**Report**

**Programming Based Project -2**

**Integration of Instant Messenger with RSA**

****

**Pavan Kumar Revanuru**

**01578776**

**4/20/2016**

**RSA Implementation:**

RSA is the name given after the three scientists: Rivest-Shamir-Adleman

The algorithm works in the following way:

* Two primes p , q are chosen such that p ≠ q
* n is calculated by the formula n = (p)\*(q)
* phi is calculated as phi = (p-1)\*(q-1)
* e is chosen such that e and phi are co-primes, i.e. both should not have any common factors other than 1
* Calculate d is such a way that [e\*d] mod (phi) = 1

As the values of p, q, n, e and d are obtained, the encryption part is described below.

* The input that is entered with the help of raw\_input command is taken character by character.
* First the string is converted into the ASCII with the help of ord() function.
* The ASCII value is raised to the power of e and mod with n
* This is the encrypted Cipher Text.
* The encrypted cipher text is sent with the help of sendto command.

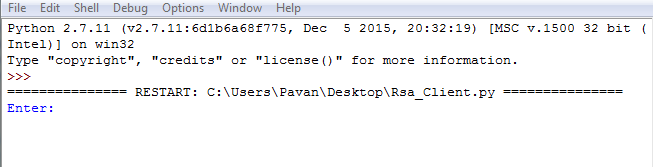
The decryption part is described as follows:

* The receiver receives the encrypted cipher text.
* Length of the cipher text is calculated with the help of len() function.
* The output of this is divided by 4 to get the number of characters.
* A for loop is executed for the times as many characters.
* Inside the for loop, the string is parsed for the initial 4 digits to the cipher of first character.
* The first 4 characters are raised to the power of d and mod with n.
* It is converted back to string with the help of chr() function.
* The loop is executed once again with next 4 digits.
* This happens for all the characters.
* The characters are concatenated and displayed.

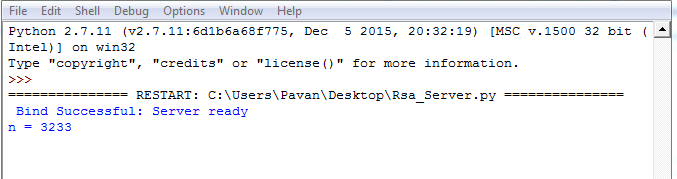
As this is an instant messenger, the connection has to be continued. Instant messaging (IM) is a type of online chat which offers real-time text transmission over the Internet. A LAN messenger operates in a similar way over a local area network. Short messages are typically transmitted bi-directionally between two parties, when each user chooses to complete a thought and select "send". Some IM applications can use push technology to provide real-time text, which transmits messages character by character, as they are composed. More advanced instant messaging can add file transfer, clickable hyperlinks, Voice over IP, or video chat.

**Screenshots:**

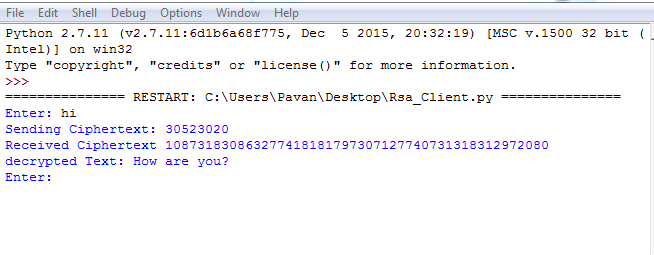
Client part: Initializing part



Server part: Initializing part



Client part: After encryption and decryption



Server part: After encryption and decryption

