Name : Tejas Redkar
PRN: 1032210937
Panel : C
Roll No : PC-44

ICS Lab A6

* FAQ's

Q1) What is Diffie - Hellman key exchange?

Ans Diffie Hellman key exchange is a cryptographic protocol that allows two parties to securely exchange cryptographic keys ~~are~~ over an insecure communication channel. It enables them to agree upon a shared secret key without needing to transmit the key itself.

Q2) What is Diffie-Hellman most commonly used for?

Ans Diffie- Hellman is most commonly used for establishing secure communication channel in various applications such as securing internet connections, VPNs, & encrypted messaging. It is a fundamental component of many encryption protocols & ensures the confidentiality of data transmitted over a network.

Q3) Is Diffie - Hellman symmeteric

Ans No, Diffie-Hellman is not symmeteric, its an asymmetric cryptography protocol.

Q4) Is Diffie- Hellman secure & still used?

Ans Diffie- Hellman can be secure when implemented properly with modern variants. It is still widely used today for secure communications & encryption.

✓

A+

11/12/23