

Assignment B3

Submission Pat: 19/05/2021

Submission Pute: 21/05/2021

Aitle: Pithe - Hellman Key exchange

Problem Stutement:

10 implement Dithe - Hellman Key exchange

Objective:
- Understand bosic concepts of dishe hellman key exchange

- Understand bosic concepts of chance hellman rey exercise

- Logical implementation, of algorithm:

Outrome: Students will be understand and implement Diffie. Hellman

Key exchange

Software Requirements:

- Jupytir Nottbook

- Rymon 3.8-5

- 64 bit operating system.

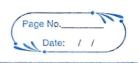
- Computer with 64 bit processor

Mordware Requirements:

· '59.87



Theory: The pithe Hellman algorithm was widely known as Key exchange algorithm or key agreement algorithm developed by Whitfield Pithe and Murtin Hellman. Diffie Hellman algorithm is wed to generate some (symmetric) private cryptographic key at the sender as well as receiver end so mot there is no need to transfer this kay from sender to seceiver. Remember, This algorithm is wed only for key agreement not for decryption or encryption of messages. If sender and seceiser went to communicate with each other, they agree on the same key generated by algorithm laker on they can use this key for encryption or decryption. Algorithm: i) Sender and receiver gets public numbers q & «. Both select private keys 'a' and 'b'. 3) Following values are computed. x=del mod g y = Xb mod g



4) Both wers exchange or and y.

5) Following computations are performed to calculate symmetric key.

Ka = y a mod q

 $Rb = x^b \mod g$

Ma=Kb

Example: i) Let g=23 and d=9

2) let a=4 and b=3

3) 22 94 mod 23 = 6

y = 93 mod 23 = 16

4) Exchange x and y

5) Ka = ya mod q = 164 mod 23 = 9

: Secret Key is 9.



lest coses:

	quality and control of the control o		
	Description	Expected OIP	Actual OIP
)	test algorithm with	Both secret keys are	Successful
	random numbers	equal	
2)	Test algorithm with	Both secret keys: 9	Successful
	above example.	J	
	,		
	Conclusion:		

therefore, we have successfully implemented Dithe hellman key exchange algorithm.