5.4 Question 4

5.4.A List the available techniques for distributing public keys, ordering them by security level.

- **Public Announcements of Keys**
  Here the public key is broadcasted to everyone. The major weakness of this method is a forgery. Anyone can create a key claiming to be someone else and broadcast it. Until forgery is discovered can masquerade as claimed user.
- **Publicly Available Directory**
  In this type, the public key is stored in a public directory. Directories are trusted here, with properties like Participant Registration, access and allow to modify values at any time, contains entries like name, public-key. Directories can be accessed electronically still vulnerable to forgery or tampering.
- **Public-Key Authority**
  In this type, the public key is stored in a public directory. Directories are trusted here, with properties like Participant Registration, access and allow to modify values at any time, contains entries like name, public-key. Directories can be accessed electronically still vulnerable to forgery or tampering.
- **Public-Key Certificates**
  This time authority provides a certificate (which binds an identity to the public key) to allow key exchange without real-time access to the public authority each time. The certificate is accompanied by some other info such as period of validity, rights of use, etc. All of this content is signed by the private key of the certificate authority and it can be verified by anyone possessing the authority's public key. First sender and receiver both request CA for a certificate which contains a public key and other information and then they can exchange these certificates and can start communication.