***SAVEETHA SCHOOL OF ENGINEERING***

***SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCE***

**EXP NO 10: Calculate the message digest of the text by implementing the MD5 hashing technique**

**AIM**

To Calculate the message digest of the text by implementing the MD5 hashing technique

**PROCEDURE**

* In the first step, we add padding bits in the original message
* add the length bit in the output of the first step
* we use the 4 buffers i.e. J, K, L, and M. The size of each buffer is 32 bits.
* After all, rounds have been performed, the buffer J, K, L, and M contains the MD5 output starting with the lower bit J and ending with Higher bits M.

**PROGRAM**

#include <stdio.h>

#include <stdint.h>

#include <string.h>

#define LEFTROTATE(x, c) (((x) << (c)) | ((x) >> (32 - (c))))

void md5(const uint8\_t \*initial\_msg, size\_t initial\_len, uint8\_t \*digest) {

uint32\_t h0 = 0x67452301, h1 = 0xEFCDAB89, h2 = 0x98BADCFE, h3 = 0x10325476;

for (size\_t offset = 0; offset < initial\_len; offset += 64) {

uint32\_t \*w = (uint32\_t \*)(initial\_msg + offset);

uint32\_t a = h0, b = h1, c = h2, d = h3;

for (int i = 0; i < 64; i++) {

uint32\_t f = (i < 16) ? ((b & c) | ((~b) & d))

: (i < 32) ? ((d & b) | ((~d) & c))

: (i < 48) ? (b ^ c ^ d)

: (c ^ (b | (~d)));

int g = (i < 16) ? i : (i < 32) ? ((5 \* i + 1) % 16) : (i < 48) ? ((3 \* i + 5) % 16) : ((7 \* i) % 16);

uint32\_t temp = d;

d = c; c = b;

b += LEFTROTATE((a + f + 0x5A827999 + w[g]), 32); a = temp;

}

h0 += a; h1 += b; h2 += c; h3 += d;

}

memcpy(digest, &h0, 4); memcpy(digest + 4, &h1, 4); memcpy(digest + 8, &h2, 4); memcpy(digest + 12, &h3, 4);

}

int main() {

char initial\_msg[] = "Hello, world!";

size\_t initial\_len = strlen(initial\_msg);

uint8\_t digest[16];

md5((uint8\_t \*)initial\_msg, initial\_len, digest);

printf("MD5 digest of '%s': ", initial\_msg);

for(int i = 0; i < 16; i++) printf("%02x", digest[i]);

printf("\n");

return 0;

}

**OUTPUT**

