Assignment 6: Implement PKI-Based Authentication

In this assignment, a PKI-based protocol for authentication and encryption will be implemented. Suppose a system comprises an application server, its clients, and a centralized certificate authority (CA). The CA in this lab is only a toy one. Real deployment of CAs usually have a hierarchical structure.

1 Initial Setup

CA has an identity ID_{ca} and its own public key PK_{ca} and private key SK_{ca}. We assume that CA's public key is publicly accessible and verifiable so that the application server and client can use PK_{ca} securely. In addition to message exchanges, the entities also perform operations such as key generation, signature generation/verification, etc. as explained below.

Application Server has an identity ID_s.

Client has an identity ID_c and its own network address: IP address IP_c and $Port_c$.

Note that there is no information preshared among the CA, application server, and client except that the CA's public key PK_{ca} is universally known.

2 Protocol

The flows of messages in the whole protocol is shown in Table 1. $RSA_{(\cdot)}$ denotes RSA encryption with the specified public key, $DES_{(\cdot)}$ means DES encryption with the specified DES key, and $Sign_{(\cdot)}$ is RSA signature generation with the specified private key.

Step (1): Before serving the clients, the application server (**S**) firstly registers with the certificate authority (**CA**) to obtain its own public/private keys and certificate. The message is encrypted with **CA**'s public key such that only **CA** can decrypt the message. The message includes a temporary DES key K_{tmp1} for **CA** to encrypt the response message. This is necessary because the response contains the private key for **S**, which is very sensitive.

Step (2): **CA** decrypts the message with its own private key and then generates a public/private key pair along with a certificate for the application server **S**. The certificate $Cert_s$ is an RSA signature over some basic information associated with **S** and **CA**.

Step (3) and (4): Client **C** acquires the public key and certificate of **S**. Messages in these steps are plaintexts since no sensitive information is included in this round.

Step (5): Before providing information for registration, **C** first verify the legimacy of the received public key PK_s and certificate $Cert_s$. $Cert_s$ is in essence an RSA signature signed with **CA**'s private key, so **C** can verify the signature with **CA**'s public key. If verified, it means that the received public key PK_s is indeed the legitimate one for the application server with identity ID_s. Thus, **C** encrypt his identity and address information with PK_s along with a temporary DES key K_{tmp2}, and sends the message to **C**.

Table 1: Message flows of the protocol.

Application Server Registration: to obtain its public/private key pair and certificate
(1) **S** $\rightarrow$ **CA**: $\text{RSA}_{PK_{ca}}[K_{tmp1}\|\|ID_s\|\|TS_1]$
(2) **CA** $\rightarrow$ **S**: $\text{DES}_{K_{tmp1}}[PK_s\|\|SK_s\|\|Cert_s\|\|ID_s\|\|TS_2]$, where $Cert_s = \text{Sign}_{SK_{ca}}[ID_s\|\|ID_{ca}\|\|PK_s]$
Client Registration: to obtain a session key for further communication
(3) **C** $\rightarrow$ **S**: $ID_s\|\|TS_3$
(4) **S** $\rightarrow$ **C**: $PK_s\|\|Cert_s\|\|TS_4$
(5) **C** $\rightarrow$ **S**: $\text{RSA}_{PK_s}[K_{tmp2}\|\|ID_c\|\|IP_c\|\|Port_c\|\|TS_5]$
(6) **S** $\rightarrow$ **C**: $\text{DES}_{K_{tmp2}}[K_{sess}\|\|Lifetime_{sess}\|\|ID_c\|\|TS_6]$
Service Request: to obtain application data
(7) **C** $\rightarrow$ **S**: $\text{DES}_{K_{sess}}[req\|\|TS_7]$
(8) **S** $\rightarrow$ **C**: $\text{DES}_{K_{sess}}[data\|\|TS_8]$

Step (6): Upon receiving the registration request, **S** generates a session key (DES key) for secure communication with **C**.

Step (7) and (8): With the session key, **C** can request service data from **S** securely.

You will implement the above protocol. To this end, you need to use proper crypto libraries in your favor to realize RSA operations, including RSA key generation, encryption, decryption, signature generation, signature verification. Also, you will also reuse your functions for socket communication and DES operations.

Hardcodeing values. Please hardcode ID_{ca} to "ID-CA", ID_s to "ID-Server", ID_c to "ID-Client", req to "memo", $data$ to "take cis3319 class this afternoon" in your code. Use your own IP address and port for IP_c and $Port_c$ such as "127.0.0.1" and "5000", respectively.

3 Deliverable

Submit your source code along with a README file as a zip file to Canvas.

No demo.

Due: 5pm, April 24.