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

ICS Lab A5

* FAQ's

Q1) List down some Hashing Algorithms.

Ans 1) MD-5
2) SHA-1
3) SHA-2 (224 & 256 / 384 & 512)
4) SHA-3 (224 / 256 / 384 / 512)

Q2) What is the MD5 message-digest algorithm?

Ans MD5 (Message digest Algorithm 5) is a widely used cryptographic hash function that produce a 128-bit (16 byte) hash value, typically represented as a 32-character hexadecimal number. It was designed by Ronald Rivest in 1991 & is commonly used for checksums & data integrity verification. However, MD5 is now considered insecure for cryptographic purposes due to vulnerabilities that allow for collision attacks, where different inputs can produce the same hash value. As a result, more secure hash functions like SHA-256 are recommended for cryptographic applications.

Q3 What are alternatives to MD5 Algorithm

Ans SHA-256, SHA-3, BLAKE2 are secure alternatives to the MD-5 algorithm

Q4) Difference between MD5 & SHA algorithm

Ans MD5 is less secure; SHA is more robust for integrity.