A purple triangle with a white tree and a red circle

Description automatically generated

**UNIVERSITI MALAYSIA TERENGGANU**

**SEMESTER 1 2023/2024**

**CYBER SECURITY CSF3233**

**LAB 3**

**PREPARED FOR:**

**MUHAMMAD ABDUL AALIM AHMAD ROSLI**

**PREPARED BY:**

**ARUN MUGILAN A/L SARGUNAN S63746**

**REFLECTIVE QUESTIONS – TASK 1**

1. List 4 examples of hash algorithms.

* MD5
* SHA-1
* SHA-256
* SHA-3

1. What is the issue with the MD5 algorithm?

* Collision Vulnerability: MD5 is prone to producing the same hash for different inputs, compromising its security.

**REFLECTIVE QUESTIONS – TASK 2**

1. Describe the functionality of hashing encryption compared to symmetric and asymmetric encryption.

* Symmetric vs. Hashing: Hashing is one-way and tests data integrity; symmetric encrypts and decrypts with the same key to provide confidentiality.
* Asymmetric vs. Hashing: Hashing verifies integrity, but asymmetric encrypts with one key and decrypts with another for secure communication.
* Symmetric vs. Asymmetric: Symmetric uses a single shared key for speed, but secure key sharing is required. For secure communication and key exchange, asymmetric employs key pairs.

**REFLECTIVE QUESTIONS – TASK 3**

1. What is the meaning of GPG?

* GNU Privacy Guard. It's free software that keeps communication secure by encrypting and authenticating data.

1. Using your own words, explain the difference between PGP and GnuPG.

* PGP is a program for secure data exchange that uses a combination of fast and safe encryption technologies. Originally exclusive. GnuPG: An open-source version of PGP, sometimes known as GPG. Both perform comparable functions, but GnuPG is free and adheres to open-source ideals.

**REFLECTIVE QUESTIONS – TASK 5**

1. Why cryptography is important in cybersecurity?

* Cryptography keeps information safe online by making it unreadable for the wrong people. It ensures data is kept private, untampered, and confirms the identity of users.

1. Give one example of an application that applied cryptography in our daily life.

* Online banking uses encryption to keep your personal and financial information secure during transactions.

1. Describe an example of such an application in question 2 which related to the objectives of cryptography.

* In online banking, encryption keeps your login and transaction details private and unaltered. This protects sensitive data from unauthorized access and tampering.

1. Describe 5 differences between symmetric and asymmetric encryption for cryptography.

|  |  |  |
| --- | --- | --- |
| **Symmetric** | **Differences** | **Asymmetric** |
| Uses 1 shared key | **Key Type** | Uses a pair of keys |
| Faster | **Speed** | Slower |
| Needs a secure way to share | **Key Distribution** | Public keys can shared freely |
| Requires less power | **Computational Resources** | Demands more resources |
| Efficient for many data | **Use Cases** | Used for secure communication and key exchange |

1. List 5 differences between cryptography and steganography.

* Objective:

Cryptography: Encrypts information to keep it safe.

Steganography: The concealment of the fact that information exists.

* Visibility:

Encrypted data is visible but unintelligible due to cryptography.

Steganography: The presence of secret data is concealed.

* Detection:

Cryptography: This is determined by the algorithm's strength.

Steganography is difficult to detect because it conceals data within other data.

* Useful Information:

Cryptography encrypts and decrypts data using keys.

Steganography: May or may not utilise keys; focuses on data concealment.

* Communication:

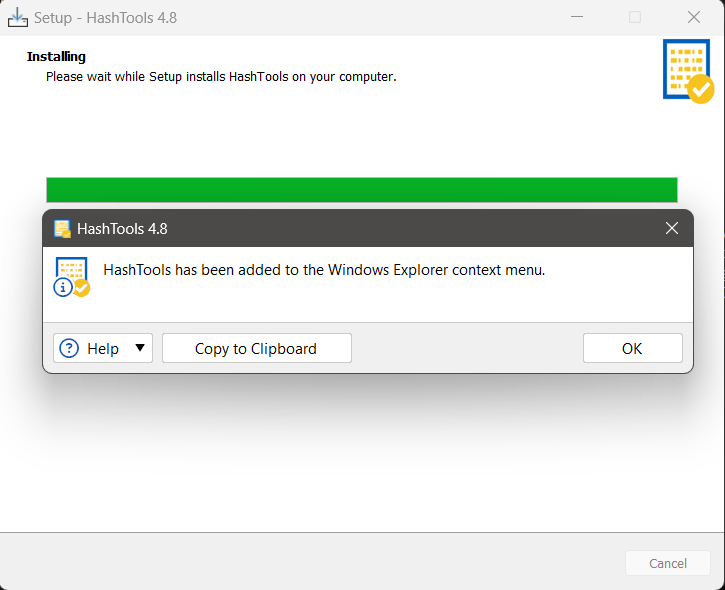
Cryptography: A method of protecting data during transmission.

Steganography: The concealment of data within other data, such as images or audio files.

TASK 1

A screenshot of a computer

Description automatically generated



A screenshot of a computer

Description automatically generated

TASK 2

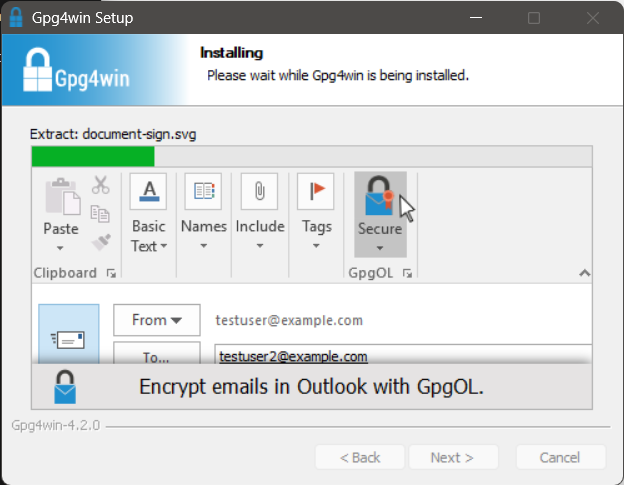
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

TASK 3



A screenshot of a computer

Description automatically generated

A screen shot of a computer screen

Description automatically generated

TASK 4

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

TASK 5

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated