

OUTPUT :

Verifier Side

Viddeshs-Air:prac8 viddeshgharpure\$ java Verifier

Enter two prime numbers p and q.

p = 3

q = 7

Waiting for a Claimant

Claimant accepted.

Verifier:: Public key -> 21

Claimant:: 1 (public key registraion)

Claimant:: 1 (commitment)

Verifier:: 0 (challenge)

Claimant:: 13 (response to the challenge)

Verifier:: Claimant Verified.

Connection terminated.

Claimant Side

Viddeshs-Air:prac8 viddeshgharpure\$ java Claimant

Connected with the verifier.

Verifier:: Public key -> 21

Choose a number as private key.

(2 4 5 8 10 11 13 16 17 19 20)

-> 8

Claimant:: 1 (registering public key)

Choose a number as commitment (between 1 and 20):: 13

Claimant:: 1 (sending commitment)

Verifier:: 0 (challenge)

Claimant:: 13 (sending response)

Verifier:: Authenticated