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)

1. **Requirements for the Key (K)**:
   - **Key Length**: The key (K) must be at least as long as the plaintext (P). This ensures that each bit or character of the plaintext has a corresponding bit or character in the key.
   - **Key Randomness**: The key (K) must be completely random. Each bit or character in the key should be generated independently and uniformly at random .
2. **Requirements for the Plaintext (P)**:
   - There are no specific requirements for the plaintext (P) other than it being the message you wish to encrypt. However, the length of the plaintext will determine the length of the key needed.

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

(6 marks)

XOR, or "exclusive OR," is a way to compare two bits (0s and 1s). When you compare two bits using XOR, the result is 1 if the bits are different, and 0 if they are the same.

Here's a simple way to think about it:

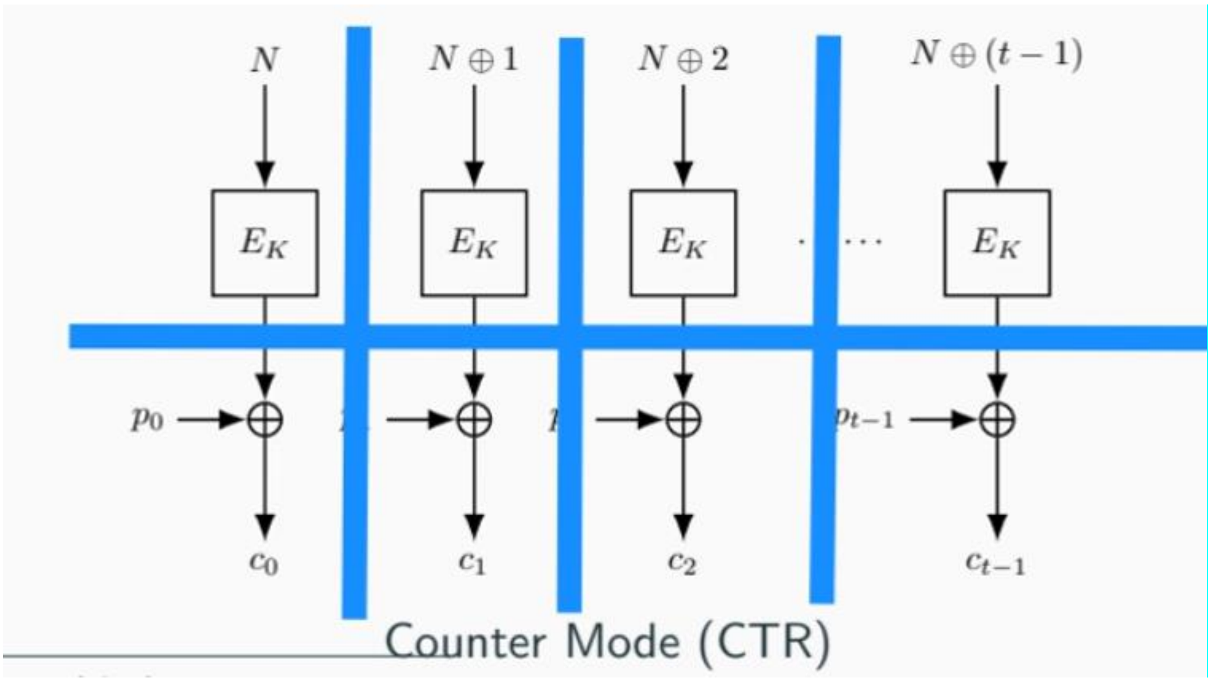
- If you have two bits, 0 and 0, XOR gives you 0 (because they are the same).
- If you have two bits, 1 and 1, XOR gives you 0 (because they are the same).
- If you have two bits, 0 and 1, XOR gives you 1 (because they are different).
- If you have two bits, 1 and 0, XOR gives you 1 (because they are different).

So, XOR is like a rule that says "give me 1 if the bits are different, and 0 if they are the same."

1. **Encryption**: You start with your message (P = 11110000) and your key (K = 11000011). You mix them together using XOR, which is like flipping bits based on the key. The result is the scrambled message (00110011).
2. **Decryption**: To get your original message back, you take the scrambled message (00110011) and mix it again with the same key (11000011) using XOR. This unmixing process gives you back your original message (11110000).

(c) Draw a diagram that illustrates the Counter Mode (CTR) of operation for blockciphers 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)

Forward secrecy is a property of cryptographic protocols that ensures that even if long-term keys are compromised, past communication sessions remain secure. In other words, each session's encryption keys are independent of each other, so compromising one key does not compromise previous or future keys.

(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)

It can’t be trusted as the revocation certificate is a formal declaration that the keypair is no longer valid. Once Bob receives the revocation certificate, he should treat the keypair as compromised and invalid.

(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)

you cannot trust the signature. The key expiration date is set to ensure that keys are not used indefinitely and to limit the risk of key compromise. Changing the system time to bypass the expiration check undermines the security protocol and can lead to potential security risks.

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)

AES (Advanced Encryption Standard) and DES (Data Encryption Standard)

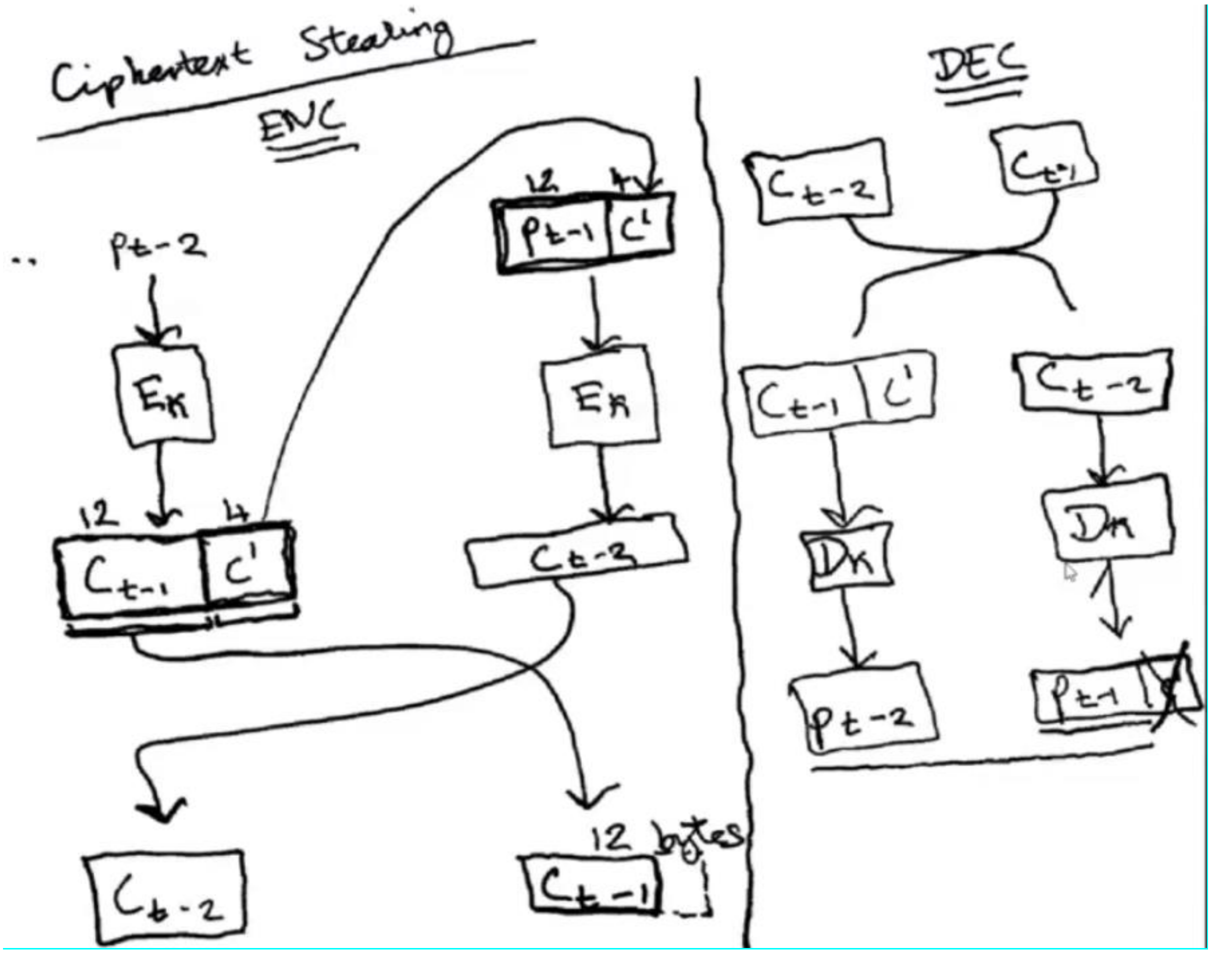
(b) PKCS#7 (a.k.a. RFC 5652) is a popular padding scheme that pads arbitrary-length plaintexts so that their length is a multiple of a block size. The scheme adds padding even when the length of the plaintext is initially a multiple of the block size. Why is padding added in this case?

(4 marks)

This is done to ensure that the padding can be unambiguously removed during decryption. If no padding were added, it would be difficult to distinguish between plaintext and padding, especially if the plaintext ends with a sequence of bytes that could be mistaken for padding.

(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)

1. No Extra Space Required: Ciphertext stealing does not require additional space for padding, which means the ciphertext remains the same length as the plaintext. This is particularly useful when storage or bandwidth is limited.
2. Preserves Data Integrity: By avoiding padding, ciphertext stealing ensures that the original data is preserved without any modifications. This helps maintain the integrity of the data and prevents any potential issues that might arise from padding.
3. Efficient Processing: Ciphertext stealing allows for efficient processing of the last two blocks of plaintext, making the encryption and decryption processes faster and more streamlined. This can be beneficial in scenarios where performance is critical.

Question 4 (20 marks)

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

A trapdoor function is easy to compute in one direction but difficult to reverse unless you have special information, known as the "trapdoor." This special information allows you to efficiently compute the inverse of the function.
An example of a trapdoor function is RSA encryption.

(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)

Smaller key sizes in ECC mean faster computations, less storage space, and lower bandwidth requirements making ECC more efficient. Despite the smaller key sizes, ECC provides the same level of security as RSA. According to the NIST table, a 7680-bit RSA key and a 256-bit ECC key both provide a security level of 192 bits. Therefore, it is equally secure to use.

(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)

A hybrid cryptosystem combines the strengths of both asymmetric (public-key) and symmetric (secret-key) cryptography. The main advantage of using a hybrid cryptosystem over a system based solely on asymmetric cryptography is efficiency. Asymmetric cryptography is computationally expensive and slow. By using asymmetric cryptography only for the key exchange and symmetric cryptography for the actual data encryption, a hybrid cryptosystem achieves both security and efficiency.

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

The equation for eliptic curves is Y2 = X3 + ax +b
Elliptic curve Diffie Hellman Key agreement (ECDH)
Elliptic curve Digital signature algorithm (ECDSA)

(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?

Collision resistance means that it is difficult to find two different inputs that produce the same hash output. Preimage resistance describes the guarantee that an attacker won't be able to find a preimage of an arbitrary hash value. There are first and second preimage resistances.

(7 marks)

(b) Name two popular hash functions that are considered secure as of today. (3 marks)

SHA256 and SHA3

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

Also known as a message authentication code (MAC) it takes the inputs of a message and secret key and outputs a fixed size unique hash value.

(3 marks)

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

when sending a financial transaction request from a client to a server, a MAC can be used to verify that the message has not been altered during transmission

(4 marks)

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

HMAC-SHA256 and HMAC-SHA3

(3 marks)