Project Title

Implementation of Secure Web Communication

Group Members

Name	Student ID
Yiu Kam Wing	20028987D
Tsz Hin LO	18050658D
Hong Jiseok	15100845D

Introduction:

Secure communication is one of the biggest security problems nowadays. Because a lot of sensitive data is transmitted on the internet now. Therefore, our team decided to dig into this security problem and implement a secure web chat application that ensures the confidentiality of the user message.

Objectives:

- Implementation of storing the global information in the web server such as users' public keys and server’ public key.
- Implementation of modified Diffie-Hellman Cryptosystem
- Implementation of ElGamal Cryptosystem

Application Features and Description:

- Login and Register
- Secure communication between two parties
- Modified Diffie-Hellman Cryptosystem:
    - global information in the web server: prime q , primitive root a, users' public keys, hash function h, encrypt function E and decrypt function D
    - Alice send $E_{server'puk}(E_{b'puk}(Y_a,E_{a'prk}(h(Y_a))),"Alice","Bob")$ to server
    - Then server send $E_{server'prk}(E_{b'puk}(Y_a,E_{a'prk}(h(Y_a))),"Alice","Bob")$ to Bob
    - Then Bob send $E_{server'puk}(E_{a'puk}(Y_b,E_{b'prk}(h(Y_b))),"Bob","Alice")$ to server
    - Then server send $E_{server'prk}(E_{a'puk}(Y_b,E_{b'prk}(h(Y_b))),"Bob","Alice")$ to Alice
    - Then Alice and Bob can use a $K = (Y_b)^{(X_a)} = (Y_a)^{(X_b)}$ to communicate with each other.