Secure Facebook API – Project 4, Part 2

Project : Facebook API
Implementations : Encryption of User Data
Implemented by : Rakesh Dammalapati [UFID: 29938403]
Tarun Gupta Akirala [UFID: 43394921]

What is working?

Successful encryption/decryption of user data using AES algorithm. Further the AES key in encrypted/decrypted using RSA Public/Private key pair. These are the features implemented in part 2, along with the features in part 1 (part 1 readme included)

Implementation?

Encryption methods used: AES, RSA

* 128 bit AES key to encrypt/decrypt the data.
* Three types of data will be encrypted:

1) Profile Information: Each profile is encrypted/decrypted with an AES key generated using secret key sent by the user.

2) Post Information: Each post is encrypted/decrypted with an AES key generated using random secret key generator.

3) Photo Information: Each photo is encrypted/decrypted with an AES key generated using random secret key generator.

* 1024bit public/private RSA key
* AES key is encrypted using RSA algorithm.

Flow?

A user encrypts the data using AES key and sends it to the server. The user(sender) then chooses the list of users(receivers) with whom he chooses to share. The sender then sends the AES key encrypted with the public key of the receiver. The receiver on receiving the encrypted AES key decrypts it with his private key and uses the decrypted AES key to decrypt the sender data.