IT352: Information Assurance and Security
Lab Assignment 4

Name: Bhagyashri Nilesh Bhamare **Roll No.: 181IT111**

Input from user - p , q , r (Random Number), s (Private Key), c (challenge)

Code-

Validation of input

1) **p and q should be prime**
2) **Random number >=1 and Random number<=p*q-1**
3) **Private Key >=1 and Private Key <=p*q-1**

After validation of input

n=p*q

Witness X=(r*r)%n

Public Key V = (s*s)%n

Response Y = r * (s^c)%n

Authentication check at server-

lhs=(y*y)%n

rhs=(x*(v^challenge))%n

If lhs==rhs :

Then Authenticated user

Else:

Not Authenticated user