

INTRODUCTION TO CRYPTOGRAPHY – LAB 4

B.Tech. Computer Science and Engineering (Cybersecurity)

Name: Anish Sudhan Nair	Roll No.: K041
Batch: K2/A2	Date of performance: 02/02/2022

Aim: To code the Diffie-Hellman algorithm for public-private key encryption

Code:

Language: C

Editor: Atom

Compiler: clang/ZSH

Note: Due to memory allocation issues in C, a small integer is input for Bob's and Alice's numbers

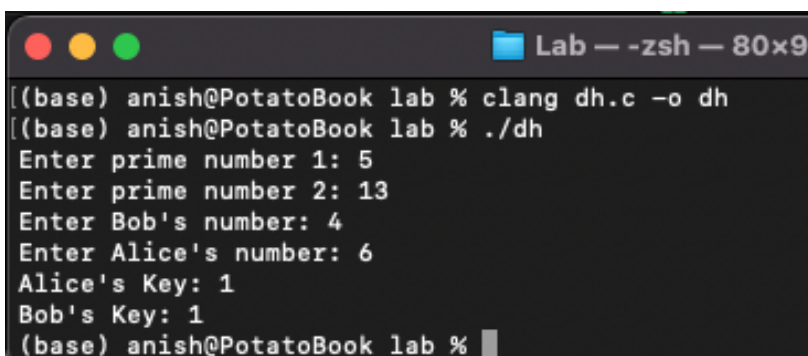
```
1  #include <stdio.h>
2  #include <stdbool.h>
3  #include <math.h>
4
5  bool ifPrime(int n){
6
7      int count=0;
8
9      for (int i = 1; i < n; i++) {
10         if (n%i==0) {
11             count++;
12         }
13     }
14
15     if (count>1) {
16         return false;
17     }
18
19     return true;
20 }
21
22 int modValue(int n, int g, int x){
23
24     int value;
25
26     value = pow(g,x);
27     value=value%n;
28
29     return value;
30 }
31
32 int keyGenerator(int x, int b, int n){
33
34     int keyValue;
35
36     keyValue = pow(b,x);
37     keyValue=keyValue%n;
38
39     return keyValue;
40 }
41
42 int main() {
43
44     int prime_number_1, prime_number_2, bob_number, alice_number, valueA, valueB, keyAlice, keyBob;
45 }
```

```

46     do {
47         printf("Enter prime number 1: ");
48         scanf("%d",&prime_number_1);
49
50         if (!ifPrime(prime_number_1)) {
51             printf("\nNot a prime number!\n");
52         }
53     } while(!ifPrime(prime_number_1));
54
55
56     do {
57         printf("Enter prime number 2: ");
58         scanf("%d",&prime_number_2);
59
60         if (!ifPrime(prime_number_2)) {
61             printf("\nNot a prime number!\n");
62         }
63     } while(!ifPrime(prime_number_2));
64
65     printf("Enter Bob's number: ");
66     scanf("%d",&bob_number);
67
68     printf("Enter Alice's number: ");
69     scanf("%d",&alice_number);
70
71     valueA=modValue(prime_number_1, prime_number_2, alice_number);
72     valueB=modValue(prime_number_1, prime_number_2, bob_number);
73
74     keyAlice=keyGenerator(alice_number, valueB, prime_number_1);
75     keyBob=keyGenerator(bob_number, valueA, prime_number_1);
76
77     printf("Alice's Key: %d\n",keyAlice );
78     printf("Bob's Key: %d\n",keyBob );
79
80     return 0;
81 }
82

```

Complete Output:



```

Lab - -zsh - 80x9
[(base) anish@PotatoBook lab % clang dh.c -o dh
[(base) anish@PotatoBook lab % ./dh
Enter prime number 1: 5
Enter prime number 2: 13
Enter Bob's number: 4
Enter Alice's number: 6
Alice's Key: 1
Bob's Key: 1
(base) anish@PotatoBook lab %

```

Questions:

1. Explain DH key exchange algorithm.

The Diffie-Hellman key exchange algorithm enables encrypted communication over an unsafe channel by using a public key.

Consider two user Anish and Hasin, who wish to communicate over a channel. In DH algorithm, each user would have a private key generated for them that is not disclosed to anyone. Using the private key and publicly informed prime numbers they each generate a key which they then share with each other. Using this shared key, their private key and the prime numbers, they generate the symmetric key which is used for encrypting and decrypting their messages.

2. List some of the protocols where DH algorithm is used.

- Secure Shell (SSH) [More secure than Telnet]
- Internet Protocol Security (IPSec)
- Transport Layer Security (TLS)

3. List advantages and disadvantages of DH algorithm.

Advantages:

- It provides a symmetric key which enables communication in insecure channels
- Due to the symmetric key exchange the users need not necessarily know each other
- The keys are generated using large numbers and so manually cracking them is quite exhaustive

Disadvantages:

- It can only be used for symmetric key exchange
- It is very resource exhaustive (computational power)
- The algorithm itself does not perform the encryption
- There is no authentication process involved opening vulnerabilities for Man in the Middle Attacks