Dr B R Ambedkar National Institute of Technology, Jalandhar

M. Tech (Computer Science and Engineering)

CS-554, NETWORK SECURITY

Assignment-2 **Submission Date: 03-May-2024**

1. In the Needham-Schroeder protocol, how is Alice authenticated by the KDC? How is Bob authenticated by the KDC? How is the KDC authenticated to Alice? How is the KDC authenticated to Bob? How is Alice authenticated to Bob? How is Bob authenticated to Alice?
2. In the Diffie-Hellman protocol, g = 7, p = 23, x = 3, and y = 5.
   a. What is the value of the symmetric key?
   b. What is the value of R1 and R2
3. List the duties of a PKI.
4. In the Diffie-Hellman protocol, what happens if x and y have the same value, that is, Alice and Bob have accidentally chosen the same number? Are R1 and R2 the same? Do the session keys calculated by Alice and Bob have the same value? Use an example to prove your claims.
5. Discuss the limitations of Diffie-Hellman key exchange algorithm.
6. Define a nonce and its use in entity authentication.
7. For p = 569, q = 683, and s = 157, show three rounds of the Fiat-Shamir protocol by calculating the values and filling in the entries of a table.
8. In the Fiat-Shamir protocol, what is the probability that a dishonest claimant correctly responds to the challenge 15 times in a row?
9. How can a system prevent a guessing attack on a password? How can a bank prevent PIN guessing if someone has found or stolen a bank card and tries to use it?
10. Discuss the various attacks at the network layer with suitable examples.
11. Discuss the UDP storm attack in detail with real-time examples.