Page No.
Class
Roll No.
Date: / /

Assignment-06

- Title :-

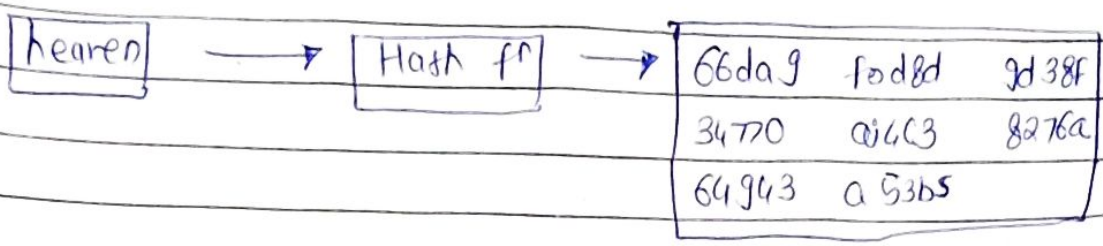
Calculate the message digest of text using SHA-I algorithm in JAVA

- Theory :-

- SHA stands for "secure hashing algorithm.
- SHA is a modified version of MD5 & used for hashing algorithm shortens input data into smaller form that can't be understood by using bitwise operations, modular additions & comparison fn.
- SHA works in which works in such a way even if a single character of message changed then it will generate a different has.
- Ex.,

hashing of two similar, but different message i.e Heaven & heaven is different.

Heaven → Hash fn → 06b73 bd7b 3b93 786da ed820 cbfa 4561b f0e8e



- SHA-1 is a cryptographic hash fn which take an input & produces a 160-bit has value.
- This hash value is known as message digest. This message digest is usually then rendered as a hexadecimal no. which is 40 digit long.
- To calculate Cryptogrphic hashing value in Java, MessageDigest class is used, under package Java.security.
- MessageDiget class of provides following cryptographic hash value of text as follows:
  - MD2
  - MD5
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
- These algo. are initialized in static method called getInstance().
- BigInteger class is used, to Convert the resultant byte array into signum representation.

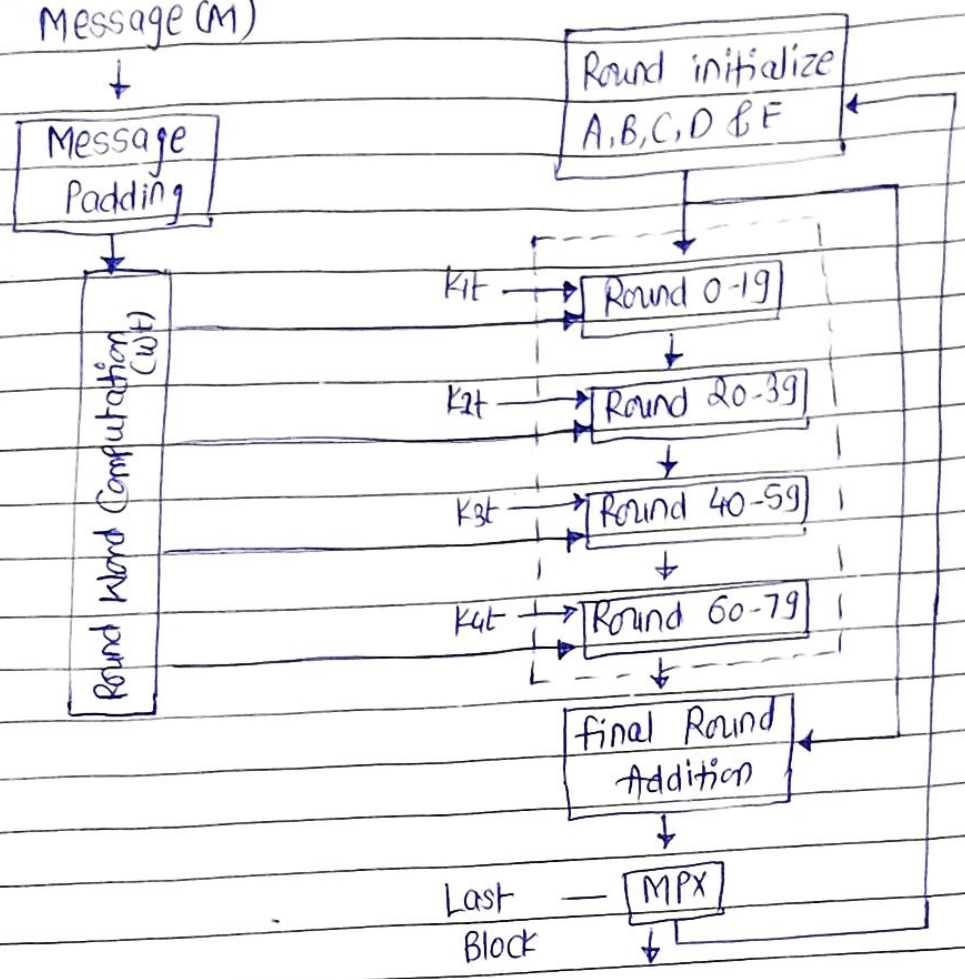
- Algorithm :-

Step 1 :- Create a MessageDiget object
- The messageDiget class provides a method name getInstance()
- This method accepts string variable specifying name of algo. to be used & returns a MessageDigest object implementing specific algo.

- step2 :- Pass the data to Created MessageDiget object
- After Creating message diget object, you need to pass to it.
- You can do so using update() method of MessageDigest() class.
- This method accepts a byte array representing message & add it to above created object.

- step3 :- Generate message digest
- You can generate message diget using diget () method od MessageDiget class this method computes hash fn on current obj. & returns msg digest in form of byte array.

- flowchart :-


Message (M)
Message Padding
Round Word Computation (wt)
Round initialize A,B,C,D & F
Kt
Round 0-19
K2t
Round 20-39
K3t
Round 40-59
K4t
Round 60-79
final Round Addition
Last Block
MPX

Page No.	
Class	
Roll No.	
Date:	/ /

- Conclusion:-

Hence, we had studied the SHA-1 algorithm successfully.