Name John Ryan C. Paderna BSIT 4-B Date October 17, 2023

1. Explain the basic principles of cryptography.

*Cryptography* is the study and practice of techniques for secure communication in the presence of third parties called adversaries. An *Adversary* is a malicious entity, which aims to retrieve precious information or data thereby undermining the principles of information security.

Consider two parties Alice and Bob. Now, Alice wants to send a message m to Bob over a secure channel. So, what happens is as follows. The sender's message or sometimes called the Plaintext, is converted into an unreadable form using a Key k. The resultant text obtained is called the Ciphertext. This process is known as Encryption. At the time of received, the Ciphertext is converted back into the plaintext using the same Key k, so that it can be read by the receiver. This process is known as Decryption.

Alice (Sender) Bob (Receiver)

C = E (m, k) ----> m = D (C, k)

Here, C refers to the Ciphertext while E and D are the Encryption and Decryption algorithms respectively. Let's consider the case of Caesar Cipher or Shift Cipher as an example. As the name suggests, in Caesar's Cipher each character in a word is replaced by another character under some defined rules. Thus, if A is replaced by D, B by E and so on. Then, each character in the word would be shifted by a position of 3.

*Types of Cryptography*:

There are several types of cryptography, each with its own unique features and applications. Some of the most common types of cryptography include:

1. *Symmetric-key cryptography:* This type of cryptography involves the use of a single key to encrypt and decrypt data. Both the sender and receiver use the same key, which must be kept secret to maintain the security of the communication.

2. *Asymmetric-key cryptography*: Asymmetric-key cryptography, also known as public-key cryptography, uses a pair of keys – a public key and a private key – to encrypt and decrypt data. The public key is available to anyone, while the private key is kept secret by the owner.

*Hash functions*: A hash function is a mathematical algorithm that converts data of any size into a fixed-size output. Hash functions are often used to verify the integrity of data and ensure that it has not been tampered with.

2. List and explain the major protocols used for secure communications.
   - *SSL and TLS*
     - The Secure Sockets Layer (SSL) protocol encrypts data, authenticates data origins, and ensures message integrity.
     - SSL sessions use cryptographic algorithms similar to the algorithms used by the client and server (determined during the handshake).
     - Transport Layer Security (TLS) is an SSL-based protocol defined by the IETF (SSL is not).
   - *HTTP and HTTPS*

- HTTP is an application protocol that specifies rules for web file transfers. Users indirectly use HTTP when they open their web browser. It runs on top of the Internet protocol suite.
- HTTPS is the secure version of HTTP, securing the communication between browsers and websites. It helps prevent DNS spoofing and man-in-the-middle attacks, which is important for websites that transmit or receive sensitive information. All websites requiring user logins or handling financial transactions are attractive data theft targets and should be using HTTPS.

- *Internet Protocol (IP)*
  - IP functions similarly to a postal service. When users send and receive data from their device, the data gets spliced into packets. Packets are like letters with two IP addresses: one for the sender and one for the recipient.
  - After the packet leaves the sender, it goes to a gateway, like a post office, that directs it in the proper direction. Packets continue to travel through gateways until they reach their destinations.
- *Datagram Transport Layer Security (DTLS)*
  - DTLS is a datagram communication security protocol based on TLS. It does not guarantee message delivery or that messages arrive in order. DTLS introduces the advantages of datagram protocols, including lower latency and reduced overhead.
- *Kerberos Protocol*
  - Kerberos is a service request authentication protocol for untrusted networks like the public Internet. It authenticates requests between trusted hosts, offering built-in Windows, Mac, and Linux operating system support.
  - Kerberos uses shared secret cryptography to authenticate packets and protect them during transmission.