always @(posedge clk)

begin

If(reset==1'b1)

begin

m0[7:0] = msg[7:0];

m1[7:0] = msg[15:8];0

m2[7:0] = msg[23:16];

m3[7:0] = msg[31:24];

Sh[0] = H[0]^ m0[0]^m0[1]^m0[2]^m0[3]^m0[4]^m0[5]^m0[6]^m0[7];

Sh[1] = H[1]^ m1[0]^m1[1]^m1[2]^m1[3]^m1[4]^m1[5]^m1[6]^m1[7];

Sh[2] = H[2]^ m2[0]^m2[1]^m2[2]^m2[3]^m2[4]^m2[5]^m2[6]^m2[7];

Sh[3] = H[3]^ m3[0]^m3[1]^m3[2]^m3[3]^m3[4]^m3[5]^m3[6]^m3[7];

Sv[0] = V[0]^m0[0]^m1[0]^m2[0]^m3[0];

Sv[1] = V[1]^m0[1]^m1[1]^m2[1]^m3[1];

Sv[2] = V[2]^m0[2]^m1[2]^m2[2]^m3[2];

Sv[3] = V[3]^m0[3]^m1[3]^m2[3]^m3[3];

Sv[4] = V[4]^m0[4]^m1[4]^m2[4]^m3[4];

Sv[5] = V[5]^m0[5]^m1[5]^m2[5]^m3[5];

Sv[6] = V[6]^m0[6]^m1[6]^m2[6]^m3[6];

Sv[7] = V[7]^m0[7]^m1[7]^m2[7]^m3[7];

Hm1[0] = m1[0]^m0[1]^m1[4]^m2[3]^m3[6];

Hm1[1] = m1[0]^m0[5]^m1[4]^m3[2]^m3[6];

Hm1[2] = m0[1]^m0[5]^m1[4]^m2[7];

Hm1[3] = m2[3]^m3[2]^m3[6]^m2[7];

Hm2[0] = m2[0]^m1[1]^m0[6]^m1[5]^m3[3];

Hm2[1] = m2[0]^m0[2]^m0[6]^m2[4]^m3[3];

Hm2[2] = m1[1]^m0[2]^m0[6]^m3[7];

Hm2[3] = m1[5]^m2[4]^m3[3]^m3[7];

Hm3[0] = m0[0]^m0[4]^m2[2]^m3[1]^m2[6];

Hm3[1] = m0[0]^m1[3]^m2[2]^m3[5]^m2[6];

Hm3[2] = m0[4]^m1[3]^m0[6]^m3[7];

Hm3[3] = m3[1]^m2[5]^m2[6]^m1[7];

Hm4[0] = m0[3]^m1[2]^m3[0]^m3[4]^m1[6];

Hm4[1] = m0[3]^m2[1]^m3[0]^m2[5]^m1[6];

Hm4[2] = m1[2]^m2[1]^m3[0]^m0[7];

Hm4[3] = m3[4]^m2[5]^m1[6]^m3[7];