
a			
b			
A			
B			

(6 marks)

(b) The Diffie-Hellman (DH) protocol is a key-agreement protocol that provides *forward secrecy*. Explain what is meant by the term forward secrecy and why it is a favourable property of a cryptographic protocol.

(5 marks)

(c) Alice uses OpenPGP to generate a keypair and a revocation certification. She meets her friend Bob in person, and gives him her public-key. One day, Alice cannot find her private-key. Therefore, she sends her revocation certificate to Bob. However, later that day, Alice finds her private-key. She sends a message, signed using her private-key, asking Bob to ignore the revocation. Can Bob trust this message? Explain your answer.

(4 marks)

(d) Suppose you receive a message signed by a private-key, for which you possess the corresponding public-key. You try to verify the signature, but OpenPGP says that the key has expired. You change the system time on your computer, and retry the process. This time, OpenPGP says that the signature is valid. Can you trust the signature? What is the purpose of the key expiration date if you can change the system time on your computer?

(5 marks)

Question 3 **(20 marks)**

(a) With block ciphers, certain modes of operation require the length of the plaintext to be a multiple of the block size. Name two modes (not just the acronym) that have this requirement.

(4 marks)

(b) PKCS#7 (a.k.a. RFC 5652) is a popular padding scheme that pads arbitrary-length plaintexts so that their length is a multiple of a block size. The scheme adds padding even when the length of the plaintext is initially a multiple of the block size. Why is padding added in this case?

(4 marks)

(c) Ciphertext stealing is an alternative to padding that alters the processing of the last two blocks. Draw a diagram that illustrates how ciphertext stealing processes the last two blocks when encrypting plaintext. Your diagram should show the flow of data from the last two plaintext blocks to the encryption processes, and to the ciphertext blocks, and it should identify the portion of the ciphertext that is 'stolen'.

(6 marks)

(d) List three advantages of ciphertext stealing over padding.

(6 marks)

Question 4 **(20 marks)**

(a) What is a trapdoor function? Provide an example of one.

(4 marks)

(b) The following table shows the NIST Recommended Key Sizes for two popular schemes in asymmetric cryptography: the RSA algorithm and Elliptic Curve Cryptography (ECC)-based algorithms.

Security (bits)	RSA Key Size	ECC Key Size
112	2048	224
128	3072	256
192	7680	384
256	15 360	512

Explain the significance of the smaller values in the ECC column when compared with the RSA column. According to the NIST table, is it more secure to use a 7680-bit RSA key or a 256-bit ECC key?

(4 marks)

(c) The Elliptic Curve Integrated Encryption Scheme (ECIES) is a *hybrid cryptosystem* for encrypting and decrypting data. Explain what is meant by a hybrid cryptosystem? What is the main advantage in using such a system over a system based solely on asymmetric cryptography?

(8 marks)

(d) In ECC, you need to choose a curve. Curves vary by security and performance. Name two popular elliptic curves used in ECC.

(4 marks)

Question 5 **(20 marks)**

(a) A cryptographic hash function must be collision resistant and preimage resistant. What is meant by both of these terms?

(7 marks)

(b) Name two popular hash functions that are considered secure as of today.

(3 marks)

(c) What are the inputs and the outputs of a keyed hash function?

(3 marks)

(d) Keyed hash functions form the basis of message authentication codes (MACs). Briefly describe one application of MACs.

(4 marks)

(e) Name two popular keyed hash functions that are considered secure as of today.

(3 marks)