Assignment 6

Tasnim Sakib Apon

ID : 20241068

CSE 490

Spring 2021

1. Its a mutal aothentication protocol. K_{AB} is a shered symmetric key. There are several ways that trudy can use to convince Bob that she is Alice.

Such as:

(I) Eavesdropping: In this process the adversary captures the information that was sent in the protocol.

(II) Modification: In this system the adversary alters the information that was sent in the protocol.

2. (a) Yes, Bob authenticates Alice as ~~there~~ here the shared symmetric key k_{AB} is unique to Alice and Bob. Only Bob can decrypt the message encrypted with k_{AB} when it is sent by Alice. So session key is known only to Bob and Alice.

(b) Yes. Alice authenticates Bob as here the shared symmetric key k_{AB} is unique to Alice and Bob. Only Alice can decrypt the messages encrypted with k_{AB} when it is sent by Bob. So session key is only known to Bob and Alice.

3. (a) v is calculated as public key in Fiat-shamir protocol.

$V = S^v \bmod N$

(b) Given,

$N = 55$

$r = 10$

$S = 9$

$\therefore m1 = r^v \bmod N$

$= 10^v \bmod 55$

$= 45$ [Ans]

(c) $r = 10$

$e = 0$

$\therefore M3 = r \bmod N$

$= 10 \bmod 55$

$= 10$ [Ans]

(d) $r = 10,$

$e = 1.$

$\therefore m3 = r * S \bmod N$

$= 10 * 9 \bmod 55$

$= 35$ [Ans]