E0254: Network and Distributed Systems Security

Assignment No. 4

Date given: Oct. 31, 2017

Submission Due Date: Nov. 30, 2017

Write a program to achieve the following. Let A, B, C be three nodes. Nodes B and C get a public key certificate about their public key from node A. Then they use the public key certificate to establish a shared key between them. Nodes B and C would give the following information to node A, which would issue the public key certificate to them after verification through other channel like mobile number and e-mail. In the assignment, you do not need to do these verifications. However, note that node A still needs to verify that the sender indeed has the corresponding private key. You can only use 512-bit integer as in case of assignment 3. You can assume that the public key of node A is known.

(i) Name of the user(In reality as recorded for mobile number or Aadhar card or NIN)
(ii) Mobile number
(iii) E-mail address
(iv) Aadhar number or any other national identification number
(v) Diffie-Hellman or RSA public key
(vi) Type of public key
(vii) Public key parameters
(viii) Other functions such as hash function used in the public key certificate

If you use Diffie-Hellman public key, you can use assignment 3 to establish the shared key using the public key certificates. But if you choose to use RSA public key, you need to use a suitable protocol to establish a shared secret key using the public key certificates.

Please submit the tarred and compressed files of your assignment using e-mail along with a description of the assignment. The description should include the protocols used in the implementation, and the traces of output.