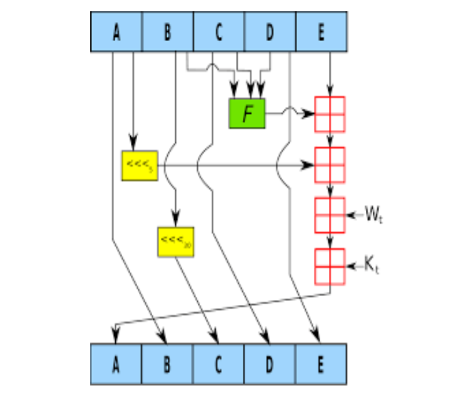
**AIM: To implement the SHA-I hashing technique using C program.**

DESCRIPTION: In cryptography, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function. SHA-1 produces a 160-bit hash value known as a message digest. The way this algorithm works is that for a message of size < 264 bits it computes a 160-bit condensed output called a message digest. The SHA-1 algorithm is designed so that it is practically infeasible to find two input messages that hash to the same output message. A hash functions such as SHA-1 is used to calculate an alphanumeric string that serves as the cryptographic representation of a file or a piece of data. This is called a digest and can serve as a digital signature. It is supposed to be unique and non-reversible.

**EXAMPLE:**



**ALGORITHM:**

STEP-1: Read the 256-bit key values.

STEP-2: Divide into five equal-sized blocks named A, B, C, D and E.

STEP-3: The blocks B, C and D are passed to the function F.

STEP-4: The resultant value is permuted with block E.

STEP-5: The block A is shifted right by ‘s’ times and permuted with the result of step-4.

STEP-6: Then it is permuted with a weight value and then with some other key pair and taken as the first block.

STEP-7: Block A is taken as the second block and the block B is shifted by ‘s’ times and taken as the third block.

STEP-8: The blocks C and D are taken as the block D and E for the final output.

**PROGRAM: (Secure Hash Algorithm)**

import java.security.\*;

public class SHA1 {

public static void main(String[] args) {

try {

MessageDigest md = MessageDigest.getInstance("SHA-1");

System.out.println("Message digest object info: ");

System.out.println(" Algorithm = " + md.getAlgorithm());

System.out.println(" Provider = " + md.getProvider());

System.out.println(" ToString = " + md.toString());

String input = "";

md.update(input.getBytes());

byte[] output = md.digest();

System.out.println();

System.out.println("SHA1(\"" + input + "\") = " + bytesToHex(output));

input = "abc";

md.update(input.getBytes());

output = md.digest();

System.out.println();

System.out.println("SHA1(\"" + input + "\") = " + bytesToHex(output));

input = "abcdefghijklmnopqrstuvwxyz";

md.update(input.getBytes());

output = md.digest();

System.out.println();

System.out.println("SHA1(\"" + input + "\") = " + bytesToHex(output));

} catch (Exception e) {

System.out.println("Exception: " + e);

}

}

public static String bytesToHex(byte[] b) {

char hexDigit[] = {'0', '1', '2', '3', '4', '5', '6',

'7', '8', '9', 'A', 'B', 'C', 'D', 'E', 'F'};

StringBuilder buf = new StringBuilder();

for (byte value : b) {

buf.append(hexDigit[(value >> 4) & 0x0f]);

buf.append(hexDigit[value & 0x0f]);

}

return buf.toString();

}

}

**OUTPUT:**

