2012

Question 1

a

Bob receives a message from Alice and wants to ensure the message

- hasn't been seen since being sent by Alice (confidentiality)
- hasn't changed since sent my Alice (integrity)

You can have one without the other

- Confidentiality without integrity: The message is encrypted but not signed
  - Trudy can intercept the original message and send her own message encrypted with your public key. Message has been changed, but original is still confidential.
- Integrity without confidentiality: The message is signed but not encrypted
  - Trudy can intercept the message and read it using the sender's public key. However, she can't tamper with the message, otherwise it can't be validated at the other end.

Signing:

1. Alice writes a message, M
2. She computes the hash of the message, $H(M)$
3. She signs the message with her private key or symmetric key, $K_A^-(H(M))$
4. She sends the message with the signed hashed version, $(M, K_A^-(H(M)))$ (can also optionally sign the message too, done in PGP)
5. Bob decrypts the signed version with Alice's public key or the symmetric key, $H(M) = K_A^+(K_A^-(H(M)))$
6. He computes the hash of his message $H(\bar{M})$
7. He checks if his version of the hashed message matches Alice's newly encrypted version of the hashed message

b

$$\text{CipherText} = (\text{PlainText})^d \mod n$$

$$\text{PlainText} = (\text{CipherText})^e \mod n$$

Bob:

- public key $= (3, 33)$
- private key $= 7$

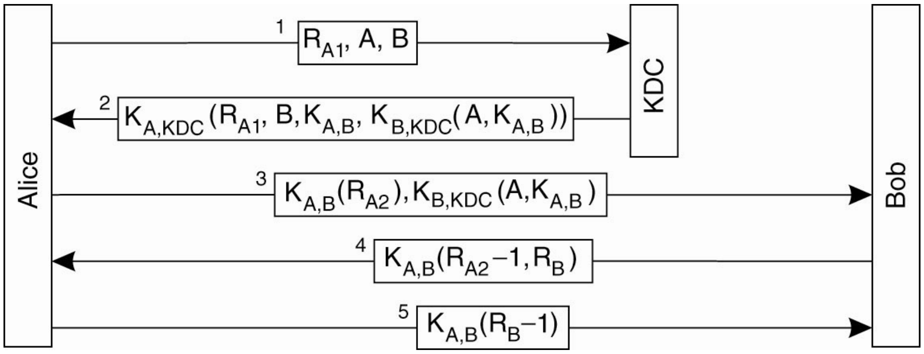
Trudy:

- public key $= (7, 33)$
- private key $= 3$
- Bob encrypts message $m = 9$
  - $9^7 \mod 33 \equiv 15$
- Trudy decrypts message $c = 15$
  - $15^3 \mod 33 \equiv 9$

c

The Needham-Schorder authentical protocol uses a Key Distribution Center. The first challenge is used to authenticate the KDC and prevent against replay attacks. The KDC responds with her ticket $K_{B,KDC}(K_{A,B}))$ which Bob can decrypt to get the shared key between himself and Alice. They also send the challenge (or nonce) encrypted with $K_{A,B}$.

Alice then sends another challenge to Bob, encrypted with the shared key the KDC generated, to also authenticate him and protect against replay attacks. Bob sends back this challenge minus one, along with his own challenge. This proves to Alice that not only does he know the key, but he has also decrypted the challenge. Alice also sends back his challenge minus one.



Alice
KDC
Bob
1 R_{A1}, A, B
2 $K_{A,KDC}(R_{A1}, B, K_{A,B}, K_{B,KDC}(A, K_{A,B}))$
3 $K_{A,B}(R_{A2}), K_{B,KDC}(A, K_{A,B})$
4 $K_{A,B}(R_{A2}-1, R_B)$
5 $K_{A,B}(R_B-1)$

Figure 1: Needham-Schroder

d

Authentication header provides message authentication and integrity services. Doesn't work through a NATed network as it hashes both the payload and header of a packet whilst a NAT changes the IP header of a packet during translation which the receiving device will then reject.

Encapsulation Security Payload provides encryption. In tunnel mode, ESP provides integrity and authentication services. The hash for data integrity does not include the IP header of the packet, so ESP works normally through a NATed device.