Network Security

Section: L01

Talha Abdullah Punjabi

QUID: 201903446

Assignment 1

**Task 1:**

In your own words and using appropriate diagrams, design the security of your messaging application and explain how it satisfies the three security properties listed above. Key exchange should be seamless, secure, and take advantages of symmetric and asymmetric properties. To achieve this, use asymmetric cryptography for key exchange, to exchange symmetric keys that will be used for encrypting and decrypting the data by any two users in a communication session. The symmetric keys should only be valid for one session, that is, a new symmetric key should be generated for every new session.

Answer)

Diagram

Description automatically generated

The Users use asymmetric key exchange, and thus exchange the symmetric keys. The users then login to the system, which is the first factor and then the cloud, will verify from the subscriber’s database through hash checking. These databases are stored with backup databases to avoid unavailability. Then second factor takes place that is the verification ID, hence the property of **non-repudiation**. Signup and login, and even the messages are done in AES to avoid any alteration of messages through the channel. The server verifies both users, thus they are authenticated. This method provides the property of **integrity** and **confidentiality**. Thus, after the verification the cloud will provide peer to peer connection between the users who intend to communicate. These messages also are stored in Message databases. The Users can now communicate with each other securely.

**Task 2:**

Database IP and Port Number

Graphical user interface, application

Description automatically generated

Role in the Database

Graphical user interface, application

Description automatically generated

**Messages Table**

Table

Description automatically generated

**Subscribers Table**

Graphical user interface, table

Description automatically generated

**Task 3:**

**Attached Visual Basics Code**