Course Title: Cryptography and Network Security Lab	**Course Code**: BCSE309P
Faculty: Prof. Karthika V	Slot: L11-L12
Regno: 21BCE1964	Name: Aadityaa.N

Exercise-5: MD5

Code:

```
import struct
from enum import Enum
from math import floor, sin
from bitarray import bitarray

# Define the four auxiliary functions that produce one 32-bit word.
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 rotate_left(x, n):
    return x << n | x >> 32 - n

def modular_add(a, b):
    return (a + b) % pow(2, 32)

# T table
T = [floor(pow(2, 32) * abs(sin(i + 1))) for i in range(64)]

class MD5:
    input_string = None
    buffers = {
        "A": 0x67452301,
        "B": 0xEFCDAB89,
        "C": 0x98BADCFE,
        "D": 0x10325476,
    }
```

```
    def hash(self, string):
        self.input_string = string
        # convert string to bit array for easier operation and add padding
        temp = self.step_1()
        # Append length of message to end of data
        preprocessed_bit_array = self.step_2(temp)
        self.step_3(preprocessed_bit_array)
        return self.step_4()

    def step_1(self):
        bit_array = bitarray(endian="big")
        bit_array.frombytes(self.input_string.encode("utf-8"))
        bit_array.append(1)
        while len(bit_array) % 512 != 448:
            bit_array.append(0)
        # go back to littler endian for ease
        return bitarray(bit_array, endian="little")

    def step_2(self, step_1_result):
        # get length of message in bits
        length = (len(self.input_string) * 8) % pow(2, 64)
        length_bit_array = bitarray(endian="little")
        length_bit_array.frombytes(struct.pack("<Q", length))
        result = step_1_result.copy()
        result.extend(length_bit_array)
        return result

    def step_3(self, step_2_result):
        # The total number of 32-bit words to process
        N = len(step_2_result) // 32
        # Process each block
        for chunk_index in range(N // 16):
            # Break the chunk into 16 words of 32 bits in list X.
            start = chunk_index * 512
            X = [step_2_result[start + (x * 32) : start + (x * 32) + 32] for x
in range(16)]
            # Convert the `bitarray` objects to integers to prevent errors in
the F,G,H,I functions
            X = [int.from_bytes(word.tobytes(), byteorder="little") for word in
X]
            # Simplify
            A = self.buffers["A"]
            B = self.buffers["B"]
            C = self.buffers["C"]
            D = self.buffers["D"]
```

```
            # Execute the four rounds with 16 operations each.
            for i in range(4 * 16):
                if 0 <= i <= 15:
                    k = i
                    s = [7, 12, 17, 22]
                    temp = F(B, C, D)
                elif 16 <= i <= 31:
                    k = ((5 * i) + 1) % 16
                    s = [5, 9, 14, 20]
                    temp = G(B, C, D)
                elif 32 <= i <= 47:
                    k = ((3 * i) + 5) % 16
                    s = [4, 11, 16, 23]
                    temp = H(B, C, D)
                elif 48 <= i <= 63:
                    k = (7 * i) % 16
                    s = [6, 10, 15, 21]
                    temp = I(B, C, D)
                temp = modular_add(temp, X[k])
                temp = modular_add(temp, T[i])
                temp = modular_add(temp, A)
                temp = rotate_left(temp, s[i % 4])
                temp = modular_add(temp, B)
                A = D
                D = C
                C = B
                B = temp
                print("Round", i+1, "A:", A, "B:", B, "C:", C, "D:", D)
            # Final Updated for this chunk
            self.buffers["A"] = modular_add(self.buffers["A"], A)
            self.buffers["B"] = modular_add(self.buffers["B"], B)
            self.buffers["C"] = modular_add(self.buffers["C"], C)
            self.buffers["D"] = modular_add(self.buffers["D"], D)
            print("Buffers:", self.buffers)
            print(f"Chunk {chunk_index + 1} of {N // 512} done")

    def step_4(self):
        # Convert the buffers to little-endian to make it easier
        A = struct.unpack("<I", struct.pack(">I", self.buffers["A"]))[0]
        B = struct.unpack("<I", struct.pack(">I", self.buffers["B"]))[0]
        C = struct.unpack("<I", struct.pack(">I", self.buffers["C"]))[0]
        D = struct.unpack("<I", struct.pack(">I", self.buffers["D"]))[0]
        # return all the blocks joined together
        return f"{format(A, '08x')}{format(B, '08x')}{format(C,
'08x')}{format(D, '08x')}"
```

```
if __name__ == "__main__":
    print("Exactly 448 Bits: 56 characters")
    string1 = "This is aadityaa 21BCE1964 studying in VIT Chennai India"
    print("Input Message", string1)
    print("Hash:", MD5().hash(string1))

    print("\nLess than 448 Bits: 11 characters")
    string2 = "Aadityaa .N"
    print("Input Message", string2)
    print("Hash:", MD5().hash(string2))

    print("\nGreater than 448 bits: 118 characters")
    string3 = "This is Aadityaa Nagarajan 21BCE1964 studying in vit chennai
India i like programming and this is a wonderfull world ."
    print("Input Message", string3)
    print("Hash:", MD5().hash(string3))
```

Output1:

```
PS D:\SEM - 6> python -u "d:\SEM - 6\CNS\Lab - 5\Md5.py"
Exactly 448 Bits: 56 characters
Input Message This is aadityaa 21BCE1964 studying in VIT Chennai India
Round 1 A: 271733878 B: 4029348956 C: 4023233417 D: 2562383102
Round 2 A: 2562383102 B: 80915138 C: 4029348956 D: 4023233417
Round 3 A: 4023233417 B: 2303716 C: 80915138 D: 4029348956
Round 4 A: 4029348956 B: 3748474408 C: 2303716 D: 80915138
Round 5 A: 80915138 B: 1391240892 C: 3748474408 D: 2303716
Round 6 A: 2303716 B: 3062762097 C: 1391240892 D: 3748474408
Round 7 A: 3748474408 B: 902147834 C: 3062762097 D: 1391240892
Round 8 A: 1391240892 B: 683806872 C: 902147834 D: 3062762097
Round 9 A: 3062762097 B: 950182484 C: 683806872 D: 902147834
Round 10 A: 902147834 B: 553234413 C: 950182484 D: 683806872
Round 11 A: 683806872 B: 4028362948 C: 553234413 D: 950182484
Round 12 A: 950182484 B: 1076905104 C: 4028362948 D: 553234413
Round 13 A: 553234413 B: 3368761691 C: 1076905104 D: 4028362948
Round 14 A: 4028362948 B: 1498667694 C: 3368761691 D: 1076905104
Round 15 A: 1076905104 B: 4197423262 C: 1498667694 D: 3368761691
Round 16 A: 3368761691 B: 2590524063 C: 4197423262 D: 1498667694
Round 17 A: 1498667694 B: 1592733326 C: 2590524063 D: 4197423262
Round 18 A: 4197423262 B: 1861812498 C: 1592733326 D: 2590524063
Round 19 A: 2590524063 B: 1614740110 C: 1861812498 D: 1592733326
Round 20 A: 1592733326 B: 559557058 C: 1614740110 D: 1861812498
Round 21 A: 1861812498 B: 1653985600 C: 559557058 D: 1614740110
Round 22 A: 1614740110 B: 2394439785 C: 1653985600 D: 559557058
Round 23 A: 559557058 B: 990650184 C: 2394439785 D: 1653985600
Round 24 A: 1653985600 B: 1787542960 C: 990650184 D: 2394439785
Round 25 A: 2394439785 B: 2878495029 C: 1787542960 D: 990650184
Round 26 A: 990650184 B: 2442541743 C: 2878495029 D: 1787542960
Round 27 A: 1787542960 B: 578734253 C: 2442541743 D: 2878495029
Round 28 A: 2878495029 B: 1621964504 C: 578734253 D: 2442541743
Round 29 A: 2442541743 B: 1071160823 C: 1621964504 D: 578734253
Round 30 A: 578734253 B: 1277223686 C: 1071160823 D: 1621964504
Round 31 A: 1621964504 B: 2505557223 C: 1277223686 D: 1071160823
Round 32 A: 1071160823 B: 2723486135 C: 2505557223 D: 1277223686
Round 33 A: 1277223686 B: 443588300 C: 2723486135 D: 2505557223
Round 34 A: 2505557223 B: 1997432571 C: 443588300 D: 2723486135
Round 35 A: 2723486135 B: 615362450 C: 1997432571 D: 443588300
```

```
Round 40 A: 1476986456 B: 1271487317 C: 285858542 D: 4113888633
Round 41 A: 4113888633 B: 1431894360 C: 1271487317 D: 285858542
Round 42 A: 285858542 B: 3389763795 C: 1431894360 D: 1271487317
Round 43 A: 1271487317 B: 3898436454 C: 3389763795 D: 1431894360
Round 44 A: 1431894360 B: 2353077043 C: 3898436454 D: 3389763795
Round 45 A: 3389763795 B: 1620688048 C: 2353077043 D: 3898436454
Round 46 A: 3898436454 B: 3377900123 C: 1620688048 D: 2353077043
Round 47 A: 2353077043 B: 3213678568 C: 3377900123 D: 1620688048
Round 48 A: 1620688048 B: 222326913 C: 3213678568 D: 3377900123
Round 49 A: 3377900123 B: 1465958646 C: 222326913 D: 3213678568
Round 50 A: 3213678568 B: 745169552 C: 1465958646 D: 222326913
Round 51 A: 222326913 B: 1117121776 C: 745169552 D: 1465958646
Round 52 A: 1465958646 B: 118490661 C: 1117121776 D: 745169552
Round 53 A: 745169552 B: 1983093817 C: 118490661 D: 1117121776
Round 54 A: 1117121776 B: 22318856 C: 1983093817 D: 118490661
Round 55 A: 118490661 B: 603781169 C: 22318856 D: 1983093817
Round 56 A: 1983093817 B: 1118035916 C: 603781169 D: 22318856
Round 57 A: 22318856 B: 258766204 C: 1118035916 D: 603781169
Round 58 A: 603781169 B: 1206181873 C: 258766204 D: 1118035916
Round 59 A: 1118035916 B: 2865707960 C: 1206181873 D: 258766204
Round 60 A: 258766204 B: 1639512226 C: 2865707960 D: 1206181873
Round 61 A: 1206181873 B: 4008099256 C: 1639512226 D: 2865707960
Round 62 A: 2865707960 B: 2789526597 C: 4008099256 D: 1639512226
Round 63 A: 1639512226 B: 3874545513 C: 2789526597 D: 4008099256
Round 64 A: 4008099256 B: 3534012164 C: 3874545513 D: 2789526597
Buffers: {'A': 2592876662, 'B': 3679071621, 'C': 4137671823, 'D': 742054574}
Chunk 2 of 0 done
Hash: 76288c9a852d4adb8fdc9ff6aeda3a2c
```

Output2:

```
Less than 448 Bits: 11 characters
Input Message Aadityaa .N
Round 1 A: 742054574 B: 123944324 C: 3679071621 D: 4137671823
Round 2 A: 4137671823 B: 2302629498 C: 123944324 D: 3679071621
Round 3 A: 3679071621 B: 2267428261 C: 2302629498 D: 123944324
Round 4 A: 123944324 B: 2884489579 C: 2267428261 D: 2302629498
Round 5 A: 2302629498 B: 3063940011 C: 2884489579 D: 2267428261
Round 6 A: 2267428261 B: 2344434417 C: 3063940011 D: 2884489579
Round 7 A: 2884489579 B: 176480095 C: 2344434417 D: 3063940011
Round 8 A: 3063940011 B: 1641993599 C: 176480095 D: 2344434417
Round 9 A: 2344434417 B: 3308062420 C: 1641993599 D: 176480095
Round 10 A: 176480095 B: 3056401660 C: 3308062420 D: 1641993599
Round 11 A: 1641993599 B: 939302400 C: 3056401660 D: 3308062420
Round 12 A: 3308062420 B: 3161782354 C: 939302400 D: 3056401660
Round 13 A: 3056401660 B: 1498368389 C: 3161782354 D: 939302400
Round 14 A: 939302400 B: 4263004336 C: 1498368389 D: 3161782354
Round 15 A: 3161782354 B: 3009984117 C: 4263004336 D: 1498368389
Round 16 A: 1498368389 B: 1009304711 C: 3009984117 D: 4263004336
Round 17 A: 4263004336 B: 2814984137 C: 1009304711 D: 3009984117
Round 18 A: 3009984117 B: 3937314468 C: 2814984137 D: 1009304711
Round 19 A: 1009304711 B: 517163024 C: 3937314468 D: 2814984137
Round 20 A: 2814984137 B: 3427006185 C: 517163024 D: 3937314468
Round 21 A: 3937314468 B: 365679028 C: 3427006185 D: 517163024
Round 22 A: 517163024 B: 2200941367 C: 365679028 D: 3427006185
Round 23 A: 3427006185 B: 3147912567 C: 2200941367 D: 365679028
Round 24 A: 365679028 B: 438686029 C: 3147912567 D: 2200941367
Round 25 A: 2200941367 B: 1687448891 C: 438686029 D: 3147912567
Round 26 A: 3147912567 B: 999665160 C: 1687448891 D: 438686029
Round 27 A: 438686029 B: 1063500235 C: 999665160 D: 1687448891
Round 28 A: 1687448891 B: 1404936676 C: 1063500235 D: 999665160
Round 29 A: 999665160 B: 566141512 C: 1404936676 D: 1063500235
Round 30 A: 1063500235 B: 2391507839 C: 566141512 D: 1404936676
Round 31 A: 1404936676 B: 512734678 C: 2391507839 D: 566141512
Round 32 A: 566141512 B: 484879694 C: 512734678 D: 2391507839
Round 33 A: 2391507839 B: 111027304 C: 484879694 D: 512734678
Round 34 A: 512734678 B: 2891294015 C: 111027304 D: 484879694
Round 35 A: 484879694 B: 4016498585 C: 2891294015 D: 111027304
```

```
Round 31 A: 1404936676 B: 512734678 C: 2391507839 D: 566141512
Round 32 A: 566141512 B: 484879694 C: 512734678 D: 2391507839
Round 33 A: 2391507839 B: 111027304 C: 484879694 D: 512734678
Round 34 A: 512734678 B: 2891294015 C: 111027304 D: 484879694
Round 35 A: 484879694 B: 4016498585 C: 2891294015 D: 111027304
Round 36 A: 111027304 B: 798434367 C: 4016498585 D: 2891294015
Round 37 A: 2891294015 B: 404249464 C: 798434367 D: 4016498585
Round 38 A: 4016498585 B: 143036928 C: 404249464 D: 798434367
Round 39 A: 798434367 B: 684111660 C: 143036928 D: 404249464
Round 40 A: 404249464 B: 2858028763 C: 684111660 D: 143036928
Round 41 A: 143036928 B: 1463448119 C: 2858028763 D: 684111660
Round 42 A: 684111660 B: 4288435502 C: 1463448119 D: 2858028763
Round 43 A: 2858028763 B: 286217696 C: 4288435502 D: 1463448119
Round 44 A: 1463448119 B: 2109971375 C: 286217696 D: 4288435502
Round 45 A: 4288435502 B: 3284236491 C: 2109971375 D: 286217696
Round 46 A: 286217696 B: 4042143095 C: 3284236491 D: 2109971375
Round 47 A: 2109971375 B: 2581181717 C: 4042143095 D: 3284236491
Round 48 A: 3284236491 B: 4208009668 C: 2581181717 D: 4042143095
Round 49 A: 4042143095 B: 20003953 C: 4208009668 D: 2581181717
Round 50 A: 2581181717 B: 4286739384 C: 20003953 D: 4208009668
Round 51 A: 4208009668 B: 3455161790 C: 4286739384 D: 20003953
Round 52 A: 20003953 B: 2389742090 C: 3455161790 D: 4286739384
Round 53 A: 4286739384 B: 345578356 C: 2389742090 D: 3455161790
Round 54 A: 3455161790 B: 289423505 C: 345578356 D: 2389742090
Round 55 A: 2389742090 B: 295590445 C: 289423505 D: 345578356
Round 56 A: 345578356 B: 2593063286 C: 295590445 D: 289423505
Round 57 A: 289423505 B: 1936639762 C: 2593063286 D: 295590445
Round 58 A: 295590445 B: 2879855847 C: 1936639762 D: 2593063286
Round 59 A: 2593063286 B: 390481283 C: 2879855847 D: 1936639762
Round 60 A: 1936639762 B: 2603214449 C: 390481283 D: 2879855847
Round 61 A: 2879855847 B: 1537477117 C: 2603214449 D: 390481283
Round 62 A: 390481283 B: 894872866 C: 1537477117 D: 2603214449
Round 63 A: 2603214449 B: 3584124451 C: 894872866 D: 1537477117
Round 64 A: 1537477117 B: 1980387813 C: 3584124451 D: 894872866
Buffers: {'A': 4130353779, 'B': 1364492138, 'C': 3426828978, 'D': 1636927440}
Chunk 1 of 0 done
Hash: 733230f66a7f5451b24241ccd0879161
```

Output 3:

```
Greater than 448 bits: 118 characters
Input Message This is Aadityaa Nagarajan 21BCE1964 studying in vit chennai India i like programming and this is a wonderfull world .
Round 1 A: 1636927440 B: 3400295272 C: 1364492138 D: 3426828978
Round 2 A: 3426828978 B: 2654907550 C: 3400295272 D: 1364492138
Round 3 A: 1364492138 B: 4180496519 C: 2654907550 D: 3400295272
Round 4 A: 3400295272 B: 372924875 C: 4180496519 D: 2654907550
Round 5 A: 2654907550 B: 2215852778 C: 372924875 D: 4180496519
Round 6 A: 4180496519 B: 909448834 C: 2215852778 D: 372924875
Round 7 A: 372924875 B: 940374397 C: 909448834 D: 2215852778
Round 8 A: 2215852778 B: 782733327 C: 940374397 D: 909448834
Round 9 A: 909448834 B: 959118776 C: 782733327 D: 940374397
Round 10 A: 940374397 B: 804464436 C: 959118776 D: 782733327
Round 11 A: 782733327 B: 2165495495 C: 804464436 D: 959118776
Round 12 A: 959118776 B: 2095893485 C: 2165495495 D: 804464436
Round 13 A: 804464436 B: 2946409944 C: 2095893485 D: 2165495495
Round 14 A: 2165495495 B: 2731034074 C: 2946409944 D: 2095893485
Round 15 A: 2095893485 B: 3831086936 C: 2731034074 D: 2946409944
Round 16 A: 2946409944 B: 3741317298 C: 3831086936 D: 2731034074
Round 17 A: 2731034074 B: 195785408 C: 3741317298 D: 3831086936
Round 18 A: 3831086936 B: 2238740563 C: 195785408 D: 3741317298
Round 19 A: 3741317298 B: 732477954 C: 2238740563 D: 195785408
Round 20 A: 195785408 B: 893070931 C: 732477954 D: 2238740563
Round 21 A: 2238740563 B: 946515232 C: 893070931 D: 732477954
Round 22 A: 732477954 B: 1176037269 C: 946515232 D: 893070931
Round 23 A: 893070931 B: 3162961243 C: 1176037269 D: 946515232
Round 24 A: 946515232 B: 4157542371 C: 3162961243 D: 1176037269
Round 25 A: 1176037269 B: 3640339075 C: 4157542371 D: 3162961243
Round 26 A: 3162961243 B: 471610234 C: 3640339075 D: 4157542371
Round 27 A: 4157542371 B: 3443050625 C: 471610234 D: 3640339075
Round 28 A: 3640339075 B: 2190222750 C: 3443050625 D: 471610234
Round 29 A: 471610234 B: 3336866459 C: 2190222750 D: 3443050625
Round 30 A: 3443050625 B: 1962652038 C: 3336866459 D: 2190222750
Round 31 A: 2190222750 B: 592902298 C: 1962652038 D: 3336866459
Round 32 A: 3336866459 B: 3221095267 C: 592902298 D: 1962652038
Round 33 A: 1962652038 B: 461623683 C: 3221095267 D: 592902298
Round 34 A: 592902298 B: 1190936323 C: 461623683 D: 3221095267
Round 35 A: 3221095267 B: 2474780943 C: 1190936323 D: 461623683
Round 36 A: 461623683 B: 1301535947 C: 2474780943 D: 1190936323
```

```
Round 32 A: 1391485101 B: 979043711 C: 1292476367 D: 3048181788
Round 33 A: 3048181788 B: 20290967 C: 979043711 D: 1292476367
Round 34 A: 1292476367 B: 1976185687 C: 20290967 D: 979043711
Round 35 A: 979043711 B: 1488005798 C: 1976185687 D: 20290967
Round 36 A: 20290967 B: 694383112 C: 1488005798 D: 1976185687
Round 37 A: 1976185687 B: 865472400 C: 694383112 D: 1488005798
Round 38 A: 1488005798 B: 1411232612 C: 865472400 D: 694383112
Round 39 A: 694383112 B: 1739974590 C: 1411232612 D: 865472400
Round 40 A: 865472400 B: 2617330602 C: 1739974590 D: 1411232612
Round 41 A: 1411232612 B: 1505978442 C: 2617330602 D: 1739974590
Round 42 A: 1739974590 B: 854981635 C: 1505978442 D: 2617330602
Round 43 A: 2617330602 B: 303216174 C: 854981635 D: 1505978442
Round 44 A: 1505978442 B: 2955584501 C: 303216174 D: 854981635
Round 45 A: 854981635 B: 1576810643 C: 2955584501 D: 303216174
Round 46 A: 303216174 B: 3196938897 C: 1576810643 D: 2955584501
Round 47 A: 2955584501 B: 3819630498 C: 3196938897 D: 1576810643
Round 48 A: 1576810643 B: 873254912 C: 3819630498 D: 3196938897
Round 49 A: 3196938897 B: 4086554207 C: 873254912 D: 3819630498
Round 50 A: 3819630498 B: 1420841965 C: 4086554207 D: 873254912
Round 51 A: 873254912 B: 821899708 C: 1420841965 D: 4086554207
Round 52 A: 4086554207 B: 520036406 C: 821899708 D: 1420841965
Round 53 A: 1420841965 B: 2835892409 C: 520036406 D: 821899708
Round 54 A: 821899708 B: 2967556649 C: 2835892409 D: 520036406
Round 55 A: 520036406 B: 922283591 C: 2967556649 D: 2835892409
Round 56 A: 2835892409 B: 1713444179 C: 922283591 D: 2967556649
Round 57 A: 2967556649 B: 631828208 C: 1713444179 D: 922283591
Round 58 A: 922283591 B: 2587344858 C: 631828208 D: 1713444179
Round 59 A: 1713444179 B: 1031771929 C: 2587344858 D: 631828208
Round 60 A: 631828208 B: 3038954865 C: 1031771929 D: 2587344858
Round 61 A: 2587344858 B: 3208669832 C: 3038954865 D: 1031771929
Round 62 A: 1031771929 B: 631241929 C: 3208669832 D: 3038954865
Round 63 A: 3038954865 B: 2801844299 C: 631241929 D: 3208669832
Round 64 A: 3208669832 B: 3687966818 C: 2801844299 D: 631241929
Buffers: {'A': 720509403, 'B': 2394775140, 'C': 616711975, 'D': 219154082}
Chunk 2 of 0 done
Hash: db19f22a645ebd8e2747c224a206100d
PS D:\SEM - 6>
```