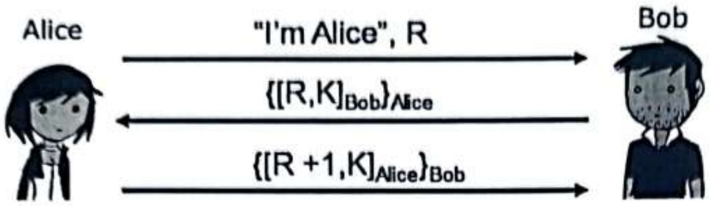
3

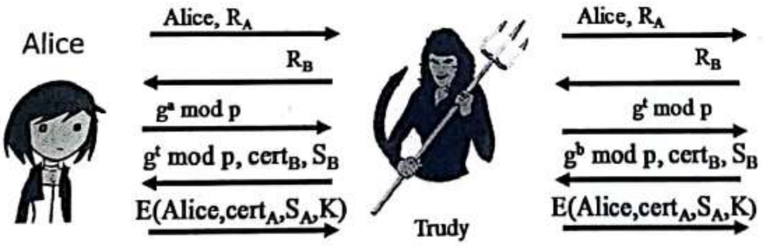


4

Briefly explain whether or not the resulting protocol provides an effective means for secure mutual authentication and a secure session key K.

so, in the above scenario, the resulting protocol provides an effective means fo secure mutual authentication because both Alice & Bob share a mutual signature through a private protocol.

Also the k is a session key. which will be expired soon. So k is also secure.


Alice
$Alice, R_A$
R_B
$g^a \bmod p$
$g^t \bmod p, cert_B, S_B$
$E(Alice, cert_A, S_A, K)$
Trudy
$Alice, R_A$
R_B
$g^t \bmod p$
$g^b \bmod p, cert_B, S_B$
$E(Alice, cert_A, S_A, K)$
Bob

3

In the above SSH protocol, Trudy is pursuing MiM attack. Where does this attack fail?

MiM attack will fail in the fourth step.

Trudy can get the certificate cause Bob isn't encrypting it while he sending the certificate. Also Bob will get g^t mod p so here trudy can also get the information.

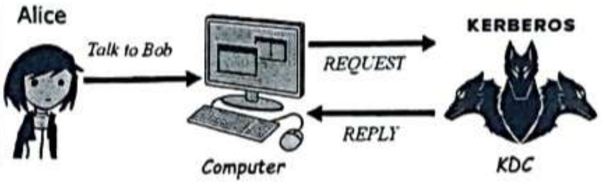
& g^t will help trudy to understand the information.

1 Consider the Kerberos interaction as shown in the diagram and **explain**, 4

a. Why is the ticket to Bob encrypted with K_B?

c. In the REPLY message, why is the ticket to Bob encrypted with the key S_A?

REQUEST = (TGT, authenticator) where
authenticator = E(timestamp, S_A)
REPLY = E("Bob", K_{AB}, ticket to Bob, S_A)
ticket to Bob = E("Alice", K_{AB}, K_B)



(a) The ticket to Bob encrypted with k_B cause it is the key that's only known by Bob. & only he can decrypt it.

(b) S_A is the session key here & it will expire after a while. so, mim get labelled. That's why the ticket to Bob encrypted with S_A.

2 Assume that, N = 80 and a secret S is 25 (Should be known by Alice and Bob). If Alice chooses r = 10 and Bob sends e = 1, prove that Alice knows the secret using Fiat-Shamir protocol. 4

$$\text{Alice} \xrightarrow[\quad]{x = r^2 \bmod N = 10^2 \bmod 80 = 20} \text{Bob}$$

$$\xleftarrow{\quad e = 1 \quad}$$

$y = r * s^e \bmod N$
$= 10 * 25^1 \bmod 80$
$= 10$

$$\xrightarrow{\qquad\qquad}$$

$v = s^2 \bmod N$
$= 25^2 \bmod 80$
$= 65$

For B;
$y^2 = x * v^e \bmod N$
$\Rightarrow 10^2 \underset{80}{\bmod} = 20 \times 65^1 \bmod 80$
$\Rightarrow 20 = 1300 \bmod 80$
$= 20$

$\therefore$ $20 = 20$ or L.H.S = R.H.S

so, Alice knows the secret.

Crop Extract Text Share CS Sign More