Classmate

Name: Tejas Redkar

PRN: 1032210937

Panel: C

ROLLNO: PC-44

## ICS Lab A6

FAQUS

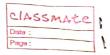
What is Diffie - Hellman key exchange? Diyfie Hellman key exchange is a coupto graphic purotocal that allows two parties to isecurely exchange cryptographic keys and over an insecure communication channel. It enables them to agree upon a shaved servet key without

needing to Turansmit the key itself.

What is Diffie-Hellman most commonly used you? Diffie-Hellman is most commonly used forestablishing secure communication channel in various applications usuch as securing internet connections, VPNs, & encompted messaging. It is a fundamental component of many encryption purotocols & ensures the confidentiality of data treansmitted over a network.

13 Diffie - Hellman wymmeteric

No, Diffie-Hellman is not exymmetric, its an asymmetric comprophy purotoscol.



	Page:
<b>Q</b> 4)	Is Diffie- Hellman secure d'atillused?
Ans	Diffie- Helman can be secure when implemented
	peroperly with modern variants. It is satill widely used today for secure communications a enoughtion.
	used today your secure communications a enoughtion.
<u> </u>	
(6)	X \ nh
1	
-	
1 - 2 - 1 -	and the second of the second o
7 3	
Y Y Y	
idite (	
100	
, s,	