Page No.)
Date					$\bigg)$

Devanshu Surana PC-23, 1032210755 Panel C, Batch CI

Ics Lab A5

120/11/23

FAQS

I. List down Some hashing Algorithms.

Ans.-MDS

-SHAI

-SHA 256

-SHA-3

-Whirlpool

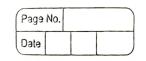
-Blake 2

-RIPEMD-160

2. What is the MDS message - digest algorithm?

Ans. MDS 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. MDS is now considered cryptographically broken and unsitiable for further use due to Vulnerabilities that allow for collision attacks.

3. What gre Alternatives to MDS algorithm?
Ans. -SHA 256, 384 and SIZ. These are part of
SHA-2 family. and are considered more Secure
than MDS



-SHA3 The member of Secure Hash Algorithm family
-Blake 2. Cryptographic hash Function
Faster than MDS and SHA2

4. Difference Between MDS and SHA Algorithm
Ans.

	MDS	SHA
	1. Message digest length	-message digest lea
	is 128	length is 160
ш		
	message is 2 2 operations	- Attack to Find the Original message - 2160
	3. There have been reported	
-11	, ,	attacks have been report
-11	is security.	so fack
- 11)	Slower due to Soiteration
-		and a 160- bit buffer
ľ		