اونيۏرسيتي مليسيا فهڠ السلطان عبدالله UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	**SUBJECT:** Data & Network Security	**CODE:** BCN2023	**MARK**: /20
	TOPIC: Chapter 2 and Chapter 3		
	ASSESSMENT: Lab Assignment	**NO:** 1	**TIME:** 2 weeks

PLEASE FOLLOW INSTRUCTIONS CAREFULLY

1. This lab assignment is an individual assignment.
2. The mark is 60% which brings 15% out of the total assessment mark.
3. Read the task instructions given carefully and follow the rubric given to complete your task.

THE LEARNING OUTCOME

This assignment will be evaluated based on the learning outcome of CO2.

CO2: Construct and organize attack and defence methods into computer and network environments. (Psychomotor).

THE TASK NEEDS TO FOLLOW

In this individual assignment, you need to complete all tasks given. There are six main tasks. Please do it on your own and in your own words and provide references where appropriate.

SUBMISSION REQUIREMENTS AND MARKS DISTRIBUTION

1. The front page must contain a **name, id, section, lecturer name and date of submission**.
2. Task 1 – 10 marks
3. Task 2 – 10 marks
4. List of references

* Submission based on each task in 2 weeks. The overall mark for lab assignments altogether is 60 marks. There will be 3 Lab Assignments throughout the semester.

UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	**SUBJECT:** Data & Network Security	**CODE:** BCN2023	**MARK**: /20
	TOPIC: Chapter 2 and Chapter 3		
	ASSESSMENT: Lab Assignment	**NO:** 1	**TIME:** 2 weeks

TASK 1

A. Find around five attacks on any cybersecurity attack data whether for a month, for a year or several years of data. Provide a reference for your attack data.

B. Given the attack data that you search, use **Microsoft Excel,** and process the data using the steps below:

1. Calculate the total attack for each category. Then, generate a graph and explain the graph.
2. Based on the graph in 1., identify the highest attack.
3. Give several possible reasons why the highest attack in 2., has been identified as the most occurred attack.
4. Create an awareness statement to the public on how to reduce and prevent the attack from happening in the future. Provide five actions that need to be taken by users.

You need to provide step by step snapshot for the Excel part on how you process the data with a clear explanation.

C. Go to https://ccid.rmp.gov.my/Laws/Computer_Crime_Act_1997.pdf webpage. Get the information below:

1. How many parts are in the CCA?
2. What are the offences covered in CCA?
3. Under which offence has the highest attack in question B.2. above applied to?
4. What is your argument for your answer in C.3. above?

اونيۏرسيتي مليسيا فهڠ السلطان عبدالله UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH	**SUBJECT:** Data & Network Security	**CODE:** BCN2023	**MARK**: /20
	TOPIC: Chapter 2 and Chapter 3		
	ASSESSMENT: Lab Assignment	**NO:** 1	**TIME:** 2 weeks

TASK 2

A. Given a plain text "WE LOVE INFORMATION SECURITY". Encrypt and decrypt back the plain text using the cryptography ciphers below:

1. Caesar cipher.
2. Playfair cipher using a key "BALL".
3. Vigenere cipher using a key "START".
4. Rail fence cipher with a key is 4.
5. Transposition cipher with a key is 31524.
6. Encrypt and decrypt back the plain text using RSA algorithm with p=5, q=11 and public key e=7. Do the encryption and decryption for each alphabet. Given the encryption formula is $C=M^e \bmod n$ and the decryption formula is $M=C^d \bmod n$.
7. Assume Hilmi and Jenny use a Diffie-Hellman protocol as a method to generate a shared private key with which they can then exchange information across an insecure channel. Hilmi and Jenny agree on using prime number, n = 47 and root number, g = 43. Hilmi's random number hr = 3 and Jenny's random number jr = 5. Compute the public keys ($Hilmi_{pb}$ and $Jenny_{pb}$) and the shared private keys ($Hilmi_{sc}$ and $Jenny_{sc}$) of the Diffie-Hellman arrangement protocol. Use the shared secret key to encrypt and decrypt the plain text using a monoalphabetic substitution cipher.

Provide a step-by-step work on how you get the answer.

B. **Cryptography Code**

Create your simple cipher code using any language. Write your pseudocode and algorithm for your version of encryption and decryption. Execute the code that will input a string of text from the user and generate the cipher text. After that, the cipher text will be input for the decryption algorithm and generate back the original string of text. Show the output.

Provide the free error code and show the executable output (explain the output)

Marking Guide

Item	0	In between	Full mark
Front page	Not provide		Provide all
Task 1	Not provide	Missing task and not complete	Provide all and complete
Task 2	Not provide	Missing task and not complete	Provide all and complete
List of references	Not provide		Correct and complete