Assignment 1

Question No: 3: Email service which provides the following features.

Authentication: Each party can have its own public/private key pair and the authentication can be ensured by using simple SSL protocol.

Authorization: An Access Control List can be maintained at the server end which ensures that a specific email should or should not be sent to the receiver. The list must contain all the information needed to stop one message to be sent from one user to another.

Confidentiality: Since it is a PKI, each sender can encrypt the email in the other person's public key such that only that person can read the message. In addition to this, can also use session keys so that even if the keys are compromised later on, all the emails aren't.

Data/Message Integrity: This can simply be done by concatenating MAC to the email body to be sent. The receiver can use this MAC to check that if the body of the email is same or changed by an attacker.

Accountability: This can be done by using logs and audit trails, however, the attacker must also not be able to change the trails or be able to detect changes to logs. Otherwise, this is of no use.

Availability: The availability is effected by different factors like a single point of failure or lots of traffic at a time etc. Both of these factors can be handles by using many data-centers at a time and cloning all the emails over them.

Non-repudiation: As the message to be sent is encrypted by the session keys which can not be recreated at will, it is hard to track the emails following through network unless we don't use this protocol which will make our service prone to be attacked.