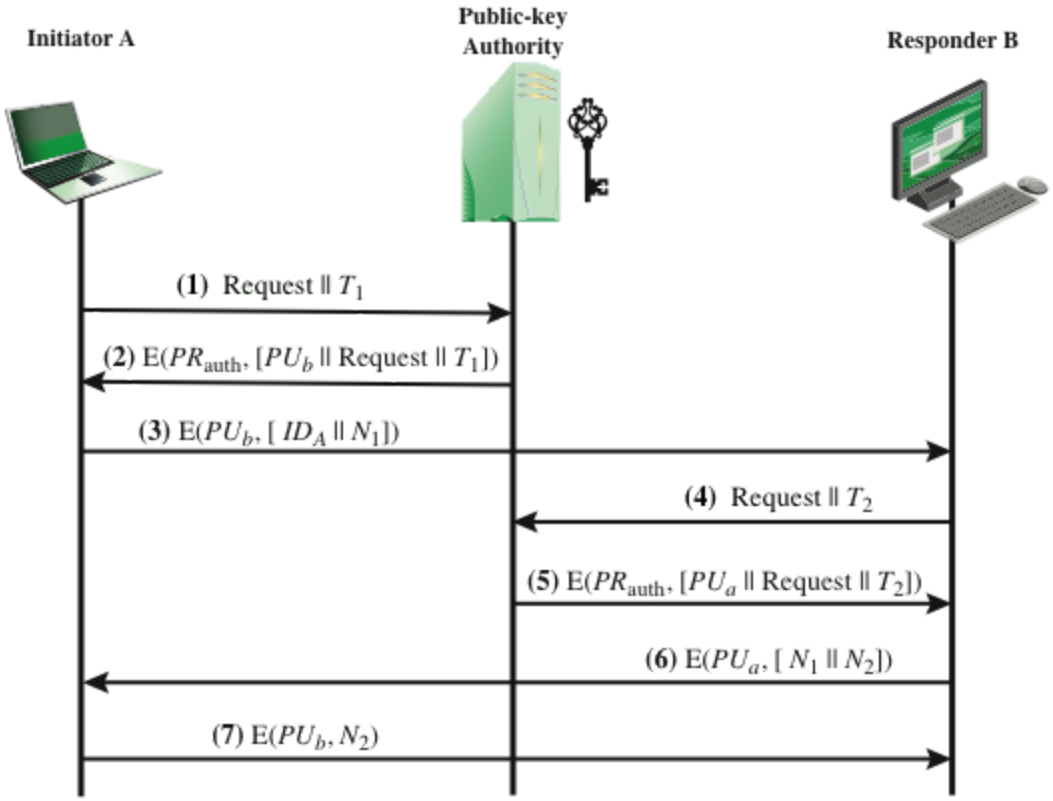
PUBLIC KEY DISTRIBUTION AUTHORITY

SIL765 - Assignment 2

Submitted By:
Mehak
2018MCS2143

PROBLEM STATEMENT

You are required to (a) build a PKDA, and (b) build clients that wish to confidentially send messages suitably encrypted with public key of receiver, but only after they know the other client's public key in a secure manner.
You are required to (a) build a, and (b) build clients that wish to send messages suitably encrypted with public key of receiver but of course only after they know each other's public key in a secure manner. Specifically use the scheme described below.



To do so, you will need to:
Assume:
4. that clients already (somehow) know the public key of the distribution authority, PKDA,
5. that the clients have their corresponding private keys with themselves, and
6. that PKDA has the public keys of all the clients,

Messages between PKDA and clients are encrypted using RSA algorithm and PKDA's private key,
Encrypted messages are sent/received between clients once they have each other client's public key, and finally
Find a way to generate and encode "current time" and "nonces".
Use the above to ensure client A can send 3 messages to B, viz Hi 1, Hi 2, and Hi 3. Client B in turn responds with Got-it 1, Got-it 2, etc. to messages received from A.

INTRODUCTION

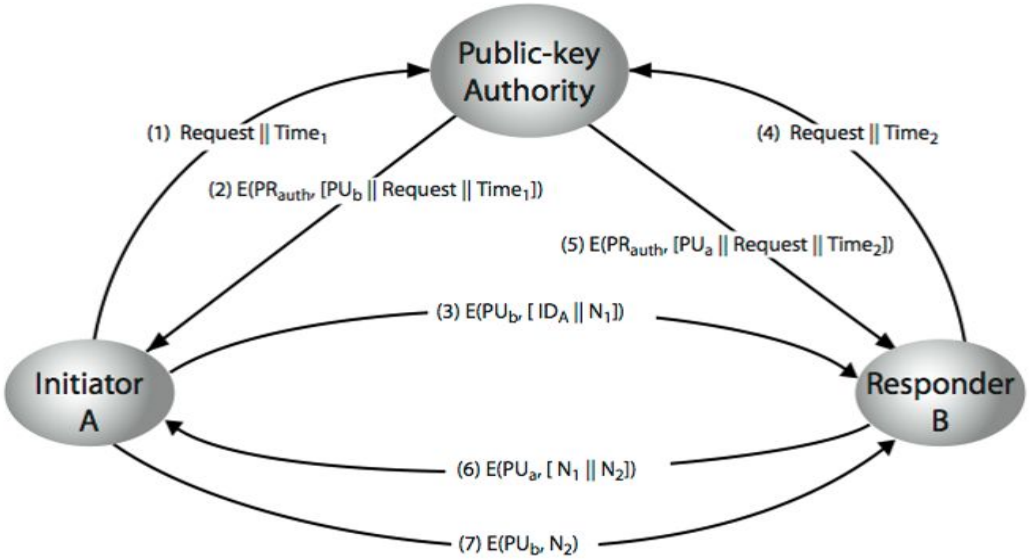
A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred. PKI provides assurance of public key. It provides the identification of public keys and their distribution. PKDA provides the facility to share the public keys between clients securely.

SYSTEM SPECIFICATION

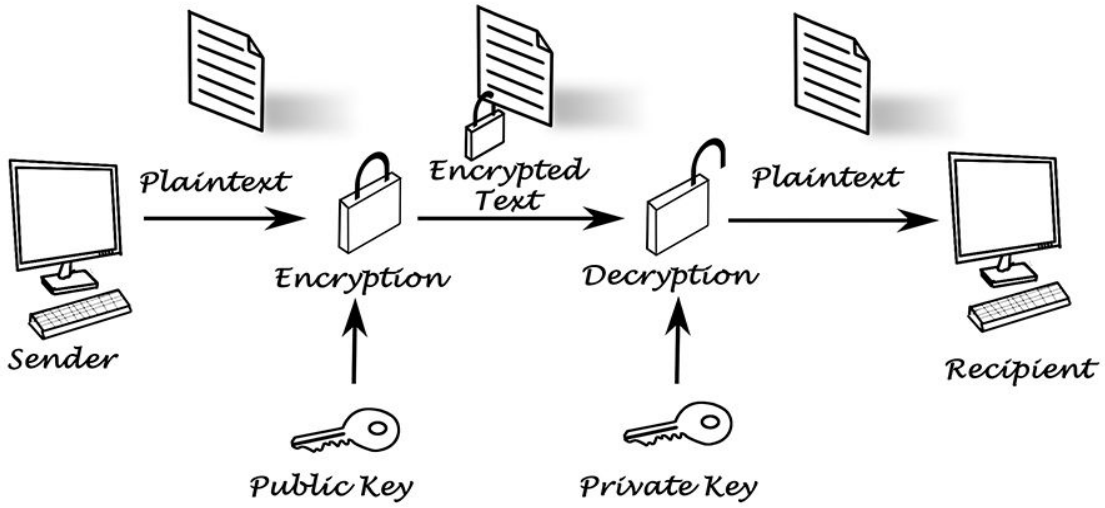
Language Used : Python
Assumptions :
1. PKDA has public keys of Client A and Client B.
2. Clients A and B have their private keys and public key of PKDA.

PROCEDURE

1. Key Exchange (Communication between clients and PKDA)

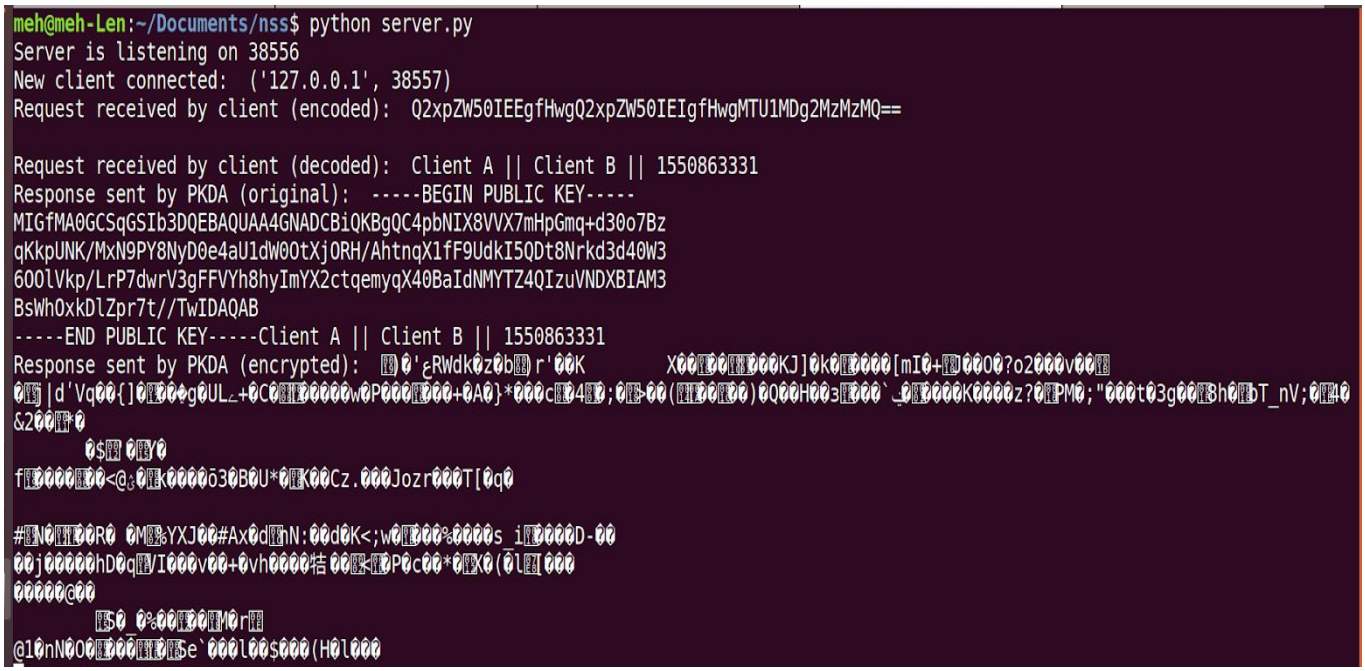


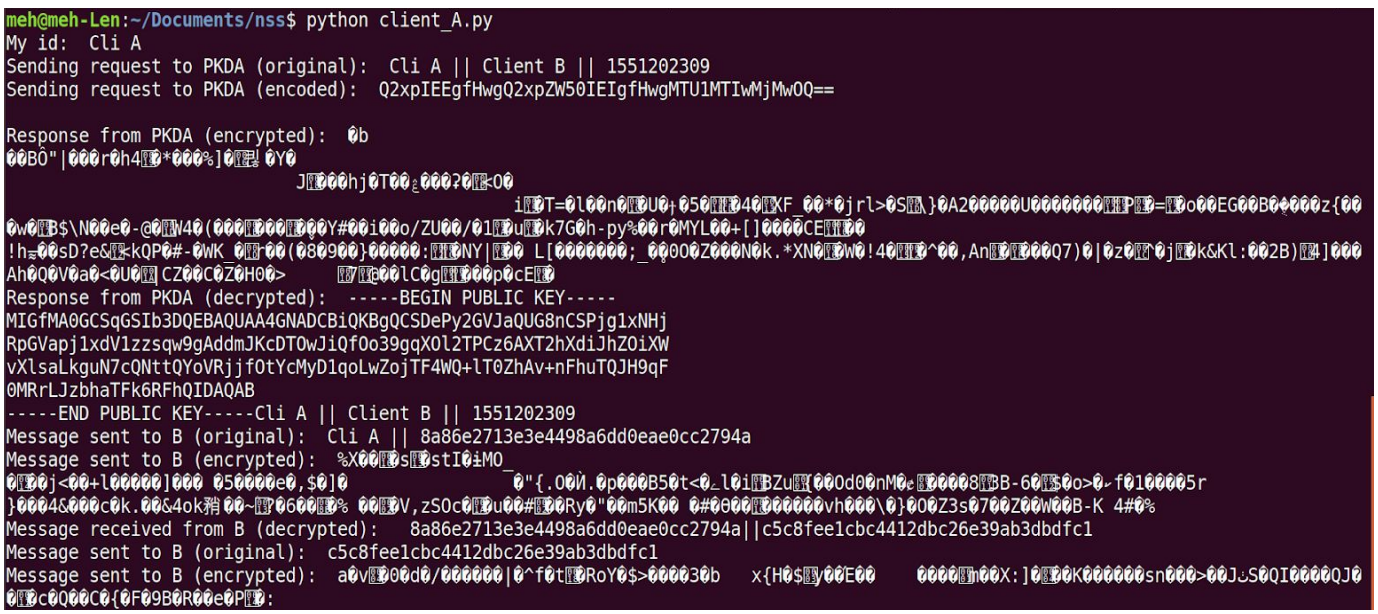
2. Communication between clients using public key encryption



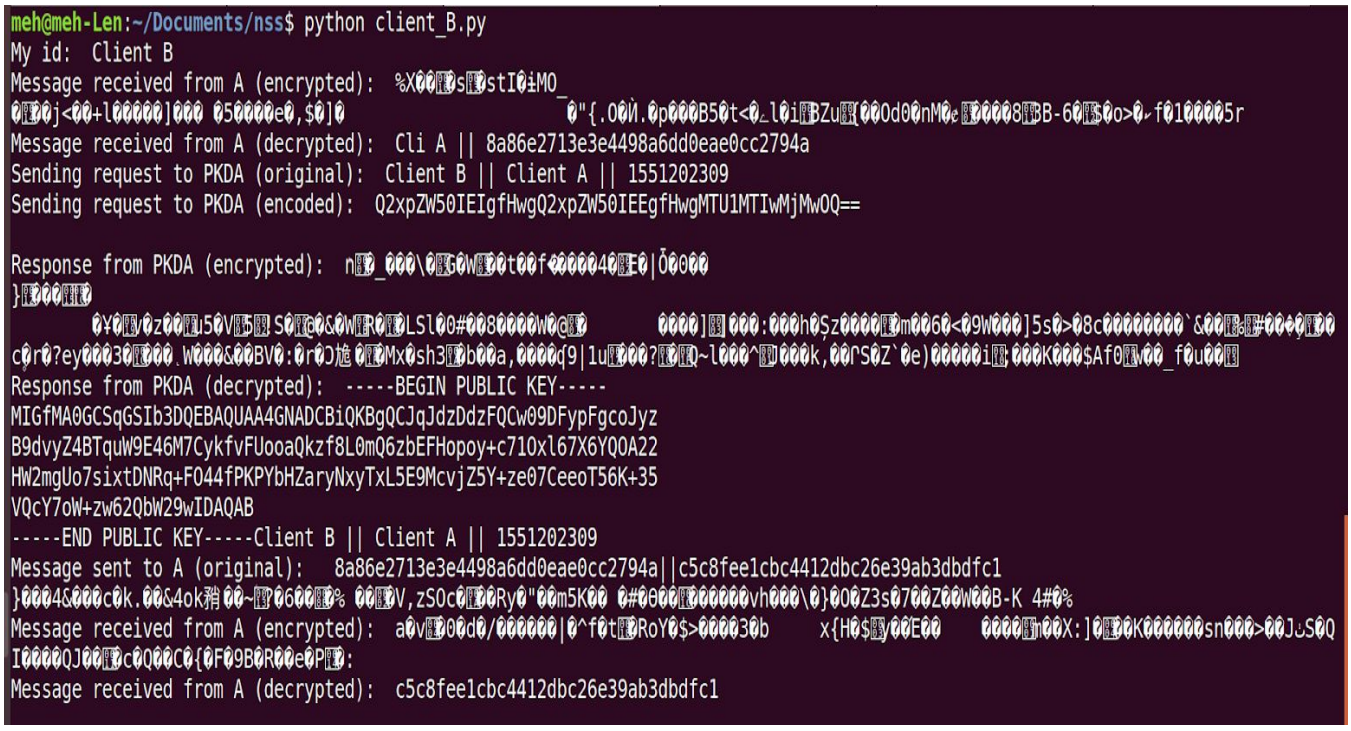
IMPLEMENTATION

1. Communication between PKDA and Client A





2. Communication between Server and Client B



3. Communication between Client A and Client B