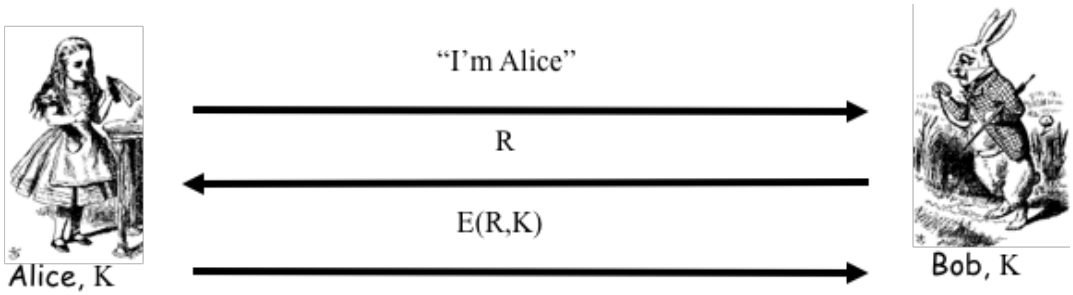
Tutorial #9
Security in Computing COSC2356/2357

Q1. Discuss if the following authentication protocols are secure or not:

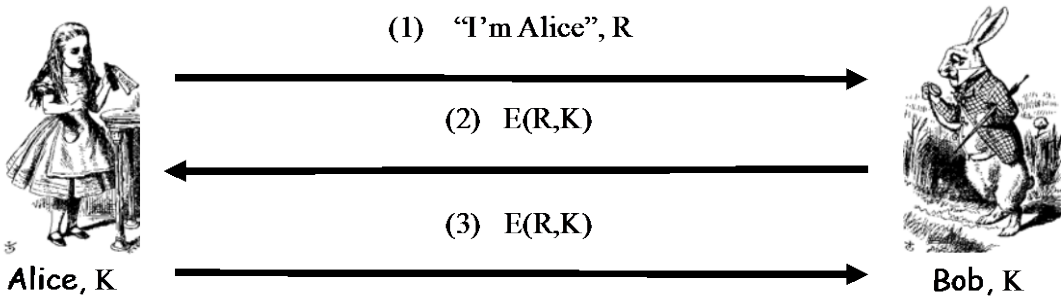
(a)



Answer:

- In the figure above, the **replay attack** is prevented by using **nonce (R)**
- Bob authenticates Alice with the help of **symmetric key cryptography**. Both Alice and Bob shares a **common key (K)**
- However, Alice does not authenticate Bob
- **Problem: no mutual authentication**

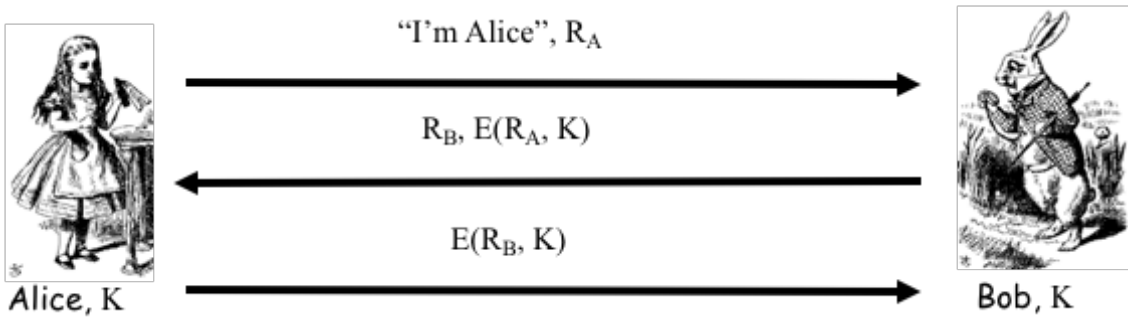
(b)



Answer:

- The message (3) is just a replay of the second. Thus, it does not prove anything about sender (i.e. Alice).
- The sender can be Alice or Trudy.
- We need to authenticate both Sender (Alice) and Receiver (Bob)
- **Problem: no mutual authentication**

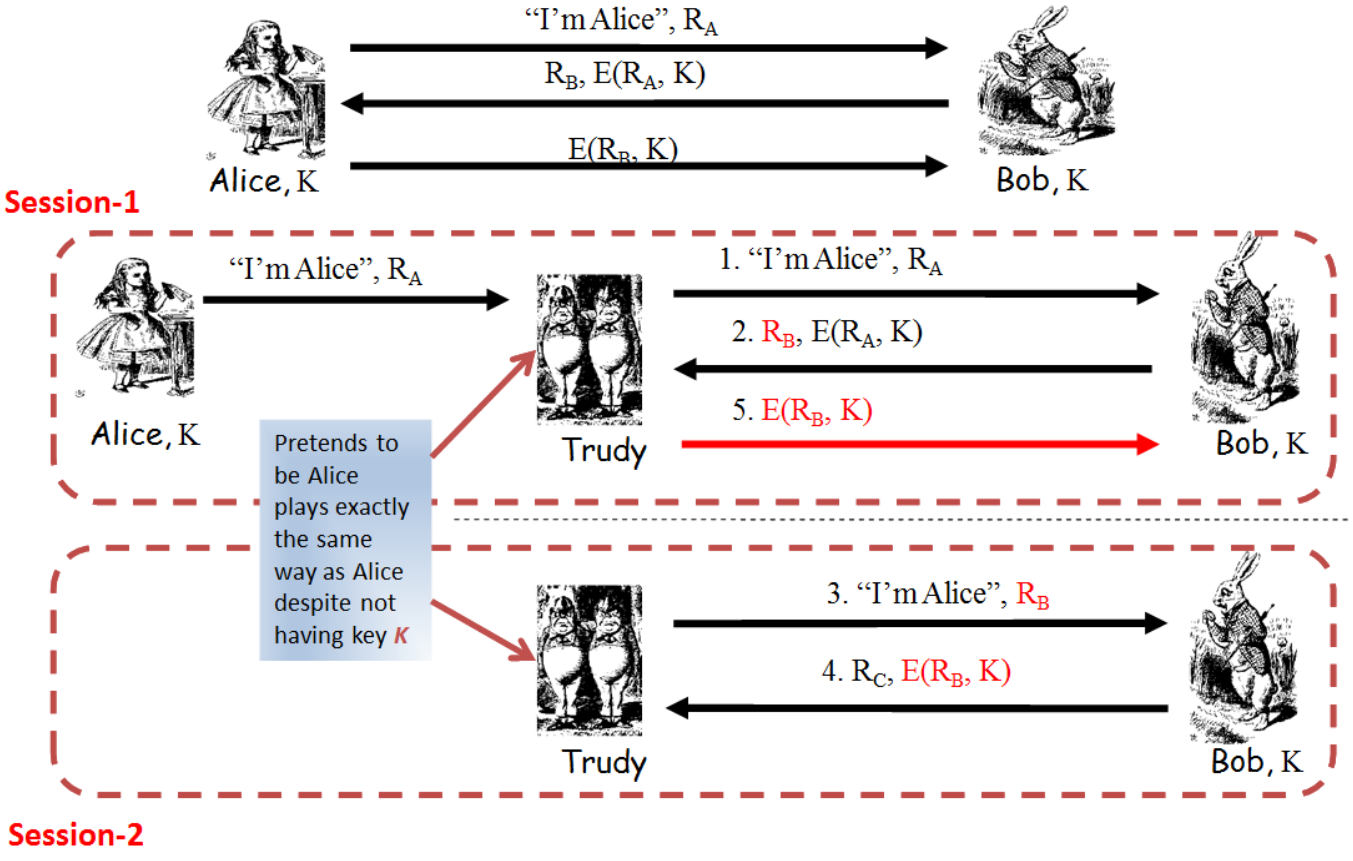
(c)



Answer:

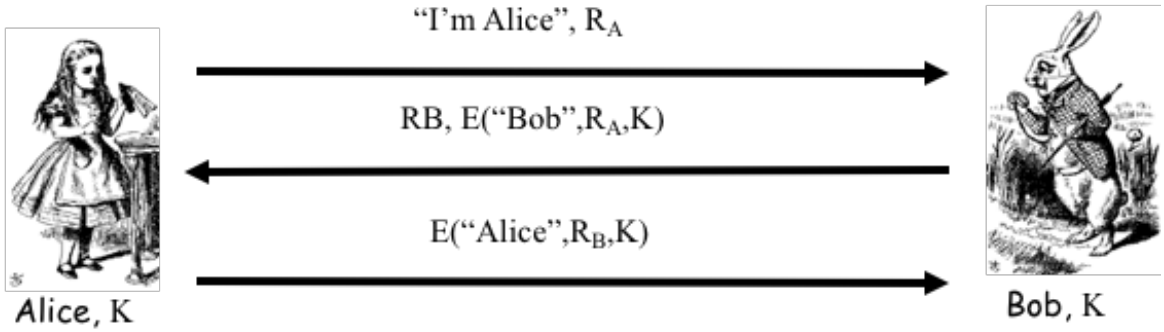
- Two nonce: R_A and R_B, are used to authenticate both Bob and Alice, respectively.
- **Problem: Insecure. Man-in-the-Middle (MiM) attack is possible**
- **The attack is discussed below:**

(Man-in-the-Middle attack Scenario)



Q2. Discuss how can we achieve mutual authentication for the scenario specified in the Q1(c)?

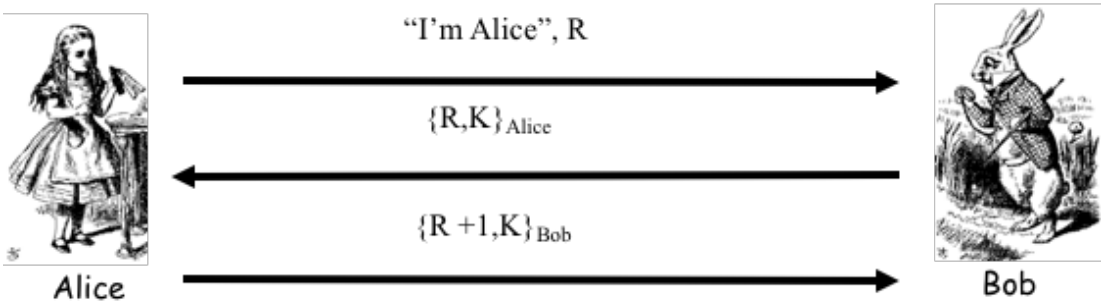
Answer:



- Two nonce: R_A and R_B, are used to authenticate both Bob and Alice, respectively.
- Additionally, user's identity is encrypted together with nonce.
- Advantage:
- Trudy cannot use a response from Bob for the third message
- Bob will realize the he encrypted it himself
- Mutual Authentication achieved

Q3. Does the following authentication protocol achieves mutual authentication? Think and discuss:

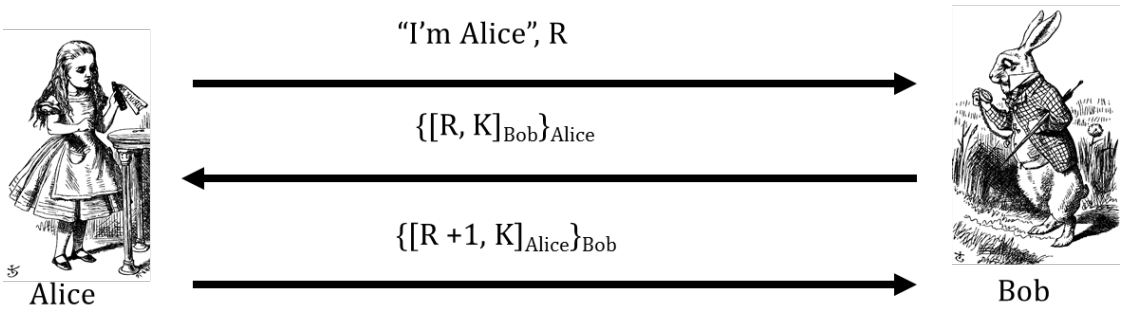
(a)



Answer:

- Public-key cryptosystem is used to share a session key
- Bob authenticates Alice with the help of public-key cryptography. Alice and Bob shares a session key
- However, Alice does not authenticate Bob
  - Alice is authenticated and session key is secure
  - Alice's "nonce", R, useless to authenticate Bob
  - The key K is acting as Bob's nonce to Alice
- **Problem: No mutual authentication. NO, the protocol is insecure.**

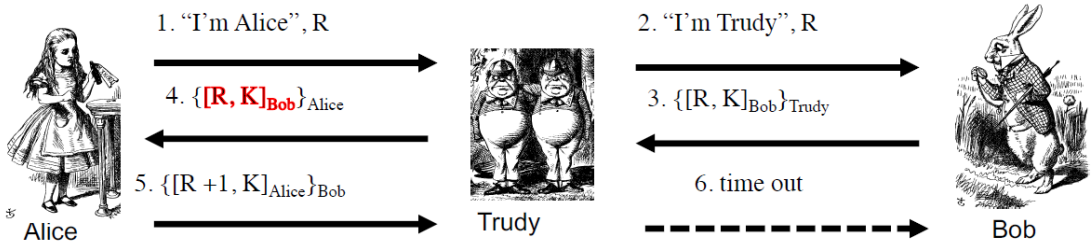
(b)



Answer:

- **Public-key cryptosystem** is used with signature.
- Signed the message first and encrypts (**signature and encryption**)
- Reveals less information. **Trudy cannot prove herself as Alice to Bob.**
- Both sender and receiver are authenticated. From that perspective, **mutual authentication is achieved, and the protocol is secure.**

  However, Trudy can convince Alice that she is Bob. The scenario can be illustrated as follows:



- Trudy can get **[R,K]Bob** and ***K*** from step (3).
- Alice uses the same ***K***
- Alice thinks that she is talking to Bob. From that perspective, **mutual authentication is not achieved, and the protocol is not secure.**