Republic of the Philippines

CAVITE STATE UNIVERSITY

Cavite City Campus
(046) 4313570/ (046) 4313580

Department of Information Technology
ITEC85 – Information Assurance and Security

Name: _Torres,Augustine Rie T,_____ Section: BSIT - 3F
Instructor: Ms. Mary Grace T. Nocon_____ Date: 12 - 3 - 2020

Activity No. 3

Direction: Research the following topics:

Questions:

1. The definition of Cryptography
2. Primary Functions of Cryptography
3. Different Types of Cryptography
4. The importance of cryptography in security
5. The difference between encryption and cryptography

Answer:

1. **Cryptography** is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

2. *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.

Authentication: The process of proving one's identity.
Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
Non-repudiation: A mechanism to prove that the sender really sent this message.
Key exchange: The method by which crypto keys are shared between sender and receiver.

3. *Secret Key Cryptography (SKC):* Uses a single key for both encryption and decryption; also called *symmetric encryption*. Primarily used for privacy and confidentiality.

Public Key Cryptography (PKC): Uses one key for encryption and another for decryption; also called *asymmetric encryption*. Primarily used for authentication, non-repudiation, and key exchange.
Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. Primarily used for message integrity.

4. Cryptography allows people to keep confidence in the electronic world. Secure communication is the straightforward use of cryptography. The key management problem has prevented secure communication from becoming commonplace. The development of public-key cryptography creates a large-scale network of people who can communication securely with one another even if they had never communicated before.

5. **Cryptography is** the study of concepts like **Encryption**, **decryption**, used to provide secure communication whereas **encryption is** the process of encoding a message with an algorithm.