Bharatiya Vidya Bhavan's

SARDAR PATEL INSTITUTE OF TECHNOLOGY

(Autonomous Institute Affiliated to University of Mumbai)
Munshi Nagar, Andheri (W), Mumbai – 400 058.

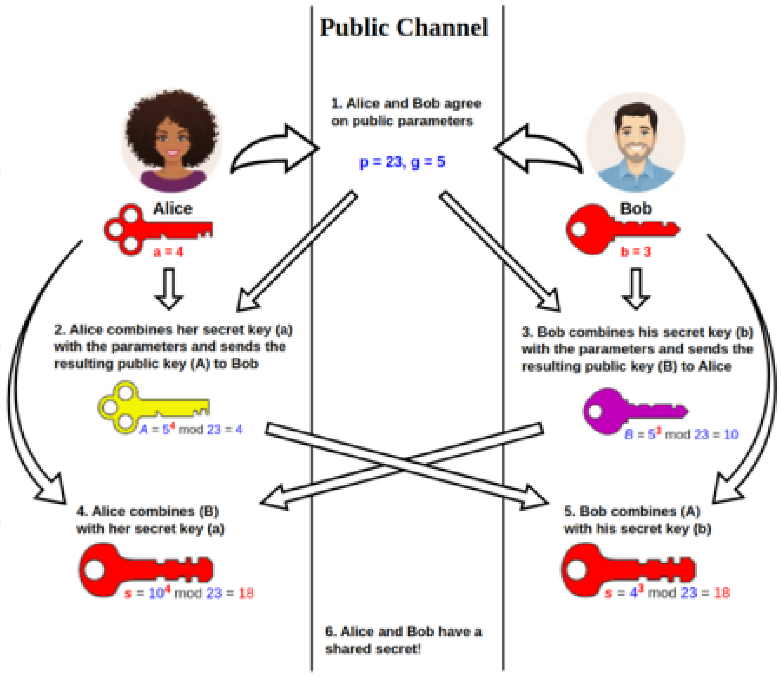
Experiment No. 4

Aim –Implement Diffie-Hellman algorithm.

Problem Definition– The experiment uses key exchange algorithm namely *Diffie-Hellman* and symmetric cryptosystem to provide two security services. In the first part, the experiment covers key distribution problem using *Diffie-Hellman key exchange algorithm*. This allows sharing secret key between sender and receiver without using any third party entity. In the second part, symmetric cryptosystem covers sending large message from the sender to the receiver using the secret key shared in the first step.

Theory –

Diffie-Hellman algorithm allows to establishing a shared secret that can be used for secret communications by exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters. It uses 4 variables, one prime ***p*** and ***g*** (a primitive root of P) and two private values ***a*** and ***b***. The prime number ***p*** and ***g*** are both publicly available numbers. Users (say Alice and Bob) pick private values ***a*** and ***b*** and they generate a key and exchange it publicly. The receiver person receives the key and that generates a secret key, after which they have the same secret key to encrypt.


Public Channel
Alice
a = 4
1. Alice and Bob agree on public parameters
p = 23, g = 5
Bob
b = 3
2. Alice combines her secret key (a) with the parameters and sends the resulting public key (A) to Bob
A = 5^4 mod 23 = 4
3. Bob combines his secret key (b) with the parameters and sends the resulting public key (B) to Alice
B = 5^3 mod 23 = 10
4. Alice combines (B) with her secret key (a)
s = 10^4 mod 23 = 18
5. Bob combines (A) with his secret key (b)
s = 4^3 mod 23 = 18
6. Alice and Bob have a shared secret!

Useful Links–Cryptography Basics - Diffie-Hellman Key Exchange https://www.youtube.com/watch?v=d1KXDGgwIpA

Details of Experimentation – You need to implement two parts in this experiment. The first part allows exchange of secret key using Diffie-Hellman algorithm and second part actual sending a message of at least 1000 letters from the sender to the receiver. The sender and receiver needs to be implemented as network services using socket programming. e.g. Receiver service on port no 3333. The sender and receiver should have menu driven options as follows:

Sender socket program should provide three options (through infinite menu) namely i) Generation of key using Diffie-Hellman algorithm, ii) Send a message to the receiver using any symmetric cryptosystem. iii) The third menu driven option is exiting from the sender program/service.

Receiver socket program should be continuous waiting for two services: i) A request for generation of secret key using Diffie-Hellman algorithm, ii) Receiver should continuously waiting receiving encrypted message which is already shared in the first option. The receiving of message is performed through any symmetric cryptosystem agreed with the sender. iii) The third menu driven option is exiting from the sender program/service.

Input – The input for this experiment is i) Key Generation, P, G, a and b and ii) Large input message of more than 1000 letters. Note you need to use some mapping to convert letter to number and vice versa. Further, you may assume any other data required for this experimentation.

Output and Submission –

1) Source code of all three entities. All these files should be in one folder named "source-codes-<your UID>"
2) All the communication input, output, keys etc in a TEXT file [NO word file] named "input-output-<your UID>"
3) Upload above mentioned Part-1 and Part-2 as zipped file named "Exp4-<your UID>"