Assignment 3

Network security
Hritik Goel (2018148)
Dushyant Panchal (2018033)
Project #1: Public Key Distribution Authority (PKDA)

DESCRIPTION:

- A,B and PKDA have their own {private key, public key} taken in code.
- A and B know the PU of PKDA.
- A and B receive the PU of each other from PKDA.
- After receiving the PU of each other, A sends 3 messages {Hi1, Hi2, Hi3} to B.
- {Got-it1, Got-it2, Got-it3} is received by A from B as a reply.

MODULES:

Class RSA

- encrypt
- decrypt
- rsa_core_operation : efficiently calculates “m^x (mod n)”
- Some utility functions
    - rsa_encode_string : encodes a string as tuple(int)
    - rsa_decode_string : decodes a tuple(int) to string

Note: Supported strings may only contain a-z and 0-9. Special characters are ignored.

Class PKDA

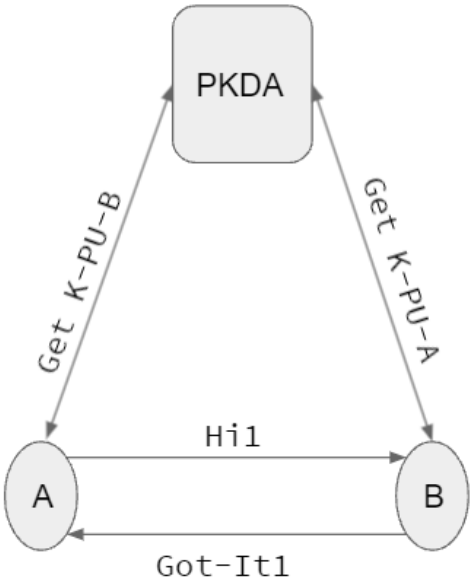
- process_message_from_client
- simulates processing a client request for public key of another client.
- nonce_response : performs nonce operation.
- generate_timestamp

Class Client

- gen_message_for_pkda : simulate sending msg to request for public key
- process_message_from_pkda : simulate processing response from pkda
- gen_message_for_client : simulate sending msg to another client
- process_message_from_client : simulate processing message from client

- Similar to PKDA
    - nonce_generate
    - nonce_response
    - generate_timestamp

SIMULATION



Following Key-Pairs were used.

- PKDA:
    - PU: (37,119)
    - PR: (13,119)

- :A
    - PU: (29,91)
    - PR: (5,91)

- B:
    - PU: (17,91)
    - PR: (17,91)

OUTPUT

```
PS C:\Users\Dushyant-PC\Desktop\NS_A3> python .\A3_Dushyant_2018033_code.py
(17, 91, 2, 76, 7)
(29, 91, 1, 76, 82)
13 53 1 hi1
13 20 1 hi2
13 65 1 hi3
(13, 54, 2, 'gotit1')
(13, 21, 2, 'gotit2')
(13, 66, 2, 'gotit3')
```