Lab- 12

Aim: Implement MD5 Hash Algorithm.

Theory:

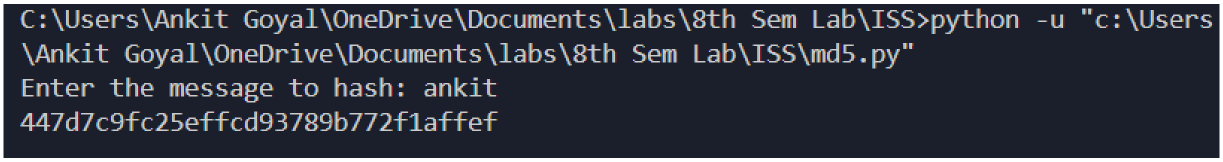
The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities.

CODE:

```
def newArray(num):
    array=[]
    for x in range(num):
        array.append(0)
    return array

def convertToWordArray(string):
    lMessageLength=len(string)
    lNumberOfWords_temp1=lMessageLength+8
    lNumberOfWords_temp2=(lNumberOfWords_temp1-(lNumberOfWords_temp1%64))/64
    lNumberOfWords=int((lNumberOfWords_temp2+1)*16)
    lWordArray=newArray(lNumberOfWords-1)
    lBytePosition=0
    lByteCount=0

    while lByteCount<lMessageLength:
        lWordCount=int((lByteCount-(lByteCount%4))/4)
        lBytePosition=(lByteCount%4)*8

lWordArray[lWordCount]=(lWordArray[lWordCount]|(ord(string[int(lByteCount)])<<lBytePosition))
        lByteCount+=1

    lWordCount=int((lByteCount-(lByteCount%4))/4)
    lBytePosition=(lByteCount%4)*8
    lWordArray[lWordCount]=lWordArray[lWordCount]|(0x80<<lBytePosition)
    lWordArray[lNumberOfWords-2]=lMessageLength<<3
    lWordArray.append(lMessageLength>>29)

    return lWordArray
```

```
def F(x,y,z):
    return (x & y) | ((~x) & z)

def G(x,y,z):
    return (x & z) | (y & (~z))

def H(x,y,z):
    return x ^ y ^ z

def I(x,y,z):
    return y ^ (x | (~z))

def XX(func, a, b, c, d, x, s, ac):
    res=0
    res=res+a+func(b,c,d)
    res+=x
    res+=ac
    res=res & 0xffffffff
    res=rol(res,s)
    res=res & 0xffffffff
    res+=b
    return res & 0xffffffff

def addu(x,y):
    ls=(x & 0xffffffff)+(y & 0xffffffff)
    return (((x>>16)+(y>>16)+(ls>>16))<<16)|(ls & 0xffffffff)

def rol(v,s):
    return (v<<s)|(v>>(32-s))

def wordToHex(lValue):
    wordToHexValue="
    wordToHexValue_temp="

    for lCount in range(4):
        lByte=(lValue>>(lCount*8)) & 255
        wordToHexValue_temp="0"+format(lByte, 'x')
        wordToHexValue=wordToHexValue+wordToHexValue_temp[-2:]
    return wordToHexValue

def md5hash(message):
    x=convertToWordArray(message)
    a=0x67452301
    b=0xEFCDAB89
    c=0x98BADCFE
    d=0x10325476
    xl=len(x)
    j=0

    while j<xl:
        aa=a
        bb=b
        cc=c
        dd=d
        a=XX(F,a,b,c,d, x[j+0], 7,0xD76AA478)
        d=XX(F,d,a,b,c, x[j+1],12,0xE8C7B756)
        c=XX(F,c,d,a,b, x[j+2],17,0x242070DB)
        b=XX(F,b,c,d,a, x[j+3],22,0xC1BDCEEE)
        a=XX(F,a,b,c,d, x[j+4], 7,0xF57C0FAF)
        d=XX(F,d,a,b,c, x[j+5],12,0x4787C62A)
        c=XX(F,c,d,a,b, x[j+6],17,0xA8304613)
        b=XX(F,b,c,d,a, x[j+7],22,0xFD469501)
        a=XX(F,a,b,c,d, x[j+8], 7,0x698098D8)
        d=XX(F,d,a,b,c, x[j+9],12,0x8B44F7AF)
        c=XX(F,c,d,a,b,x[j+10],17,0xFFFF5BB1)
        b=XX(F,b,c,d,a,x[j+11],22,0x895CD7BE)
        a=XX(F,a,b,c,d,x[j+12], 7,0x6B901122)
        d=XX(F,d,a,b,c,x[j+13],12,0xFD987193)
        c=XX(F,c,d,a,b,x[j+14],17,0xA679438E)
        b=XX(F,b,c,d,a,x[j+15],22,0x49B40821)
        a=XX(G,a,b,c,d, x[j+1], 5,0xF61E2562)
        d=XX(G,d,a,b,c, x[j+6], 9,0xC040B340)
        c=XX(G,c,d,a,b,x[j+11],14,0x265E5A51)
        b=XX(G,b,c,d,a, x[j+0],20,0xE9B6C7AA)
        a=XX(G,a,b,c,d, x[j+5], 5,0xD62F105D)
        d=XX(G,d,a,b,c,x[j+10], 9,0x2441453)
        c=XX(G,c,d,a,b,x[j+15],14,0xD8A1E681)
        b=XX(G,b,c,d,a, x[j+4],20,0xE7D3FBC8)
        a=XX(G,a,b,c,d, x[j+9], 5,0x21E1CDE6)
        d=XX(G,d,a,b,c,x[j+14], 9,0xC33707D6)
        c=XX(G,c,d,a,b, x[j+3],14,0xF4D50D87)
        b=XX(G,b,c,d,a, x[j+8],20,0x455A14ED)
        a=XX(G,a,b,c,d,x[j+13], 5,0xA9E3E905)
        d=XX(G,d,a,b,c, x[j+2], 9,0xFCEFA3F8)
        c=XX(G,c,d,a,b, x[j+7],14,0x676F02D9)
        b=XX(G,b,c,d,a,x[j+12],20,0x8D2A4C8A)
        a=XX(H,a,b,c,d, x[j+5], 4,0xFFFA3942)
        d=XX(H,d,a,b,c, x[j+8],11,0x8771F681)
        c=XX(H,c,d,a,b,x[j+11],16,0x6D9D6122)
        b=XX(H,b,c,d,a,x[j+14],23,0xFDE5380C)
        a=XX(H,a,b,c,d, x[j+1], 4,0xA4BEEA44)
        d=XX(H,d,a,b,c, x[j+4],11,0x4BDECFA9)
        c=XX(H,c,d,a,b, x[j+7],16,0xF6BB4B60)
        b=XX(H,b,c,d,a,x[j+10],23,0xBEBFBC70)
        a=XX(H,a,b,c,d,x[j+13], 4,0x289B7EC6)
        d=XX(H,d,a,b,c, x[j+0],11,0xEAA127FA)
        c=XX(H,c,d,a,b, x[j+3],16,0xD4EF3085)
        b=XX(H,b,c,d,a, x[j+6],23,0x4881D05)
        a=XX(H,a,b,c,d, x[j+9], 4,0xD9D4D039)
        d=XX(H,d,a,b,c,x[j+12],11,0xE6DB99E5)
        c=XX(H,c,d,a,b,x[j+15],16,0x1FA27CF8)
        b=XX(H,b,c,d,a, x[j+2],23,0xC4AC5665)
        a=XX(I,a,b,c,d, x[j+0], 6,0xF4292244)
        d=XX(I,d,a,b,c, x[j+7],10,0x432AFF97)
        c=XX(I,c,d,a,b,x[j+14],15,0xAB9423A7)
        b=XX(I,b,c,d,a, x[j+5],21,0xFC93A039)
        a=XX(I,a,b,c,d,x[j+12], 6,0x655B59C3)
        d=XX(I,d,a,b,c, x[j+3],10,0x8F0CCC92)
        c=XX(I,c,d,a,b,x[j+10],15,0xFFEFF47D)
        b=XX(I,b,c,d,a, x[j+1],21,0x85845DD1)
        a=XX(I,a,b,c,d, x[j+8], 6,0x6FA87E4F)
        d=XX(I,d,a,b,c,x[j+15],10,0xFE2CE6E0)
        c=XX(I,c,d,a,b, x[j+6],15,0xA3014314)
        b=XX(I,b,c,d,a,x[j+13],21,0x4E0811A1)
        a=XX(I,a,b,c,d, x[j+4], 6,0xF7537E82)
        d=XX(I,d,a,b,c,x[j+11],10,0xBD3AF235)
        c=XX(I,c,d,a,b, x[j+2],15,0x2AD7D2BB)
        b=XX(I,b,c,d,a, x[j+9],21,0xEB86D391)
        a=addu(a,aa)
        b=addu(b,bb)
        c=addu(c,cc)
        d=addu(d,dd)
        j+=16

    return (wordToHex(a)+wordToHex(b)+wordToHex(c)+wordToHex(d)).lower()


message = input ("Enter the message to hash: ")
print (md5hash (message))
```

OUTPUT:



```
C:\Users\Ankit Goyal\OneDrive\Documents\labs\8th Sem Lab\ISS>python -u "c:\Users
\Ankit Goyal\OneDrive\Documents\labs\8th Sem Lab\ISS\md5.py"
Enter the message to hash: ankit
447d7c9fc25effcd93789b772f1affef
```