SIL765: Networks and System Security
Semester II, 2020-2021
Assignment-2

February 25, 2021

Submission Instructions

1. You will submit the assignment on Moodle.
2. You should submit a single pdf file which should be named as: ⟨Your Entry Number⟩-assignment-⟨Assignment Number⟩.
   Example: 2020EE10350-assignment-2.pdf
3. You can use Piazza for any queries related to the assignment.
4. Failure to strictly follow the above steps will adversely affect the grades.

Problem: Secret Key Sharing (100 Marks)

In this problem, you need to enable two nodes, Alice and Bob, to securely share a secret key, under different conditions. You can assume that the public key of all parties are published and known to other parties. You can consider AES (with block size = 128 bits) for encryption using secret key. You can utilize RSA (with $n = 1024$) for encryption using public/private key.

Conditions

1. Condition-1 (25 Marks): Assume that there is a trusted third party, Charlie. In other words, Charlie is trusted by both Alice and Bob. Under these conditions, design a key agreement protocol to enable Alice and Bob to share a secret key $K_{a,b}$.
2. Condition-2 (75 Marks): Assume that there is a honest-but-curious third party, Charlie. In other words, Alice and Bob do not want to reveal their secret key to Charlie. However, Alice and Charlie share a secret key $K_{a,c}$, and Bob and Charlie share a secret key $K_{b,c}$. Under these conditions, design a key agreement protocol to enable Alice and Bob to share a secret key $K_{a,b}$.

Grading

For each of the two conditions, the grades will be assigned based on two evaluation criteria.

- *Security (50%):* The proposed key agreement protocol should not be vulnerable to known attacks. In the submitted file, include arguments about how your schemes prevents potential attacks, such as man-in-the-middle attack, replay attack, etc.
- Computational efficiency (25%): How many operations would it take for Alice and Bob to successfully complete the protocol? In the submitted file, include the discussion on techniques employed by you to minimize the computational cost.
- Communication efficiency (25%): How many bits are transmitted by Alice and Bob to successfully complete the protocol? In the submitted file, include the discussion on techniques employed by you to minimize the communication cost.