IIT PALAKKAD

COMPUTER SCIENCE AND ENGINEERING
Indian Institute of Technology, Palakkad
CS4150: Computer Networks Lab
Lab 11 (RSA and Digital Signature)

28 Oct, 2020

Time: 60 hrs

1. Write a code to generate the public and private keys, using RSA, for two users **A** and **B**. Store these keys as ASCII in the files `A.pub`, `A.pri`, `B.pub` and `B.pri`. [50]

2. **A** wants to digitally sign a message and securely send it to **B**. Write a code that will sign and encrypt the ASCII text in file `message.txt`. Store the signed and encrypted text as ASCII in the file `secret.txt`. *Note: You are required to use the keys generated in the previous question.* [25]

3. Write a code that will decrypt the message in `secret.txt` and verify if the message was indeed sent by **A**. If the verification is successful, your code should print the original message from **A**. Else, your code should print the text `Message not verified`. *Note: You are required to use the keys generated in the first question.* [25]

End of paper