Don Bosco Institute of Technology
Department of Information Technology

Security Lab (ITL502) Assignment No-1

Name: Lavena Babu **Roll no.: 29** **Date: 15/10/22**

I. Define the following terms with respect to Cryptography.

1) **Vulnerability**
   Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

2) **Threat**
   Threat is a possible security violation that might exploit the vulnerability of a system or asset. The origin of the threat may be accidental, environmental (natural disaster), human negligence, or human failure.

3) **Control**
   Cryptographic controls refer to a set of security practices to be used with the objective to ensure proper and effective use of cryptography to protect information, according to perceived risks, either when it is at rest or during communication.

4) **Risk**
   A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

5) **Cryptography**
   Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.

6) **Steganography**
   Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.

7) **Cryptanalysis**
   Cryptanalysis is the process of studying cryptographic systems to look for weaknesses or leaks of information.

8) **Security goals**
   The objective of Cybersecurity is to protect information from being stolen, compromised or attacked. Cybersecurity can be measured by at least one of three goals-

1.Protect the confidentiality of data.
2.Preserve the integrity of data.
3.Promote the availability of data for authorized users.

9) **Security services**

Security services provided by cryptography are also discussed such as data integrity, privacy/confidentiality, user authentication, message authentication, authorization, digital signatures, validation, access control, and non-repudiation along with their mechanisms.

10) **Security mechanisms**

This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques named Cryptography and Encipherment