CM2025 Computer Security: Midterm Coursework

Introduction

This coursework aims to assess the first five topics on the Computer Security course. The coursework consists of two parts: a written report, some short answer questions and programming tasks. You should complete both parts.

PART A: Carry out research to list 5 recently published new malware

This part is worth **40%** of the mark for the mid-term.

In the first week of this module, you delved into various types of malware, including viruses, Trojans, and more. Moreover, some of the existing malware have been introduced. Regrettably, it remains a daily occurrence to witness the emergence of numerous new malware variants, resulting in the infection of many systems.

In this task, you should carry out research to identify 5 recently published new malware (In the past 2 years, i.e. since January, 2022). To find information on recent computer viruses, I recommend checking trusted sources such as cybersecurity news websites, antivirus software providers, or government agencies specializing in cybersecurity like the Cybersecurity and Infrastructure Security Agency (CISA) in the United States.

Your submission should be in the form of a PDF report of up to 1500 words. for each malware you should provide the following information:

* For each malware, name it and identify its type, e.g. virus, Trojan, worm etc.

* A brief description of the malware including:

    - the date of the first incident's report

    - How does it work,

* Explain:

    - How one should protect his/her system against this malware

    - If infected, how one can cope with that? Is there any solution?

* For each malware, your response must be up to 300 words.

* Cite all the necessary resources you have used to answer this question

* Given that all the malware covered in the course was created over 2 years ago, you are prohibited from using them

PART B: Cryptography

This part is worth **60%** of the mark for the mid-term.

1- Alice and Bod have decided to use a symmetric encryption algorithm. They have some assumptions about their messages:
   - Messages only contain capital letters (i.e. A to Z)
   - The length of their shared key must be greater than or equal to the length of the plaintext
   - They assign each letter a number as follows: (A,0), (B,1), (C,2), (D,3),…, (Z,25)

Their algorithm combines the key and the message using modular addition. The numerical values of corresponding message and key letters are added together, modulo 26. For example, if the plain text is "HELLO" and the key is "SECRET" then the encrypted message is calculated as following:

Since the length of the plaintext is 5, we just need the first 5 letters of the key (i.e. "SECRE"), then for each letter, we should add corresponding letters in both the plaintext and the key modulo 26.

Plaintext:	H (7)	E (4)	L (11)	L (11)	O (14)
Key:	S (18)	E (4)	C (2)	R (17)	E(4)
Cipher:	Z (25)	I (8)	N(13)	C(2)	S (18)

a) Write a program in Python, C/C++ or JavaScript to take both the plaintext and the key as its input, then print out the cipher. Assume the plaintext is your name, for the key="THISISANEXAMPLEKEYINCOMPUTERSECURITYEXAM" what is the output? Add the screenshots of your program along the input and output and submit it as a PDF file. You should also submit the source code **[10 marks]**.

b) Explain how one can decrypt the encrypted message using the encryption algorithm in part (a)? Write a program, in JavaScript, C/C++ or Python to take both the plaintext and the key as its input, then print out the plaintext. Test it using the results of the previous program. Add the screenshots of your program along the input and output and submit it as a PDF file. You should also submit the source code **[10 marks].**

c) Under what conditions (specify two) can a cipher be broken, meaning that an attacker can decipher the encrypted message without having the key? Support your reasoning with example(s) **[6 marks]**.

d) Identify THREE key factors for defining a robust key to enhance algorithm security? Explain your reasons **[6 marks]**.

2- Search the Internet and learn about the Data Encryption Standard (**DES**).
Then, based on the **RSA** and **DES** answer the following questions:

a) What is the purpose of padding in cryptography algorithms such as **DES**? Explain it using a simple example **[6 marks]**.

b) We know that the size of the key in **DES** is 64 bits, assume for padding we just add 0 at the end of the plaintext (the original message), what is the result of padding for the following text? At first replace the "YYY" with the first 3 letters of your name or family then calculate the padding (show the result in hexadecimal format):
"YYYComputerSecurity"
Show your answer step by step **[6 marks]**.

c) We know that RSA works with numbers. Assume we want to encrypt the plaintext ***M="ComputerSecurity"***. We know we should use the following formula: $C=M^e \bmod N$ in which (e,N) is the public key. But before using this formula, at first, we should convert M into a number. To do so, there are different solutions. Search the Internet and explain one of them. Show different steps of the selected solution on the given plaintext ***M="ComputerSecurity"*** as an example. Consider padding as well **[10 marks]**.

d) What is a digital signature? Is it possible to generate a digital signature using **RSA**? What about **DES**? Explain your reasoning **[6 marks]**.