Network Security

Assignment 4

Ekansh 2021044

Lakshay 2021059

INDRAPRASTHA INSTITUTE *of*
INFORMATION TECHNOLOGY
DELHI

Introduction

On-the-go verification of Driver's License

In this assignment, we are required to -

- Develop an On-the-go verification of Driver's License protocol

- We had multiple RTOs and One National TO -
    - Clients (Traffic Police Officer) can verify Validity of a License using digital signal verification
    - Digital Signature ensures Non-Repudiation, Message Integrity and Authenticity.

RSA

We have created a RSA class, that will be used to -

- **Keys Pair -** It has the function to generate pair of public key and private key (*rsa_keys).*
- **Encrypt Message -** To encrypt the message, it has the function ***rsa_encrypt*** that takes *message* and *public_key* as parameters and encrypt the message by converting into integer and then calculate using **(int^e)**mod**n**.
- **Decrypt Message -** To decrypt the message, it has the function ***rsa_decrypt*** that takes *encrypted_message* and *public_key* as parameters and decrypt the message by using **(message^d)**mod**n** and then convert integer back to text.

PKDA

Here, the PKDA have three functions which are mainly using for the overall functionality of it.

- **Send Message -** It is used to connect to the host using the port and the host id, then it will send the message by encoding it.
- **Receive Message -** It will listen the message from the port given as parameter, and receive the data which will then decoded.
- **Request PKDA -** It will first decrypt the request given to it using its own private key, then it will return the request to send encrypted message that will be encrypted using its private key to the localhost and the specified address.

Client

Here, Client has only one functionalities -

- **License Verification -** On receiving a license Client sends the signed certificate to one of the RTOs along with additional information such as by whom the certificate was signed to authenticate originality of document.

Running the Code

To run the code, you need to keep all the files in a folder, then simple run ***Client.py*** using *python Client.py* in terminals, and ***TransportAuthority.py*** using *python* in another terminal. To generate Signed Certificates another file by the name of ***SignCert.py*** is available.

THANK YOU