IT352: Information Assurance and Security

Lab Program 4

Fiat Shamir Authentication

Name: Chinmayi C. Ramakrishna **Date of Submission:** 3rd March, 2021

Roll No.: 181IT113

Fiat Shamir Authentication algorithm:

1. Client sends public key and witness to verifier
2. Verifier encodes the challenge and sends it to the client.
3. Client receives the challenge, decodes it and computes the response using the following formula:

```
y = r * pow(s, c)
```

4. This encoded response is received by the verifier, its decoded and two values are computed:

```
y2 = (y*y) % n
```

```
xvc = (x * (pow(v, c))) % n
```

5. If y2 == xvc, then a VERIFIED message is sent to the client and NOT VERIFIED otherwise.
6. The test case fails if value of r and s is not less than n-1 at all rounds