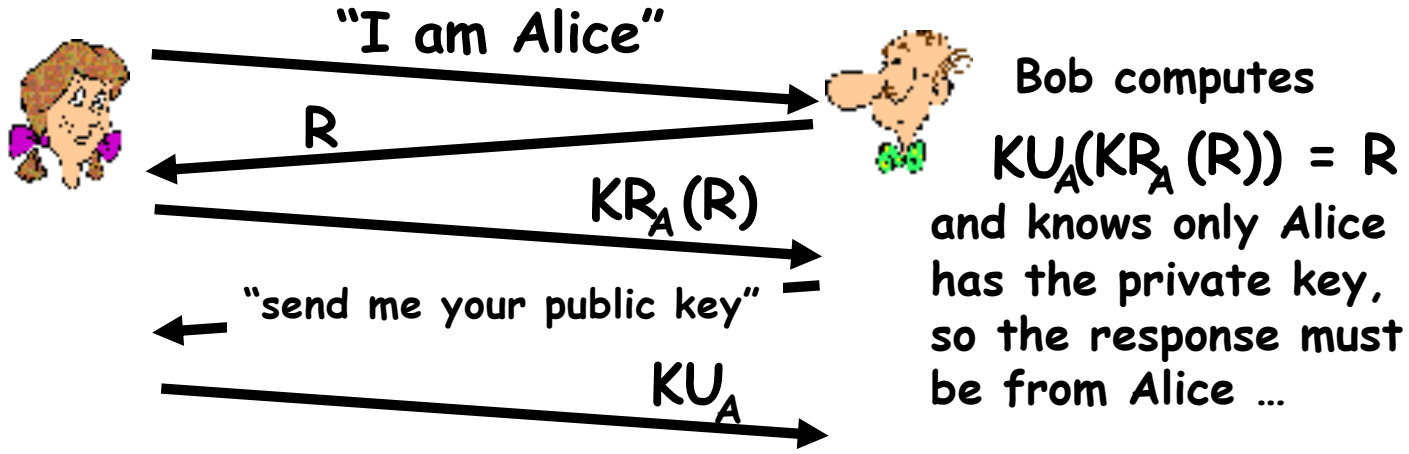
Feedback on Topic 9 Ex

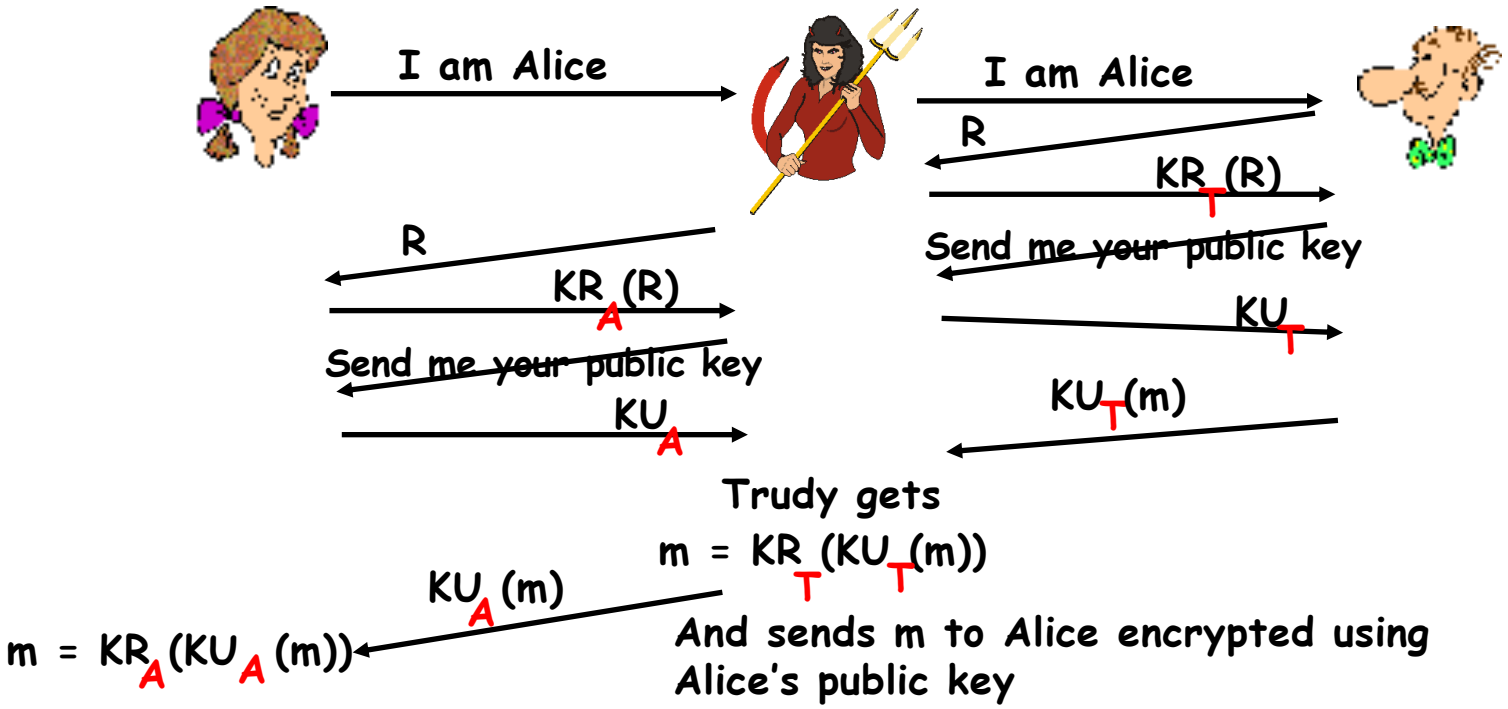
Exercise Question – E9.1

Many authentication protocols are based on the use of a symmetric key/secret. What if that 'trust relationship' has not been established? Using nonce (random number) and a public-key cipher can be a solution. Is the following authentication protocol secure? Justify your answer.



Exercise Question – E9.1 - A

Man-in-the-middle-attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)



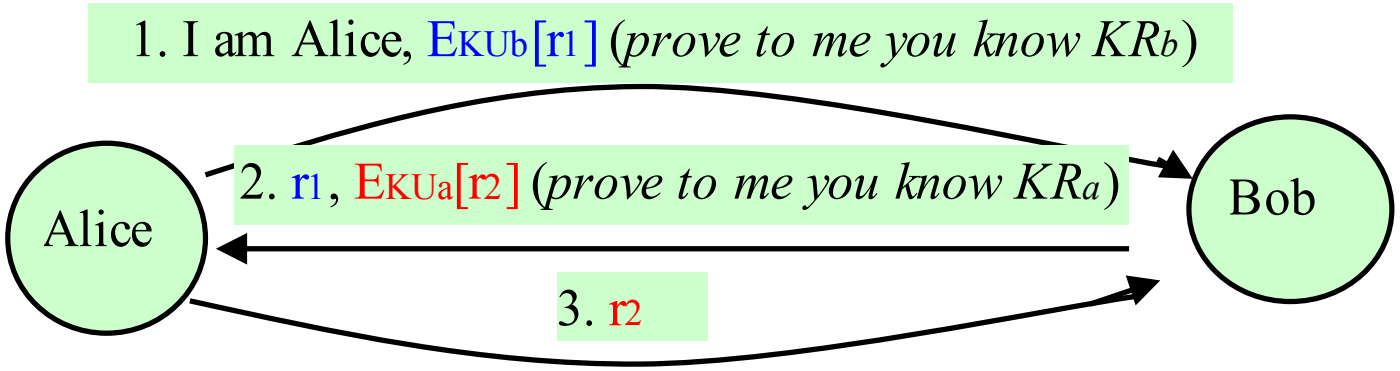
Exercise Question – E9.2

Design two different X.509 certificate based authentication protocols to support mutual authentication between two entities, Alice and Bob.

Exercise Question – E9.2 – A(1)

X.509/certificate based Authentication (using public keys)

- Assuming that Alice and Bob have already got each other's certificates and trust the certificates.
- As only *B* can recover the random number (nonce), r_1, the blue items in messages (1&2) authenticate *B* to *A*.
- Similarly, the red items in messages (2&3) authenticate *A* to *B*.



Exercise Question – E9.2 – A(2)

X.509/certificate based Authentication (using signatures)

- $Cert_a$ and $Cert_b$ are respectively Alice's and Bob's X.509 certificates.
- As only *B* can generate the rightful signature, the blue items in messages (1&2) authenticate *B* to *A*.
- Similarly, the red items in messages (2&3) authenticate *A* to *B*.