|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Hope Foundation’s,**  **Finolex Academy of Management and Technology, Ratnagiri** | | | | | | | | | |
| **Department of Information Technology** | | | | | | | | | |
| Subject name: SECURITY LAB | | | | | | | | Subject Code: ITL502 | | | |
| Class | | TE IT | | Semester – V (CBCGS) | | | | Academic year: 2018-19 | | | |
| Name of Student | |  | | | | | **QUIZ Score :** | | | | |
| Roll No | |  | | | Experiment No. | | | | | 03 | |
| Title**:**  **Implementation of Diffie Hellman Key exchange algorithm.** | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. **Course objectives applicable:**   **LOB2**. To be able to analyze and implement Diffie Hellman Key exchange | | | | | | | | | | | |
| 1. **Course outcomes applicable:**   **LO2.** Analyze and implement public key algorithms Diffie Hellman Key exchange | | | | | | | | | | | |
| **3. Learning Objectives:**   * To understand the security factors with respect to the fact that solving the discrete algorithm is very challenging. * To understand that the shared key (i.e. the secret) is never itself transmitted over the channel. | | | | | | | | | | | |
| **Practical applications of the assignment/experiment:**  SSL/TLS is composed of two layers: the lower layer called the Record Protocol rides on TCP  and manages the symmetric (private) cryptography so the communication is private and reliable. The upper layer is called the Handshake Protocol and is responsible for authentication of the parties and negotiation of encryption methods and keys. It is in this layer that Diffie Hellman Key exchange can be used. | | | | | | | | | | | |
| **Prerequisites**:  The mathematical properties to produce a common computational result between two (or more) parties wishing to exchange information, without any of them providing all the necessary variables. By agreeing on two variables and providing each other with a computed public key, the resulting secret key will be identical throughout the exchange. | | | | | | | | | | | |
| **6. Hardware Requirements**:   1. PC with 4GB RAM, 500GB HDD.   **7. Software Requirements:**  1. Programming language C, C++, Java, Python | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **8. Quiz Questions (if any): (Online Exam will be taken separately batchwise, attach the certificate/ Marks obtained)**   1. How can two parties agree on a secret value when all of their messages might be overheard by an eavesdropper? 2. What’s the difference between Diffie-Hellman and RSA? | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **9. Experiment/Assignment Evaluation:** | | | | | | | | | | | |
| **Sr. No.** | **Parameters** | | | | | | | | **Marks obtained** | | **Out of** |
| **1** | Technical Understanding (Assessment may be done based on Q & A **or** any other relevant method.) Teacher should mention the other method used - | | | | | | | |  | | 6 |
| **2** | Neatness/presentation | | | | | | | |  | | 2 |
| **3** | Punctuality | | | | | | | |  | | 2 |
| **Date of performance (DOP)** | | |  | | | **Total marks obtained** | | |  | | **10** |
| **Date of checking (DOC)** | | |  | | | **Signature of teacher** | | | | | |

**Results:**

**SOURCE CODE:**

#Diffie Hellman Algorithm

p=(int)(input("User A: Enter a prime number\n"))

g=(int)(input("User B: Enter a prime number\n"))

x=(int)(input("User A: Enter a random number\n"))

y=(int)(input("User B: Enter a random number\n"))

r1=(pow(g,x))%p

r2=(pow(g,y))%p

k1=(pow(r2,x))%p

k2=(pow(r1,y))%p

if k1==k2:

print("Successfully implemented Diffie Hellman Algorithm\n")

print("K=",k1)

else:

print("Better luck next time")

**OUTPUT:**

User A: Enter a prime number

23

User B: Enter a prime number

7

User A: Enter a random number

3

User B: Enter a random number

6

Successfully implemented Diffie Hellman Algorithm

('K=', 18)

**References** :

[1] Burnett, S. and Paine, S. (2001) RSA Security’s Official Guide to Cryptography. McGraw-Hill.

[2] Carts, D.A. (2001) A Review of the Diffie-Hellman Algorithm and its Use in Secure Internet Protocols. [Online] Available at http://www.sans.org/reading\_room/whitepapers/vpns/review-diffie-hellman-algorithm-secure-internet-protocols\_751 [Accessed 25 October 2012].

[3] EMC Corporation (2012) “What Is Diffie-Hellman?”, RSA Laboratories [Online] Available at http://www.rsa.com/rsalabs/node.asp?id=2248 [Accessed 26 October 2012].