Ganpat University
॥ विद्यया समाजोत्कर्षः ॥
Institute of Computer Technology

Name: Tushar Panchal

En.No: 21162101014

Sub: INS (INFORMATION SECURITY)

Branch: CBA

Batch:61

----------PRACTICAL 08----------

❖ AIM :

For encryption purpose two parties Alice and Bob want to share some secrete key over a communication network, Which Key Exchange algorithm is best suited for this scenario. Prepare suitable environment for the same.

✓ Source Code :

```
import random

prime_number = int(input('Enter any prime number: '))
alpha = []
l1 = []

def check(values, prime):
    for i in range(1, prime):
        if i in values:
            continue
        else:
            return False

for i in range(2, prime_number):
    for j in range(1, prime_number):
        val = (i**j) % prime_number
        l1.append(val)
    alpha.append(l1)
    l1 = []
```

```
final_alpha = []
for i in range(len(alpha)):
    if check(alpha[i], prime_number) != False:
        final_alpha.append(alpha.index(alpha[i]) + 2)

if not final_alpha:
    print("No suitable alpha value found. Please try again with a different prime
number.")
    exit()

selected_alpha = min(final_alpha)
if selected_alpha == 2:
    final_alpha.remove(2)
    selected_alpha = min(final_alpha)

a = random.randint(1, prime_number)
b = random.randint(1, prime_number)
while a == b:
    b = random.randint(1, prime_number)

public_A = (selected_alpha**a) % prime_number
public_B = (selected_alpha**b) % prime_number

c = a * b
key_a = (selected_alpha**c) % prime_number
key_b = (selected_alpha**c) % prime_number

print(f'Selected value for alpha: {selected_alpha}')
print(f'Public_A: {public_A}')
print(f'Public_B: {public_B}')
print(f'Selected key of Sender Side: {key_a}')
print(f'Selected key of Receiver Side: {key_b}')

if key_a == key_b:
    print('Key Matched. Exchange of key was successful')
else:
    print('Key Not Matched. Exchange of key was unsuccessful')
```

✓ **Output :**

```
>_ pwsh 8 8ms
>> python -u "c:\Users\Tushar\Documents\SEM 6\INS\CODES\8\8.py"
Enter any prime number: 23
Selected value for alpha: 5
Public_A: 6
Public_B: 7
Selected key of Sender Side: 18
Selected key of Receiver Side: 18
Key Matched. Exchange of key was successful
>_ pwsh 8 1s 556ms
>>
```