SHA-256

Name: Ranjan Yadav

Roll no: EVD17I009

Work Plan(Week 3): I intend to work on finishing the code for **complete SHA-256 code** for writing the code for its verification using system verilog.

So for the code, we need to implement some of the functions, namely Compression function, Maj function, Smallsigma 0 & 1 and Capitalsigma 0&1.

$$
\begin{aligned}
Ch(x,y,z) &= (x \wedge y) \oplus (\neg x \wedge z) \\
Maj(x,y,z) &= (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \\
\Sigma_0(x) &= S^2(x) \oplus S^{13}(x) \oplus S^{22}(x) \\
\Sigma_1(x) &= S^6(x) \oplus S^{11}(x) \oplus S^{25}(x) \\
\sigma_0(x) &= S^7(x) \oplus S^{18}(x) \oplus R^3(x) \\
\sigma_1(x) &= S^{17}(x) \oplus S^{19}(x) \oplus R^{10}(x)
\end{aligned}
$$

Other than that I have implemented the message padding module(week1), better to write it as a function as well in order to optimize the code and also implement the message expanded block in a single always block, we reduce the need of other modules as well.

$\oplus$	bitwise XOR
$\wedge$	bitwise AND
$\vee$	bitwise OR
$\neg$	bitwise complement
$+$	mod 2^{32} addition
R^n	right shift by n bits
S^n	right rotation by n bits

Necessary Notation

Code:

Main module for SHA-256(With all necessary functions defined inside).

```
module sha_256(input_data,out_data,clk,reset);
input [255:0]input_data;
output reg [255:0] out_data;
input reset;
input clk;

reg [31:0]a;
reg [31:0]b;
reg [31:0]c;
reg [31:0]d;
reg [31:0]e;
reg [31:0]f;
reg [31:0]g;
reg [31:0]h;

reg [31:0]constant_h[7:0];
reg [31:0]constant_k[63:0];
reg [511:0] padded_data;
reg [0:2047] W;

int j;
int i;

reg [31:0] temp1;
reg [31:0] temp2;
reg [31:0] temp3;
reg [31:0] temp4;
reg [31:0] temp5;
```

```
reg [31:0] temp6;


reg [31:0] ch;
reg [31:0] maj;
reg [31:0] cs1;
reg [31:0] cs0;
reg [31:0] ss1;
reg [31:0] ss0;
reg [31:0] ct1;
reg [31:0] ct2;


function [31:0]Ch;
input [31:0] x;
input [31:0] y;
input [31:0] z;
begin
 Ch= (x&y)^((~x)&z);
end
endfunction


function [31:0]Maj;
input [31:0] x;
input [31:0] y;
input [31:0] z;
begin
        Maj=(x&y)^(x&z)^(y&z);
end
endfunction


function [31:0]SmallSigma0;
```

```
input [31:0]msg;
begin
SmallSigma0 = {msg[6:0],msg[31:7]} ^ {msg[17:0],msg[31:18]} ^ {3'b0,msg[31:3]};
end
endfunction

function [31:0]SmallSigma1;
input [31:0]msg;
begin
SmallSigma1 = {msg[16:0],msg[31:17]} ^ {msg[18:0],msg[31:19]} ^ {10'b0,msg[31:10]} ;
end
endfunction

function [31:0]CapitalSigma0;
input [31:0]msg;
begin
CapitalSigma0 ={msg[1:0],msg[31:2]}^{msg[12:0],msg[31:13]}^{msg[21:0],msg[31:22]};
end
endfunction

function [31:0]CapitalSigma1;
input [31:0]msg;
begin
CapitalSigma1 ={msg[5:0],msg[31:6]}^{msg[10:0],msg[31:11]}^{msg[24:0],msg[31:25]};
end
endfunction

reg [63:0]length=64'd256; //binary rep of 256 is feeded into 64 bit register
reg add_one=1'b1;
reg [190:0]append_zero=191'b0;
```

```
function [511:0]message_padding;
input [255:0] msg;
begin
        message_padding={msg,add_one,append_zero,length};
end
endfunction

always @(posedge clk)
        begin
                if(reset==1)
                        begin
                        padded_data=message_padding(input_data);
                        $display("Padded Message is = %h\n\n",padded_data);

                constant_h[0] = 32'h6a09e667;
                constant_h[1] = 32'hbb67ae85;
                constant_h[2] = 32'h3c6ef372;
                constant_h[3] = 32'ha54ff53a;
                constant_h[4] = 32'h510e527f;
                constant_h[5] = 32'h9b05688c;
                constant_h[6] = 32'h1f83d9ab;
                constant_h[7] = 32'h5be0cd19;
                #10;

                W[0:511]=padded_data[511:0];

                a<=constant_h[0];
                b<=constant_h[1];
                c<=constant_h[2];
```

```
d<=constant_h[3];
e<=constant_h[4];
f<=constant_h[5];
g<=constant_h[6];
h<=constant_h[7];

#10;
constant_k[0] <= 32'h428a2f98;
constant_k[1] <= 32'h71374491;
constant_k[2] <= 32'hb5c0fbcf;
constant_k[3] <= 32'he9b5dba5;
constant_k[4] <= 32'h3956c25b;
constant_k[5] <= 32'h59f111f1;
constant_k[6] <= 32'h923f82a4;
constant_k[7] <= 32'hab1c5ed5;
constant_k[8] <= 32'hd807aa98;
constant_k[9] <= 32'h12835b01;
constant_k[10]<= 32'h243185be;
constant_k[11]<= 32'h550c7dc3;
constant_k[12]<= 32'h72be5d74;
constant_k[13]<= 32'h80deb1fe;
constant_k[14]<= 32'h9bdc06a7;
constant_k[15]<= 32'hc19bf174;
constant_k[16]<= 32'he49b69c1;
constant_k[17]<= 32'hefbe4786;
constant_k[18]<= 32'h0fc19dc6;
constant_k[19]<= 32'h240ca1cc;
constant_k[20]<= 32'h2de92c6f;
constant_k[21]<= 32'h4a7484aa;
constant_k[22]<= 32'h5cb0a9dc;
```

```
        constant_k[23]<= 32'h76f988da;
    constant_k[24]<= 32'h983e5152;
    constant_k[25]<= 32'ha831c66d;
    constant_k[26]<= 32'hb00327c8;
    constant_k[27]<= 32'hbf597fc7;
    constant_k[28]<= 32'hc6e00bf3;
    constant_k[29]<= 32'hd5a79147;
    constant_k[30]<= 32'h06ca6351;
        constant_k[31]<= 32'h14292967;
    constant_k[32]<= 32'h27b70a85;
    constant_k[33]<= 32'h2e1b2138;
    constant_k[34]<= 32'h4d2c6dfc;
    constant_k[35]<= 32'h53380d13;
    constant_k[36]<= 32'h650a7354;
    constant_k[37]<= 32'h766a0abb;
    constant_k[38]<= 32'h81c2c92e;
    constant_k[39]<= 32'h92722c85;
    constant_k[40]<= 32'ha2bfe8a1;
        constant_k[41]<= 32'ha81a664b;
    constant_k[42]<= 32'hc24b8b70;
    constant_k[43]<= 32'hc76c51a3;
    constant_k[44]<= 32'hd192e819;
    constant_k[45]<= 32'hd6990624;
    constant_k[46]<= 32'hf40e3585;
    constant_k[47]<= 32'h106aa070;
    constant_k[48]<= 32'h19a4c116;
    constant_k[49]<= 32'h1e376c08;
    constant_k[50]<= 32'h2748774c;
            constant_k[51]<= 32'h34b0bcb5;
    constant_k[52]<= 32'h391c0cb3;
```

```
constant_k[53]<= 32'h4ed8aa4a;
constant_k[54]<= 32'h5b9cca4f;
constant_k[55]<= 32'h682e6ff3;
constant_k[56]<= 32'h748f82ee;
constant_k[57]<= 32'h78a5636f;
constant_k[58]<= 32'h84c87814;
constant_k[59]<= 32'h8cc70208;
constant_k[60]<= 32'h90befffa;
constant_k[61]<= 32'ha4506ceb;
constant_k[62]<= 32'hbef9a3f7;
constant_k[63]<= 32'hc67178f2;
        #10;

        for(j=16;j<=63;j=j+1)
                begin
                        temp1= W[(j-2)*32+:32];
                        temp2= SmallSigma1(temp1);

                        temp3= W[(j-7)*32+:32];

                        temp4= W[(j-15)*32+:32];
                        temp5= SmallSigma0(temp4);

                        temp6= W[(j-16)*32+:32];

                        W[j*32 +: 32]= temp2 + temp3 + temp5 + temp6;
                end

    for(i=0;i<=63;i=i+1)
        begin
```

```
                $display("Iteration No. %d : a = %h, b = %h, c = %h, d = %h, e = %h, f = %h, g = %h, h
=%h \n",i,a,b,c,d,e,f,g,h);

                ss1=CapitalSigma1(e);

                ch=Ch(e,f,g);

                maj=Maj(a,b,c);

                ss0=CapitalSigma0(a);


                ct1= h+ss1+ch+ constant_k[i]+ W[i*32+:32];

                ct2= ss0+maj;


                #10;


                h=g;

                g=f;

                f=e;

                e=d+ct1;

                d=c;

                c=b;

                b=a;

                a=ct1+ct2;


                #10;
        end


        #10;


        constant_h[0]=a+constant_h[0];

        constant_h[1]=b+constant_h[1];

        constant_h[2]=c+constant_h[2];

        constant_h[3]=d+constant_h[3];
```

```
                constant_h[4]=e+constant_h[4];

                constant_h[5]=f+constant_h[5];

                constant_h[6]=g+constant_h[6];

                constant_h[7]=h+constant_h[7];


                out_data = {h[0],h[1],h[2],h[3],h[4],h[5],h[6],h[7]};


                $display("Iteration No. %d  : a = %h, b = %h, c = %h, d = %h, e = %h, f = %h, g = %h, h =%h\n",i,a,b,c,d,e,f,g,h);

                $display("Hashed Output:    : h[0] = %h, h[1] = %h, h[2] = %h, h[3] = %h, h[4] = %h, h[5] = %h, h[6] = %h, h[7]= %h\n",constant_h[0],constant_h[1],constant_h[2],constant_h[3],constant_h[4],constant_h[5],constant_h[6], constant_h[7]);

                $display("**********DONE**********\n");

                 end


                else

                        begin

                        out_data<=256'b0;

                        $display("Not ready to perform the HASH Function, Please provide reset as 1'b1\n");

                        end

end

endmodule
```

//

Test Bench:

```
module test;
reg clk,reset;
reg [255:0]input_data;

wire [255:0]out_data;

sha_256 block(input_data,out_data,clk,reset);
initial
clk = 1'b0;
always
#750 clk = ~clk;

initial
begin
reset = 1'b0;
input_data=255'b01100001_01100010_01100011_01100010_01100010_01100010_01100010_01100010_0
1100010_01100010_01100010_01100010_01100010_01100010_01100010_01100010_01100010_0110001
0_01100010_01100010_01100010_01100010_01100010_01100010_01100010_01100010_01100010_0110
0010_01100010_01100010_01100010_01100010;

#1500
reset <= 1'b1;
input_data=255'b01100001_01100010_01100011_01100100_01100101_01100110_01100111_01101000_0
1101001_01101010_01101011_01101100_01101101_01101110_01101111_01110000_01110001_0111001
0_01110011_01110100_01110101_01110110_01110111_01111000_01111001_01111010_01100001_0110
0010_01100011_01100100_01100101_01100110;

#1500
input_data=255'b01100001_01100010_01100011_01100010_01100010_01100010_01100010_01100010_0
1100010_01100010_01100010_01100010_01100010_01100010_01100010_01100010_01100010_0110001
0_01100010_01100010_01100010_01100010_01100010_01100010_01100010_01100010_01100010_0110
0010_01100010_01100010_01100010_01100010;

end

initial
#6750 $finish;

endmodule
```

Results: The complete code for SHA-256 has been implemented on questasim using system verilog and output has been for 256-random input given by user. For verification with real output , I have used an online website link as follows: https://www.movable type.co.uk/scripts/sha256.html , which generates the SHA-256 output for a message.

Screenshots: Wave-form is difficult to analyze, hence using display keyword , I have displayed all the iterations and final output and using Transcript it is easier to analyze the output.

1. **When reset is 0**

```
SIM 7> run -all
# Not ready to perform the HASH Function, Please provide reset as 1'b1
#
```

As per code, only when reset is 1 it can compute the hash function.

2. **Now reset=1, and with input of 256 bit binary of "abcdefghijklmnopqrstuvwxyzabcdef"**

```
# Padded Message is = 6162636465666768696a6b6c6d6e6f707172737475767778797a6162636465668000000000000000000000000000000000000000000000000000000000000000000000000000000100
#
#
# Iteration No.          0 : a = 6a09e667, b = bb67ae85, c = 3c6ef372, d = a54ff53a, e = 510e527f, f = 9b05688c, g = 1f83d9ab, h =5be0cd19
#
# Iteration No.          1 : a = 5d6aebb1, b = 6a09e667, c = bb67ae85, d = 3c6ef372, e = fa2a4606, f = 510e527f, g = 9b05688c, h =1f83d9ab
#
# Iteration No.          2 : a = 323062d2, b = 5d6aebb1, c = 6a09e667, d = bb67ae85, e = 51b4d2d1, f = fa2a4606, g = 510e527f, h =9b05688c
#
# Iteration No.          3 : a = a5204460, b = 323062d2, c = 5d6aebb1, d = 6a09e667, e = 8ac84df3, f = 51b4d2d1, g = fa2a4606, h =510e527f
#
# Iteration No.          4 : a = edce7fe2, b = a5204460, c = 323062d2, d = 5d6aebb1, e = 975b48cb, f = 8ac84df3, g = 51b4d2d1, h =fa2a4606
#
# Iteration No.          5 : a = 25281b47, b = edce7fe2, c = a5204460, d = 323062d2, e = 5fd725da, f = 975b48cb, g = 8ac84df3, h =51b4d2d1
#
# Iteration No.          6 : a = 4a6482e8, b = 25281b47, c = edce7fe2, d = a5204460, e = 244e5353, f = 5fd725da, g = 975b48cb, h =8ac84df3
#
# Iteration No.          7 : a = 34f24381, b = 4a6482e8, c = 25281b47, d = edce7fe2, e = d4d59948, f = 244e5353, g = 5fd725da, h =975b48cb
#
# Iteration No.          8 : a = d242e2f6, b = 34f24381, c = 4a6482e8, d = 25281b47, e = 03762b76, f = d4d59948, g = 244e5353, h =5fd725da
#
# Iteration No.          9 : a = e523ebdf, b = d242e2f6, c = 34f24381, d = 4a6482e8, e = 0f3b5263, f = 03762b76, g = d4d59948, h =244e5353
#
# Iteration No.         10 : a = 853805b5, b = e523ebdf, c = d242e2f6, d = 34f24381, e = b320f84a, f = 0f3b5263, g = 03762b76, h =d4d59948
#
# Iteration No.         11 : a = 227c17d3, b = 853805b5, c = e523ebdf, d = d242e2f6, e = e55678a4, f = b320f84a, g = 0f3b5263, h =03762b76
#
# Iteration No.         12 : a = 5b73274f, b = 227c17d3, c = 853805b5, d = e523ebdf, e = 0224a7d1, f = e55678a4, g = b320f84a, h =0f3b5263
#
# Iteration No.         13 : a = 032c9de9, b = 5b73274f, c = 227c17d3, d = 853805b5, e = c49d52ca, f = 0224a7d1, g = e55678a4, h =b320f84a
#
# Iteration No.         14 : a = b39a0a8c, b = 032c9de9, c = 5b73274f, d = 227c17d3, e = 17615e64, f = c49d52ca, g = 0224a7d1, h =e55678a4
#
# Iteration No.         15 : a = 958c0aff, b = b39a0a8c, c = 032c9de9, d = 5b73274f, e = 9424e648, f = 17615e64, g = c49d52ca, h =0224a7d1
#
# Iteration No.         16 : a = 27eb7fcc, b = 958c0aff, c = b39a0a8c, d = 032c9de9, e = 6d1e4ba5, f = 9424e648, g = 17615e64, h =c49d52ca
#
# Iteration No.         17 : a = e6e772fd, b = 27eb7fcc, c = 958c0aff, d = b39a0a8c, e = d82535e3, f = 6d1e4ba5, g = 9424e648, h =17615e64
#
# Iteration No.         18 : a = 455d4d95, b = e6e772fd, c = 27eb7fcc, d = 958c0aff, e = dd6ac105, f = d82535e3, g = 6d1e4ba5, h =9424e648
#
# Iteration No.         19 : a = a17677a2, b = 455d4d95, c = e6e772fd, d = 27eb7fcc, e = 8647d62a, f = dd6ac105, g = d82535e3, h =6d1e4ba5
#
# Iteration No.         20 : a = 7c9ef374, b = a17677a2, c = 455d4d95, d = e6e772fd, e = f27cdead, f = 8647d62a, g = dd6ac105, h =d82535e3
#
# Iteration No.         21 : a = 38ab2658, b = 7c9ef374, c = a17677a2, d = 455d4d95, e = baea97c9, f = f27cdead, g = 8647d62a, h =dd6ac105
#
```

```
# Iteration No.          22 : a = 9b0b83fe, b = 38ab2658, c = 7c9ef374, d = a17677a2, e = 1737edf6, f = baea97c9, g = f27cdead, h =8647d62a
#
# Iteration No.          23 : a = 168207d4, b = 9b0b83fe, c = 38ab2658, d = 7c9ef374, e = e833192b, f = 1737edf6, g = baea97c9, h =f27cdead
#
# Iteration No.          24 : a = 6f003834, b = 168207d4, c = 9b0b83fe, d = 38ab2658, e = 9df4be0d, f = e833192b, g = 1737edf6, h =baea97c9
#
# Iteration No.          25 : a = 94f7b05b, b = 6f003834, c = 168207d4, d = 9b0b83fe, e = d41d2b0f, f = 9df4be0d, g = e833192b, h =1737edf6
#
# Iteration No.          26 : a = e571baf0, b = 94f7b05b, c = 6f003834, d = 168207d4, e = b0dae8a2, f = d41d2b0f, g = 9df4be0d, h =e833192b
#
# Iteration No.          27 : a = a8a2fd32, b = e571baf0, c = 94f7b05b, d = 6f003834, e = b182c5f2, f = b0dae8a2, g = d41d2b0f, h =9df4be0d
#
# Iteration No.          28 : a = 59dfc706, b = a8a2fd32, c = e571baf0, d = 94f7b05b, e = 5ba315cf, f = b182c5f2, g = b0dae8a2, h =d41d2b0f
#
# Iteration No.          29 : a = d33357e1, b = 59dfc706, c = a8a2fd32, d = e571baf0, e = acdde2b2, f = 5ba315cf, g = b182c5f2, h =b0dae8a2
#
# Iteration No.          30 : a = ae399d58, b = d33357e1, c = 59dfc706, d = a8a2fd32, e = b359b5f8, f = acdde2b2, g = 5ba315cf, h =b182c5f2
#
# Iteration No.          31 : a = 51e3266e, b = ae399d58, c = d33357e1, d = 59dfc706, e = f80bd83e, f = b359b5f8, g = acdde2b2, h =5ba315cf
#
# Iteration No.          32 : a = 3ea8b554, b = 51e3266e, c = ae399d58, d = d33357e1, e = 99c1652d, f = f80bd83e, g = b359b5f8, h =acdde2b2
#
# Iteration No.          33 : a = c532de9c, b = 3ea8b554, c = 51e3266e, d = ae399d58, e = 51ddf837, f = 99c1652d, g = f80bd83e, h =b359b5f8
#
# Iteration No.          34 : a = 303f50db, b = c532de9c, c = 3ea8b554, d = 51e3266e, e = 7a054ab2, f = 51ddf837, g = 99c1652d, h =f80bd83e
#
# Iteration No.          35 : a = 4160f897, b = 303f50db, c = c532de9c, d = 3ea8b554, e = a774111d, f = 7a054ab2, g = 51ddf837, h =99c1652d
#
# Iteration No.          36 : a = 2412aac4, b = 4160f897, c = 303f50db, d = c532de9c, e = 8a881f52, f = a774111d, g = 7a054ab2, h =51ddf837
#
# Iteration No.          37 : a = 8d6201c3, b = 2412aac4, c = 4160f897, d = 303f50db, e = 1cd34cd4, f = 8a881f52, g = a774111d, h =7a054ab2
#
# Iteration No.          38 : a = 61d7400e, b = 8d6201c3, c = 2412aac4, d = 4160f897, e = 277002cd, f = 1cd34cd4, g = 8a881f52, h =a774111d
#
# Iteration No.          39 : a = 471f4d1c, b = 61d7400e, c = 8d6201c3, d = 2412aac4, e = 9e275daf, f = 277002cd, g = 1cd34cd4, h =8a881f52
#
# Iteration No.          40 : a = a74aafac, b = 471f4d1c, c = 61d7400e, d = 8d6201c3, e = 81f47ec1, f = 9e275daf, g = 277002cd, h =1cd34cd4
#
# Iteration No.          41 : a = fc570714, b = a74aafac, c = 471f4d1c, d = 61d7400e, e = a45098a8, f = 81f47ec1, g = 9e275daf, h =277002cd
#
# Iteration No.          42 : a = 9f52b8be, b = fc570714, c = a74aafac, d = 471f4d1c, e = be1c7924, f = a45098a8, g = 81f47ec1, h =9e275daf
#
# Iteration No.          43 : a = 6d524508, b = 9f52b8be, c = fc570714, d = a74aafac, e = cc5c33a1, f = be1c7924, g = a45098a8, h =81f47ec1
#
# Iteration No.          44 : a = cdfb9aa3, b = 6d524508, c = 9f52b8be, d = fc570714, e = fdf06ace, f = cc5c33a1, g = be1c7924, h =a45098a8
#
# Iteration No.          45 : a = 76c3d9db, b = cdfb9aa3, c = 6d524508, d = 9f52b8be, e = ddbe4202, f = fdf06ace, g = cc5c33a1, h =be1c7924
```

```
# Iteration No.          46 : a = 2553dc0d, b = 76c3d9db, c = cdfb9aa3, d = 6d524508, e = 3ac68d8d, f = ddbe4202, g = fdf06ace, h =cc5c33a1
#
# Iteration No.          47 : a = e984dd3b, b = 2553dc0d, c = 76c3d9db, d = cdfb9aa3, e = 0ab560b0, f = 3ac68d8d, g = ddbe4202, h =fdf06ace
#
# Iteration No.          48 : a = 98df670e, b = e984dd3b, c = 2553dc0d, d = 76c3d9db, e = 004c8fc8, f = 0ab560b0, g = 3ac68d8d, h =ddbe4202
#
# Iteration No.          49 : a = bfb2ee33, b = 98df670e, c = e984dd3b, d = 2553dc0d, e = a8bfc5a4, f = 004c8fc8, g = 0ab560b0, h =3ac68d8d
#
# Iteration No.          50 : a = ddb05bf1, b = bfb2ee33, c = 98df670e, d = e984dd3b, e = f3a3bfde, f = a8bfc5a4, g = 004c8fc8, h =0ab560b0
#
# Iteration No.          51 : a = 3e569aa6, b = ddb05bf1, c = bfb2ee33, d = 98df670e, e = 209bcca6, f = f3a3bfde, g = a8bfc5a4, h =004c8fc8
#
# Iteration No.          52 : a = d0e46fdb, b = 3e569aa6, c = ddb05bf1, d = bfb2ee33, e = a9422f52, f = 209bcca6, g = f3a3bfde, h =a8bfc5a4
#
# Iteration No.          53 : a = 281c01d3, b = d0e46fdb, c = 3e569aa6, d = ddb05bf1, e = ef81a07d, f = a9422f52, g = 209bcca6, h =f3a3bfde
#
# Iteration No.          54 : a = b784d53f, b = 281c01d3, c = d0e46fdb, d = 3e569aa6, e = a8481929, f = ef81a07d, g = a9422f52, h =209bcca6
#
# Iteration No.          55 : a = 1e0d4c5a, b = b784d53f, c = 281c01d3, d = d0e46fdb, e = 5497296e, f = a8481929, g = ef81a07d, h =a9422f52
#
# Iteration No.          56 : a = cde77154, b = 1e0d4c5a, c = b784d53f, d = 281c01d3, e = 905cd0d0, f = 5497296e, g = a8481929, h =ef81a07d
#
# Iteration No.          57 : a = 5fd22714, b = cde77154, c = 1e0d4c5a, d = b784d53f, e = c44df330, f = 905cd0d0, g = 5497296e, h =a8481929
#
# Iteration No.          58 : a = 7f5bcf17, b = 5fd22714, c = cde77154, d = 1e0d4c5a, e = 6f4f18d7, f = c44df330, g = 905cd0d0, h =5497296e
#
# Iteration No.          59 : a = 5ef57a6b, b = 7f5bcf17, c = 5fd22714, d = cde77154, e = 54de0acb, f = 6f4f18d7, g = c44df330, h =905cd0d0
#
# Iteration No.          60 : a = d99631f1, b = 5ef57a6b, c = 7f5bcf17, d = 5fd22714, e = 769c2fe4, f = 54de0acb, g = 6f4f18d7, h =c44df330
#
# Iteration No.          61 : a = 32524edd, b = d99631f1, c = 5ef57a6b, d = 7f5bcf17, e = 912072d3, f = 769c2fe4, g = 54de0acb, h =6f4f18d7
#
# Iteration No.          62 : a = cf578691, b = 32524edd, c = d99631f1, d = 5ef57a6b, e = 809664c3, f = 912072d3, g = 769c2fe4, h =54de0acb
#
# Iteration No.          63 : a = 2571a8d4, b = cf578691, c = 32524edd, d = d99631f1, e = 8fcf4049, f = 809664c3, g = 912072d3, h =769c2fe4
#
# Iteration No.          64  : a = b666f8bc, b = 2571a8d4, c = cf578691, d = 32524edd, e = df4b8aab, f = 8fcf4049, g = 809664c3, h =912072d3
#
# Hashed Output:    : h[0] = 2070df23, h[1] = e0d95759, h[2] = 0bc67a03, h[3] = d7a24417, h[4] = 3059dd2a, h[5] = 2ad4a8d5, h[6] = a01a3e6e, h[7]= ed013fec
#
# **********DONE**********
```

The output hash function for given input is shown as h[0] to h[7]:

Hashed Output: : h[0] = 2070df23, h[1] = e0d95759, h[2] = 0bc67a03, h[3] = d7a24417, h[4] = 3059dd2a, h[5] = 2ad4a8d5, h[6] = a01a3e6e, h[7]= ed013fec

Now using e-tool:

Enter any message to check its SHA-256 hash

Message abcdefghijklmnopqrstuvwxyzabcdef

Hash 2070df23e0d957590bc67a03d7a244173059dd2a2ad4a8d5a01a3e6eed013fec 0.890ms

Note SHA-256 hash of 'abc' should be: ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad

Hence output has been verified.

3. Now reset=1 and input as 256 binary conversion of "abcbbbbbbbbbbbbbbbbbbbbbbbbbbbbb"

```
# Padded Message is = 61626362626262626262626262626262626262626262626262626262626262628000000000000000000000000000000000000000000000000000000000000100
#
#
# Iteration No.          0 : a = 6a09e667, b = bb67ae85, c = 3c6ef372, d = a54ff53a, e = 510e527f, f = 9b05688c, g = 1f83d9ab, h =5be0cd19
#
# Iteration No.          1 : a = 5d6aebaf, b = 6a09e667, c = bb67ae85, d = 3c6ef372, e = fa2a4604, f = 510e527f, g = 9b05688c, h =1f83d9ab
#
# Iteration No.          2 : a = a77cb4c7, b = 5d6aebaf, c = 6a09e667, d = bb67ae85, e = 46f0ccc9, f = fa2a4604, g = 510e527f, h =9b05688c
#
# Iteration No.          3 : a = f74685ac, b = a77cb4c7, c = 5d6aebaf, d = 6a09e667, e = 86144501, f = 46f0ccc9, g = fa2a4604, h =510e527f
#
# Iteration No.          4 : a = c97a381b, b = f74685ac, c = a77cb4c7, d = 5d6aebaf, e = 3174d051, f = 86144501, g = 46f0ccc9, h =fa2a4604
#
# Iteration No.          5 : a = 92e2ec0e, b = c97a381b, c = f74685ac, d = a77cb4c7, e = 2e6e783c, f = 3174d051, g = 86144501, h =46f0ccc9
#
# Iteration No.          6 : a = 8697c2d2, b = 92e2ec0e, c = c97a381b, d = f74685ac, e = 0b35b52c, f = 2e6e783c, g = 3174d051, h =86144501
#
# Iteration No.          7 : a = afbf3715, b = 8697c2d2, c = 92e2ec0e, d = c97a381b, e = 3bd84697, f = 0b35b52c, g = 2e6e783c, h =3174d051
#
# Iteration No.          8 : a = 66abebdb, b = afbf3715, c = 8697c2d2, d = 92e2ec0e, e = 79cf575e, f = 3bd84697, g = 0b35b52c, h =2e6e783c
#
# Iteration No.          9 : a = 07913a9b, b = 66abebdb, c = afbf3715, d = 8697c2d2, e = cad5a0a3, f = 79cf575e, g = 3bd84697, h =0b35b52c
#
# Iteration No.         10 : a = 029a0de2, b = 07913a9b, c = 66abebdb, d = afbf3715, e = 0fa076e8, f = cad5a0a3, g = 79cf575e, h =3bd84697
#
# Iteration No.         11 : a = 15f93b5a, b = 029a0de2, c = 07913a9b, d = 66abebdb, e = 379c26f2, f = 0fa076e8, g = cad5a0a3, h =79cf575e
#
# Iteration No.         12 : a = 3a063b28, b = 15f93b5a, c = 029a0de2, d = 07913a9b, e = ddd561e1, f = 379c26f2, g = 0fa076e8, h =cad5a0a3
#
# Iteration No.         13 : a = 890b8e41, b = 3a063b28, c = 15f93b5a, d = 029a0de2, e = aed58f5f, f = ddd561e1, g = 379c26f2, h =0fa076e8
#
# Iteration No.         14 : a = 85685752, b = 890b8e41, c = 3a063b28, d = 15f93b5a, e = 307f7c04, f = aed58f5f, g = ddd561e1, h =379c26f2
#
# Iteration No.         15 : a = b4e4bf48, b = 85685752, c = 890b8e41, d = 3a063b28, e = 874066df, f = 307f7c04, g = aed58f5f, h =ddd561e1
#
# Iteration No.         16 : a = 99101111, b = b4e4bf48, c = 85685752, d = 890b8e41, e = 082c02d5, f = 874066df, g = 307f7c04, h =aed58f5f
#
# Iteration No.         17 : a = d1a46c66, b = 99101111, c = b4e4bf48, d = 85685752, e = 16c358b7, f = 082c02d5, g = 874066df, h =307f7c04
#
# Iteration No.         18 : a = d7f83617, b = d1a46c66, c = 99101111, d = b4e4bf48, e = 84ce42ad, f = 16c358b7, g = 082c02d5, h =874066df
#
# Iteration No.         19 : a = ca1e2149, b = d7f83617, c = d1a46c66, d = 99101111, e = 07b9bf5f, f = 84ce42ad, g = 16c358b7, h =082c02d5
#
# Iteration No.         20 : a = 89fc0752, b = ca1e2149, c = d7f83617, d = d1a46c66, e = 4f02f491, f = 07b9bf5f, g = 84ce42ad, h =16c358b7
#
# Iteration No.         21 : a = 65092770, b = 89fc0752, c = ca1e2149, d = d7f83617, e = 01bb6870, f = 4f02f491, g = 07b9bf5f, h =84ce42ad
#
```

```
# Iteration No.          22 : a = 45279d56, b = 65092770, c = 89fc0752, d = cale2149, e = 4da70c1c, f = 01bb6870, g = 4f02f491, h =07b9bf5f
#
# Iteration No.          23 : a = 338867b9, b = 45279d56, c = 65092770, d = 89fc0752, e = d2eaea33, f = 4da70c1c, g = 01bb6870, h =4f02f491
#
# Iteration No.          24 : a = bb634c9e, b = 338867b9, c = 45279d56, d = 65092770, e = 8fa0cb1d, f = d2eaea33, g = 4da70c1c, h =01bb6870
#
# Iteration No.          25 : a = d7ea6607, b = bb634c9e, c = 338867b9, d = 45279d56, e = c2b0cd09, f = 8fa0cb1d, g = d2eaea33, h =4da70c1c
#
# Iteration No.          26 : a = e0712136, b = d7ea6607, c = bb634c9e, d = 338867b9, e = 05521e60, f = c2b0cd09, g = 8fa0cb1d, h =d2eaea33
#
# Iteration No.          27 : a = 7ab93fba, b = e0712136, c = d7ea6607, d = bb634c9e, e = 45aeb318, f = 05521e60, g = c2b0cd09, h =8fa0cb1d
#
# Iteration No.          28 : a = 418307a3, b = 7ab93fba, c = e0712136, d = d7ea6607, e = 8269b93e, f = 45aeb318, g = 05521e60, h =c2b0cd09
#
# Iteration No.          29 : a = 23de59ce, b = 418307a3, c = 7ab93fba, d = e0712136, e = b9b3572d, f = 8269b93e, g = 45aeb318, h =05521e60
#
# Iteration No.          30 : a = b57ae0eb, b = 23de59ce, c = 418307a3, d = 7ab93fba, e = f26f3269, f = b9b3572d, g = 8269b93e, h =45aeb318
#
# Iteration No.          31 : a = 0b0909f5, b = b57ae0eb, c = 23de59ce, d = 418307a3, e = 62674a8c, f = f26f3269, g = b9b3572d, h =8269b93e
#
# Iteration No.          32 : a = 86c42d75, b = 0b0909f5, c = b57ae0eb, d = 23de59ce, e = 7b9f1d10, f = 62674a8c, g = f26f3269, h =b9b3572d
#
# Iteration No.          33 : a = 2814043c, b = 86c42d75, c = 0b0909f5, d = b57ae0eb, e = aa0148ae, f = 7b9f1d10, g = 62674a8c, h =f26f3269
#
# Iteration No.          34 : a = 13006486, b = 2814043c, c = 86c42d75, d = 0b0909f5, e = 428286ed, f = aa0148ae, g = 7b9f1d10, h =62674a8c
#
# Iteration No.          35 : a = 2cf493bf, b = 13006486, c = 2814043c, d = 86c42d75, e = 9496e012, f = 428286ed, g = aa0148ae, h =7b9f1d10
#
# Iteration No.          36 : a = f9e64ab6, b = 2cf493bf, c = 13006486, d = 2814043c, e = d40bb375, f = 9496e012, g = 428286ed, h =aa0148ae
#
# Iteration No.          37 : a = b09d512e, b = f9e64ab6, c = 2cf493bf, d = 13006486, e = 2be88c3c, f = d40bb375, g = 9496e012, h =428286ed
#
# Iteration No.          38 : a = 0fdd13e4, b = b09d512e, c = f9e64ab6, d = 2cf493bf, e = 19d2ba49, f = 2be88c3c, g = d40bb375, h =9496e012
#
# Iteration No.          39 : a = c5129314, b = 0fdd13e4, c = b09d512e, d = f9e64ab6, e = 4f9128ff, f = 19d2ba49, g = 2be88c3c, h =d40bb375
#
# Iteration No.          40 : a = 787bfa45, b = c5129314, c = 0fdd13e4, d = b09d512e, e = 09165292, f = 4f9128ff, g = 19d2ba49, h =2be88c3c
#
# Iteration No.          41 : a = 12d9dd8e, b = 787bfa45, c = c5129314, d = 0fdd13e4, e = 123f72c9, f = 09165292, g = 4f9128ff, h =19d2ba49
#
# Iteration No.          42 : a = 4b2962cf, b = 12d9dd8e, c = 787bfa45, d = c5129314, e = faf9c1c9, f = 123f72c9, g = 09165292, h =4f9128ff
#
# Iteration No.          43 : a = 3b0e2b77, b = 4b2962cf, c = 12d9dd8e, d = 787bfa45, e = 446b86e8, f = faf9c1c9, g = 123f72c9, h =09165292
#
# Iteration No.          44 : a = 6e12a349, b = 3b0e2b77, c = 4b2962cf, d = 12d9dd8e, e = 1dada37f, f = 446b86e8, g = faf9c1c9, h =123f72c9
#
# Iteration No.          45 : a = 3e00f525, b = 6e12a349, c = 3b0e2b77, d = 4b2962cf, e = da8db165, f = 1dada37f, g = 446b86e8, h =faf9c1c9
```

```
# Iteration No.          46 : a = 48ac963d, b = 3e00f525, c = 6e12a349, d = 3b0e2b77, e = 7055fbf1, f = da8db165, g = 1dada37f, h =446b86e8
#
# Iteration No.          47 : a = 9cceb1bf, b = 48ac963d, c = 3e00f525, d = 6e12a349, e = 18429040, f = 7055fbf1, g = da8db165, h =1dada37f
#
# Iteration No.          48 : a = 497427c2, b = 9cceb1bf, c = 48ac963d, d = 3e00f525, e = 4af06165, f = 18429040, g = 7055fbf1, h =da8db165
#
# Iteration No.          49 : a = 668087ad, b = 497427c2, c = 9cceb1bf, d = 48ac963d, e = dec4799f, f = 4af06165, g = 18429040, h =7055fbf1
#
# Iteration No.          50 : a = 93670a57, b = 668087ad, c = 497427c2, d = 9cceb1bf, e = 28795870, f = dec4799f, g = 4af06165, h =18429040
#
# Iteration No.          51 : a = 5c2dae2f, b = 93670a57, c = 668087ad, d = 497427c2, e = 8b4c5047, f = 28795870, g = dec4799f, h =4af06165
#
# Iteration No.          52 : a = 2fbef31c, b = 5c2dae2f, c = 93670a57, d = 668087ad, e = 12445519, f = 8b4c5047, g = 28795870, h =dec4799f
#
# Iteration No.          53 : a = 03fa4ffe, b = 2fbef31c, c = 5c2dae2f, d = 93670a57, e = e2887bfe, f = 12445519, g = 8b4c5047, h =28795870
#
# Iteration No.          54 : a = d552d022, b = 03fa4ffe, c = 2fbef31c, d = 5c2dae2f, e = 42c97719, f = e2887bfe, g = 12445519, h =8b4c5047
#
# Iteration No.          55 : a = cf303f24, b = d552d022, c = 03fa4ffe, d = 2fbef31c, e = a460844a, f = 42c97719, g = e2887bfe, h =12445519
#
# Iteration No.          56 : a = 165e6f4c, b = cf303f24, c = d552d022, d = 03fa4ffe, e = 74941dce, f = a460844a, g = 42c97719, h =e2887bfe
#
# Iteration No.          57 : a = 10c5c0eb, b = 165e6f4c, c = cf303f24, d = d552d022, e = 3723784c, f = 74941dce, g = a460844a, h =42c97719
#
# Iteration No.          58 : a = a56a6eaf, b = 10c5c0eb, c = 165e6f4c, d = cf303f24, e = 8ffe750e, f = 3723784c, g = 74941dce, h =a460844a
#
# Iteration No.          59 : a = 4dcdf8bf, b = a56a6eaf, c = 10c5c0eb, d = 165e6f4c, e = d312ba87, f = 8ffe750e, g = 3723784c, h =74941dce
#
# Iteration No.          60 : a = 7c4ce3e7, b = 4dcdf8bf, c = a56a6eaf, d = 10c5c0eb, e = 6b717d0d, f = d312ba87, g = 8ffe750e, h =3723784c
#
# Iteration No.          61 : a = 9c2ea75f, b = 7c4ce3e7, c = 4dcdf8bf, d = a56a6eaf, e = 4c00362c, f = 6b717d0d, g = d312ba87, h =8ffe750e
#
# Iteration No.          62 : a = e26a784c, b = 9c2ea75f, c = 7c4ce3e7, d = 4dcdf8bf, e = c41dcc2a, f = 4c00362c, g = 6b717d0d, h =d312ba87
#
# Iteration No.          63 : a = 0176b4bc, b = e26a784c, c = 9c2ea75f, d = 7c4ce3e7, e = ffb90b63, f = c41dcc2a, g = 4c00362c, h =6b717d0d
#
# Iteration No.          64  : a = 8e3d313a, b = 0176b4bc, c = e26a784c, d = 9c2ea75f, e = 0aac0a26, f = ffb90b63, g = c41dcc2a, h =4c00362c
#
# Hashed Output:    : h[0] = f84717a1, h[1] = bcde6341, h[2] = 1ed96bbe, h[3] = 417e9c99, h[4] = 5bba5ca5, h[5] = 9abe73ef, h[6] = e3a1a5d5, h[7]= a7e10345
#
# **********DONE**********
#
```

The output hash function for given input is shown as h[0] to h[7]:

Hashed Output: : h[0] = f84717a1, h[1] = bcde6341, h[2] = 1ed96bbe, h[3] = 417e9c99, h[4] = 5bba5ca5, h[5] = 9abe73ef, h[6] = e3a1a5d5, h[7]= a7e10345

Now using e-tool:

Hence again the output has been verified.

Remarks(if any): Implemented the SHA-256 code , and now I'll plan to implement TMDS 8b/10b in a week or two.