Security and Applied Cryptography Lab. (PV181)

Assignment - 4

Oct. 13, 2021

Lecturer: Arnab Roy

This is a programming assignment. Please upload your (python) scripts via the course web page. The deadline for submission is **Oct. 20, 2021, 08:00**. Your answer should be contained in one `.py` file. Please name the submission file as `yourfirstname_hw2`.py. It must contain comments so that it is reasonably easy to understand how to run the script for evaluating each answer.

Problems

1. Suppose Alice and Bob want to communicate secret keys using RSA asymmetric encryption. They want to obtain the certificates for their public keys (2048) from a CA. Write a function using which you can issue a RSA-SHA256 certficate for CSR from Alice or Bob. You must use 4096 bit key. You can use the function that you wrote during the lecture to generate CSR from Alice and Bob. Your script must contain these CSR generating function(s) as well. [2 points]

2. Write a function for Alice say `alice_send_skey`, which will take the certificate issued to Bob and other necessary inputs. Then it will perform the following

   (a) Verify the certificate.

   (b) If the verification is successful then it will return the suitably encrypted 128-bit cryptographically secure secret key K that is generated by Alice.

   [4 points]

3. Write a function for Bob say `bob_recv_skey`, which will take the output from the above function, certificate of Alice and other necessary inputs. Then it must perform the following

   (a) Verify the certificate of Alice

   (b) If the verification is successful then it will decrypt the message from Alice and extract the secret key K

   [4 points]