Andre Kwok

Takuya Yamashita

Approach:

1. First creates the RSA public key and c and sends to the server.

2. Upon receiving those keys, the server brute force cracking the private key.

3. The server prints the message using the private key.

4. The client keeps sending requests until it finishes on its own.

5. The server never gets shut down by the client, but rather shuts it down on its own.

Protocol:

The client first sends the request as follows:

Public: 451 c: 2623

The next time the client sends the request in a following format:

1184 2123 4124 124 1241

Structures

Client

1. Ask the public key and c from the user.

2. Open the socket using the already open port

3. Write the request that conforms with the protocol into the socket

4. After that, encrypt messages using the RSA encryption and send the request to the server

5. Keep sending until quit is typed.

6. Close the socket.

Server

1. Connect to the socket.

2. Spawn a thread to listen to the client request.

3. Receive the public key and c. Then get the private key using a brute force algorithm

4. Print the cracked message on a console.

5. Type quit to exit

Code

Nothing special to mark. Please look at our source code.

Program Usage

1. Run the server.java

2. Run the client.java

3. Type the public key and c for the client.

4. Type messages for the client.

5. Type quit to exit from the client.

6. Type quit in the server to exit from the server.

Sample Run

**Client Console**

Please enter a public key:

451

Please enter c:

2623

Sending string: Public: 451 C: 2623

Please type the string: (type quit to exit)

Hello!

Please type the string: (type quit to exit)

You are my buddy

Please type the string: (type quit to exit)

12/31/2012

Please type the string: (type quit to exit)

quit

**Server Console**

Received string: 'Public: 451 C: 2623'

The generated Private key: 1531

Received string: '1148 326 1145 1145 1780 2041 '

Decoding message:

Hello!

Finished Decoding

Received string: '33 1780 2618 1249 1073 2082 326 1249 719 1036 1249 1854 2618 1991 1991 1036 '

Decoding message:

You are my buddy

Finished Decoding

Received string: '49 2329 1999 254 49 1999 2329 2427 49 2329 '

Decoding message:

12/31/2012

Finished Decoding

quit

Server is exiting