

Ques 2 :->

Cryptography :->

-> It is the study and practice of techniques for secure communication in the presence of third parties called adversaries.

-> It deals with developing and analyzing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.

-> Secure communication refers to the scenario where the message and data shared between two parties can't be accessed by an adversary.

Core principals of modern day Crypto.

1. Confidentiality :->

-> It refers to certain rules and

guidelines usually Executed under
Confidentially agreements.

2. Data integrity :->

-> It refers to Maintaining and making
sure that the data stays
accurate.

3. Authentication :->

-> It is the process of making sure
that the data piece of data
being claimed by the user.

4. Non-repudiation :->

-> It refers to the ability to make
sure that a person or a
party associated with a contract.