Devanshu Surana
PC-23, Panel C
1032210755

ICS Lab A6

A-1 Dy 30/11/23

FAQ's

1. What is Diffie-Hellman key exchange?

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

2. What is Diffie-Hellman most commonly used for?

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

3. Is Diffie-Hellman symmetric?

Ans. No, Diffie Hellman is not symmetric, its an asymm-etric cryptography protocol.

4. Is Diffie-Hellman secure and still used?

Ans. Diffie-Hellman can be secure when implemented properly with moder variants. It is still widely used today for secure communication and encryption.