Tutorial - IX (Key Management)

1. How does the man in the middle attack occur during the Diffie-Hellman Key Exchange (DHKE) method?
2. What is the major drawback of the DHKE method? Show how it can be addressed in the digital certificates.
3. List the content of digital certificates version x.509 and bear use.
4. Illustrate Key confirmation attack and discuss Kerberos Key Exchange Method.