	Experiment 6 Sharhwal Shah
)	6000U22012C
-11	Tybtech (omps &
	Aim: Design and implement Diffie Kellman Key Exchange Algorithm.
	in the state of the solding on the state of
	Theory! The diffie - hellman algorithm is being used to establish
	a Shared secret that can be used for secret
	communications while exchanging data over a public
100	network vin the elliptical curve to generate points
5	and get the socret key using the parameters.
	For the sake of symplicity and practical implementation
	of the algorithm we will consider only hvariables only
	prime P and G (a primitue root of P) and two
	potrate values a and b.
7	in the sale of the sale of the sale of the sale of
	Pand a one both publically available numbers, vous
1	b and they generate a key and exchange it
	publically. The opposite person receives the key and
	that generates a secret key often which they have
	the same secret key to enerypt.
-	Alice and Bob get public numbers 1=23 and G=9
-	Alice selected a potrate key - a=4
	Bob selected a private key - b = 3
aram [®]	FOR EDUCATIONAL USE

1.	> Alice and Bob compute public values
	Alice - x= (9° mod 23) = 6561 mod 23 = 6
	y = (93 mod 23) = 729 mod 23 = 16
Y	-> Alice and Bob exchange public numbers.
	5 AL
	Alice receives public Rey = y = 16 and
10 %	Bob recenes public key x - 6
2800	
, V.	THE are son compare symmetric regg
3 60	Alice: ka = ya mod p = 65536 mod 2329
	Bob : kb = dix mod p = 216 mod 23 = 9
	D 9 15 the Stephen
vila :	-> 9 is the shoot secret
	The property of the second of the second of the second of
51.	Conclusion! Even while using cipher for encuptor it is
	'is sewe and yet available to the sender and receiver.
11	we learnt about the algorithm and implement it in
)	Python.
	the decidence of the control of the
	The state of the s
	is the continuity which there and have make
	the same of the sa
	A Company of the second
aram)	FOR EDUCATION AND
	FOR EDUCATIONAL USE



NAAC Accredited with "A" Grade (CGPA: 3.18)

Academic Year: 2022-2023

EXPERIMENT 6

Shashwat Shah TYBtech Comps B C22 60004220126

AIM: Study and Implement Diffie Hellman Key Exchange Algorithm.

CODE:

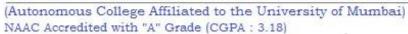
```
from random import randint
P = 17
Q = 3
print('The Value of P is :%d'%(P))
print('The Value of Q is :%d'%(Q))
# Alice will choose the private key a
a = 4
print('The Private Key a for Alice is :%d'%(a))
# gets the generated key
x = int(pow(Q,a,P))
# Bob will choose the private key b
b = 3
print('The Private Key b for Bob is :%d'%(b))
# gets the generated key
y = int(pow(Q,b,P))
# Secret key for Alice
Alice_key = int(pow(y,a,P))
# Secret key for Bob
Bob_key = int(pow(x,b,P))
print('Secret key for the Alice is : %d'%(Alice_key))
print('Secret Key for the Bob is : %d'%(Bob_key))
```

• • •



Shri Vile Parle Kelavani Mandal's

DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING





Academic Year: 2022-2023

OUTPUT:

```
uments/BTech/Docs/6th Sem/IS/Code/Exp6/Diffie-Hellman.py"
The Value of P is :17
The Value of Q is :3
The Private Key a for Alice is :4
The Private Key b for Bob is :3
Secret key for the Alice is : 4
Secret Key for the Bob is : 4
PS C:\Users\Jadhav\Documents\BTech\Docs\6th Sem\IS\Code>
```