Congratulations! You passed!

TO PASS 80% or higher

Keep Learning

GRADE
100%

Week 5 - Problem Set

LATEST SUBMISSION GRADE
100%

1. Consider the toy key exchange protocol using an online trusted 3rd party (TTP) discussed in Lecture 9.1. Suppose Alice, Bob, and Carol are three users of this system (among many others) and each have a secret key with the TTP denoted k_a, k_b, k_c respectively. They wish to generate a group session key k_{ABC} that will be known to Alice, Bob, and Carol but unknown to an eavesdropper. How would you modify the protocol in the lecture to accommodate a group key exchange of this type? (note that all these protocols are insecure against active attacks)

1 / 1 point

- ○ Alice contacts the TTP. TTP generates a random k_{ABC} and sends to Alice

  $$E(k_a, k_{ABC}), \quad \text{ticket}_1 \leftarrow E(k_b, k_{ABC}), \quad \text{ticket}_2 \leftarrow E(k_c, k_{ABC}).$$

  Alice sends k_{ABC} to Bob and k_{ABC} to Carol.
- ◉ Alice contacts the TTP. TTP generates random k_{ABC} and sends to Alice

  $$E(k_a, k_{ABC}), \quad \text{ticket}_1 \leftarrow E(k_b, k_{ABC}), \quad \text{ticket}_2 \leftarrow E(k_c, k_{ABC}).$$