DATE 1/1
PAGE NO

Assignment - 03

mycompanion 43304

* Aim → To study and implement SHA-1 (Secure Hash Algorithm)

* Objective → To implement and understand details of SHA-1

* Theory →

The National Institute of Standard and Technology (NIST) along with NSA developed the SHA. SHA works with any input message that is $< 2^{64}$ ~~bytes~~ bits in length. The output of SHA-1 is a message digest which is 160 bits in length

	SHA-1	SHA-256	SHA-384	SHA-512
Message digest	160	256	384	512
Message size	$<2^{64}$	$<2^{64}$	$<2^{128}$	$<2^{128}$
Block size	512	512	1024	1024
Word size	32	32	64	64
Number of steps	80	64	80	80
Security	80	128	192	256

* Important steps in execution of SHA:

1. Padding - Add padding to the end of message
2. Append length - The length of message excluding padding
3. Divide the input into 512 bit blocks
4. Initialize chaining variables

Variable Name	Value (in Hex)
A	01 23 45 67
B	89 AB CD EF
C	FE DC BA 98
D	76 54 32 10
E	C3 D2 E1 F0

5. Process Block
   i) Copy chaining variables A-E into ~~a-e~~ a-e.
   ii) Divide the current 512 bit block into 16 sub blocks, each consisting of 32 bits.

iii) SHA has four rounds each consisting of 20 steps

iv) This makes a total of 80 iterations. The logical operation of SHA-1, mathematically is

abcde = 1e + Process P + S^5(a) + W[t] + K[t]),

a, S^{30} (b), c, d

- Required classes:

1. Class MessageDigest (java.security.MessageDigest) - Provides functionality of a message digest algorithm, such as MD5 or SHA.

* Conclusion → This, in this assignment we learnt about SHA and implemented SHA-1 algorithm in Java