FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING
Department of Computer Engineering

Course , Subject & Experiment Details

Academic Year	2018-19	Estimated Time	02 - Hours
Course & Semester	T.E. (CMPN)- Sem VI	Subject Name & Code	CSS - (CSL604)
Module No.	02 – Mapped to CO-2	Chapter Title	Key Management Techniques

Practical No:	2
Title:	Implementation of Diffie- Hellman Key exchange algorithm and Simulation of Man In the Middle attack
Date of Performance:	
Date of Submission:	
Roll No:	
Name of the Student:	

Evaluation:

Sr. No	Rubric	Grade
1	On time submission Or completion (2)	
2	Preparedness(2)	
3	Skill (4)	
4	Output (2)	

Signature of the Teacher:

Date:

MNS

Title: Implementation of Diffie- Hellman Key exchange algorithm and Simulation of Man In the Middle attack.

Lab Objective :

This lab provides insight into:

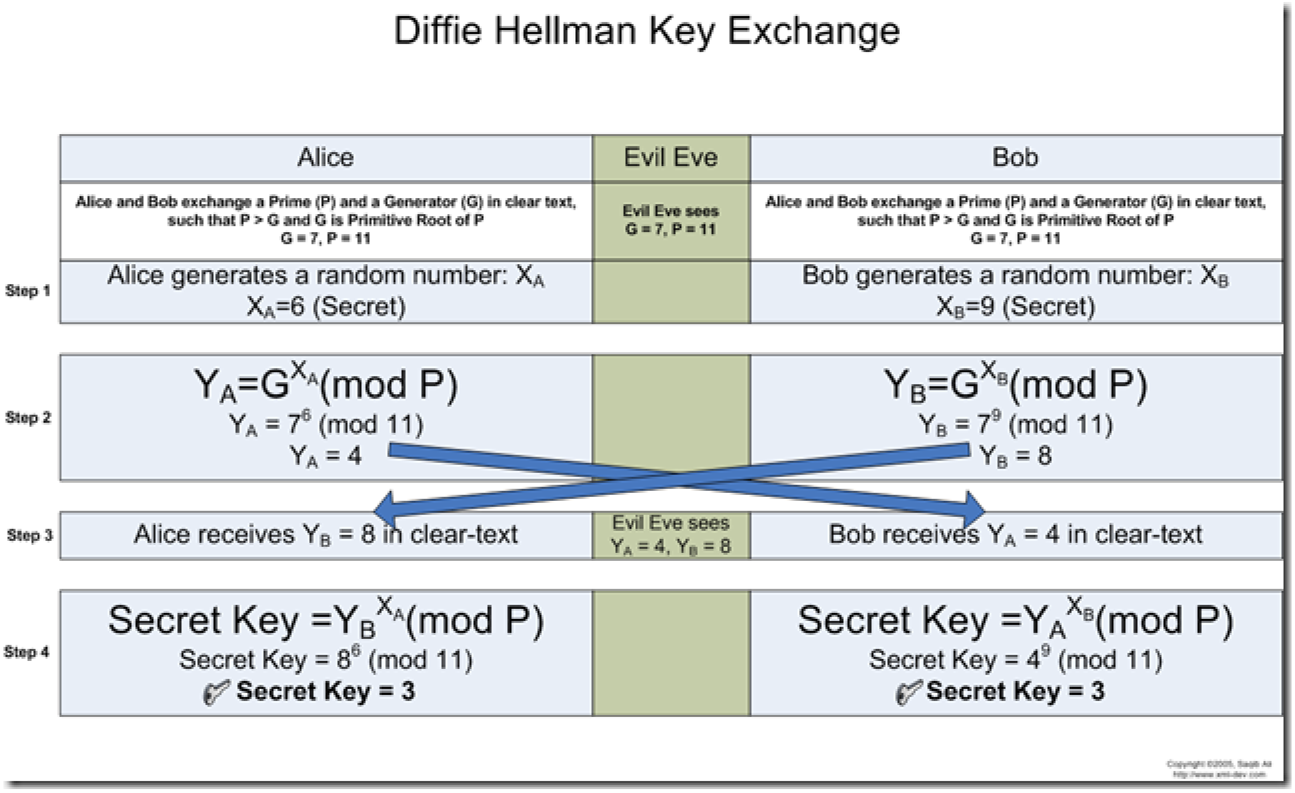
- The working of Diffie – Hellman Key Exchange Protocol.

Reference : “Cryptography and Network Security” B. A. Forouzan
“Cryptography and Network Security” Atul Kahate

Prerequisite: Any programming Language and Knowledge of Symmetric Key cryptography.

Theory:

Diffie-Hellman is a way of *generating* a shared secret between two people in such a way that the secret can't be seen by observing the communication.
This is particularly useful because you can use this technique to create an encryption key with someone, and then start encrypting your traffic with that key. And even if the traffic is recorded and later analyzed, there's absolutely no way to figure out what the key was, even though the exchanges that created it may have been visible.

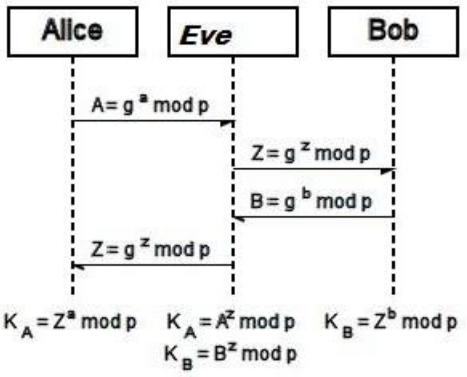


Diffie Hellman Key Exchange

	Alice	Evil Eve	Bob
	Alice and Bob exchange a Prime (P) and a Generator (G) in clear text, such that P > G and G is Primitive Root of P G = 7, P = 11	Evil Eve sees G = 7, P = 11	Alice and Bob exchange a Prime (P) and a Generator (G) in clear text, such that P > G and G is Primitive Root of P G = 7, P = 11
Step 1	Alice generates a random number: X_A X_A=6 (Secret)		Bob generates a random number: X_B X_B=9 (Secret)
Step 2	$Y_A=G^{X_A}(\text{mod } P)$ $Y_A = 7^6 \text{ (mod 11)}$ $Y_A = 4$		$Y_B=G^{X_B}(\text{mod } P)$ $Y_B = 7^9 \text{ (mod 11)}$ $Y_B = 8$
Step 3	Alice receives $Y_B = 8$ in clear-text	Evil Eve sees $Y_A = 4, Y_B = 8$	Bob receives $Y_A = 4$ in clear-text
Step 4	Secret Key $=Y_B^{X_A}(\text{mod } P)$ Secret Key $= 8^6$ (mod 11) **Secret Key = 3**		Secret Key $=Y_A^{X_B}(\text{mod } P)$ Secret Key $= 4^9$ (mod 11) **Secret Key = 3**

Man – In – The –Middle Attack

Let us take the example illustrated by Diffie-Hellman to discuss the Man-in-the-Middle Attack. Let us that Eve is in the middle of Alice and Bob. Eve does not need the value of x or y to attack the protocol. She can fool both Alice and Bob by the following process.



1. Alice choose a, calculate A=g^a mod p
2. Eve, the intruder, interpret A, she chooses z, calculate Z=g^z mod p, and sends Z to both Alice and Bob.
3. Bob choose b, calculate B=g^b mod p, and sends B to Alice; B is interpreted by Eve and never reaches Alice.
4. Alice and Eve calculate the same key g^az mod p, which become a shared key between Alice and Eve. Alice however think that it is a key shared between Bob and herself.
5. Eve and Bob calculate the same key g^bz mod p, which become a shared key between Eve and Bob. Bob, however, thinks that it is a key shared between Alice and himself.

This situation is called man-in-the-middle attack.

Practical and Real Time Applications

- Used as a method of exchanging cryptography keys for **use** in symmetric encryption algorithms like AES
- Public key encryption schemes based on DF – ElGamal encryption
- Password-authenticated key agreement
- public key infrastructure - It is possible to use DF as part of PKI

Conclusion:

The program was tested for different sets of inputs.
Program is working SATISFACTORY NOT SATISFACTORY
(Tick appropriate outcome)

Post Lab Assignment:

1. In the Diffie- Hellman protocol , what happens if x and y have the same value, that is, Alice and Bob have accidentally chosen the same number? Are A and B (values exchanged by Alice and Bob to each other) the same? Do the session keys calculated by Alice and Bob have the same value? Use an example to prove your claims.
2. How to secure Diffie-Hellman from Man-in –the –Middle attack?