Page No.
Date

Devanshu Surana
PC-23, 10322107755
Panel C, Batch C1

ICS Lab A5

A+ 4y
30/11/23

FAQs

1. List down some hashing Algorithms.

Ans. -MD5
-SHA1
-SHA 256
-SHA-3
-whirlpool
-Blake 2
-RIPEMD-160

2. What is the MD5 message-digest algorithm?

Ans. MD5 is a widely used cryptographic hash function that produces a 128-bit (16 byte) hash value. It was designed by Ronald Rivest in 1991. and is commonly used for checksums and to check the integrity of files. MD5 is now considered cryptographically broken and unsuitable for further use due to vulnerabilities that allow for collision attacks.

3. What are Alternatives to MD5 algorithm?

Ans. -SHA 256, 384 and 512. These are part of SHA-2 family. and are considered more secure than MD5

- SHA3 The member of Secure Hash Algorithm family
- Blake 2. Cryptographic hash function Faster than MD5 and SHA 2

4. Difference Between MD5 and SHA Algorithm

Ans.

MD5	SHA
1. Message digest length is 128	- message digest leg length is 160
2. Attact to find the original message is 2^{128} operations	- Attack to Find the original message - 2^{160}
3. There have been reported attempts to compromise is security.	- No successful claims of attacks have been report so fak
4. Faster due to 64 interations and a 128-bit buffer	Slower due to 80 iteration and a 160-bit buffer.