Answer to the Question-1

The two different attacks that Trudy can use to convince Bob that she is Alice is given below-

1) Trudy intercepts and records Alice's message between Alice and Bob and then he replies to Bob with message 1 and 3. In this case, Bob will think that trudy is Alice and will always reply with message 2.

2) Trudy opens one connection to Bob and sends first message and recieves second message. After that, he opens another connection to Bob and sends R+1 to Bob in the first message. Then he uses Bob's response to complete the first connection, and lets the second one to timeout.

18107107

Answer to the Question-2

a) No, Alice is not authenticated because no public key operations took place. To authentiate, public key operations are required. In this case, anyone can do it.

b) Yes, ~~he~~ Bob does authenticate Alice. In this case, ~~Alice~~ Bob send Alice E(SRVR,K) after the public key operation it means he authenticates Alice.

Answer to the Question-03

Given,

$N = 55$

$S = 9$

a) we know

$$V = S^2 \bmod N$$

$$= 9^2 \bmod 55$$

$$= 81 \bmod 55$$

$$= 26 \quad \text{(Ans)}$$

b) Here,

$r = 10$

First message, $u = r^2 \bmod N$.

$$= 10^2 \bmod 55$$

$$= 100 \bmod 55$$

$$= 45 \quad \text{(Ans)}$$

c) Given,

$r = 10$

$e = 0$

Third message,

$y = r * s^e \bmod N$

$= 10 * 9^0 \bmod 55$

$= 10 \bmod 55$

$= 10$ (Ans)

d) Given,

$r = 10$

$e = 1$

third message, $y = r * s^e \bmod N$

$= 10 * 9^1 \bmod 55$

$= 35$ (Ans)