Software: MATLAB 10.0

% Main Program and saved as finalout.m

clc;

clear all;

% Plaintext

plaintext=[0 0 0 0;0 0 0 0;0 0 0 0;0 0 0 13];

% Key Input

key0=[26 135 183 147;12 84 8 12;36 147 14 83;242 188 67 13];

% Round0

round0\_out=ARK(plaintext,key0);

% Round1

bs=BS(round0\_out);

sr=SR(bs);

mc=MC(sr);

round1\_out=ARK(mc,KS(1));

% Round2

bs=BS(round1\_out);

sr=SR(bs);

mc=MC(sr);

round2\_out=ARK(mc,KS(2));

% Round3

bs=BS(round2\_out);

sr=SR(bs);

mc=MC(sr);

round3\_out=ARK(mc,KS(3));

% Round4

bs=BS(round3\_out);

sr=SR(bs);

mc=MC(sr);

round4\_out=ARK(mc,KS(4));

% Round5

bs=BS(round4\_out);

sr=SR(bs);

mc=MC(sr);

round5\_out=ARK(mc,KS(5));

% Round6

bs=BS(round5\_out);

sr=SR(bs);

mc=MC(sr);

round6\_out=ARK(mc,KS(6));

% Round7

bs=BS(round6\_out);

sr=SR(bs);

mc=MC(sr);

round7\_out=ARK(mc,KS(7));

% Round8

bs=BS(round7\_out);

sr=SR(bs);

mc=MC(sr);

round8\_out=ARK(mc,KS(8));

% Round9

bs=BS(round8\_out);

sr=SR(bs);

mc=MC(sr);

round9\_out=ARK(mc,KS(9));

% Round10

bs=BS(round9\_out);

sr=SR(bs);

mc=sr;

round10\_out=ARK(mc,KS(10));

% Output

clc;

disp('Name: Ravi Kiran Reddy Medhisetty');

disp('Roll No: 103735458');

disp('Plaintext is as follows');

disp(dec2hex(plaintext));

disp('Key is as follows');

disp(dec2hex(key0));

disp('The following are the outputs of each round by giving desired plaintext and key as an input:');

disp('ROUND-0');

disp(dec2hex(round0\_out));

disp('ROUND-1');

disp(dec2hex(round1\_out));

disp('ROUND-2');

disp(dec2hex(round2\_out));

disp('ROUND-3');

disp(dec2hex(round3\_out));

disp('ROUND-4');

disp(dec2hex(round4\_out));

disp('ROUND-5');

disp(dec2hex(round5\_out));

disp('ROUND-6');

disp(dec2hex(round6\_out));

disp('ROUND-7');

disp(dec2hex(round7\_out));

disp('ROUND-8');

disp(dec2hex(round8\_out));

disp('ROUND-9');

disp(dec2hex(round9\_out));

disp('ROUND-10');

disp(dec2hex(round10\_out));

% ARK Function and save as ARK.m

function [ ark ] = ARK( c,d )

%UNTITLED8 Summary of this function goes here

% Detailed explanation goes here

ark=bitxor(c,d);

end

% Function BS and save as BS.m

function [ bs ] = BS( round\_temp )

%UNTITLED3 Summary of this function goes here

% Detailed explanation goes here

bs=ones(4,4);

for i=1:4

for j=1:4

c=round\_temp(i,j);

d=bitand(c,15);

e=bitshift(c,-4);

e=e+1;

d=d+1;

f=s\_box(e,d);

bs(i,j)=f;

end

end

end

% Function KS and save as KS.m

function [ roundout ] = KS( roundin )

%UNTITLED Summary of this function goes here

% Detailed explanation goes here

% Key Schedule

a=ones(16,16);

a(1,1)=99;

a(1,2)=124;

a(1,3)=119;

a(1,4)=123;

a(1,5)=242;

a(1,6)=107;

a(1,7)=111;

a(1,8)=197;

a(1,9)=48;

a(1,10)=1;

a(1,11)=103;

a(1,12)=43;

a(1,13)=254;

a(1,14)=215;

a(1,15)=171;

a(1,16)=118;

a(2,1)=202;

a(2,2)=130;

a(2,3)=201;

a(2,4)=125;

a(2,5)=250;

a(2,6)=89;

a(2,7)=71;

a(2,8)=240;

a(2,9)=173;

a(2,10)=212;

a(2,11)=162;

a(2,12)=175;

a(2,13)=156;

a(2,14)=164;

a(2,15)=114;

a(2,16)=192;

a(3,1)=183;

a(3,2)=253;

a(3,3)=147;

a(3,4)=38;

a(3,5)=54;

a(3,6)=63;

a(3,7)=247;

a(3,8)=204;

a(3,9)=52;

a(3,10)=165;

a(3,11)=229;

a(3,12)=241;

a(3,13)=113;

a(3,14)=216;

a(3,15)=49;

a(3,16)=21;

a(4,1)=4;

a(4,2)=199;

a(4,3)=35;

a(4,4)=195;

a(4,5)=24;

a(4,6)=150;

a(4,7)=5;

a(4,8)=154;

a(4,9)=7;

a(4,10)=18;

a(4,11)=128;

a(4,12)=226;

a(4,13)=235;

a(4,14)=39;

a(4,15)=178;

a(4,16)=117;

a(5,1)=9;

a(5,2)=131;

a(5,3)=44;

a(5,4)=26;

a(5,5)=27;

a(5,6)=110;

a(5,7)=90;

a(5,8)=160;

a(5,9)=82;

a(5,10)=59;

a(5,11)=214;

a(5,12)=179;

a(5,13)=41;

a(5,14)=227;

a(5,15)=47;

a(5,16)=132;

a(6,1)=83;

a(6,2)=209;

a(6,3)=0;

a(6,4)=237;

a(6,5)=32;

a(6,6)=252;

a(6,7)=177;

a(6,8)=91;

a(6,9)=106;

a(6,10)=203;

a(6,11)=190;

a(6,12)=57;

a(6,13)=74;

a(6,14)=76;

a(6,15)=88;

a(6,16)=207;

a(7,1)=208;

a(7,2)=239;

a(7,3)=170;

a(7,4)=251;

a(7,5)=67;

a(7,6)=77;

a(7,7)=51;

a(7,8)=133;

a(7,9)=69;

a(7,10)=249;

a(7,11)=2;

a(7,12)=127;

a(7,13)=80;

a(7,14)=60;

a(7,15)=159;

a(7,16)=168;

a(8,1)=81;

a(8,2)=163;

a(8,3)=64;

a(8,4)=143;

a(8,5)=146;

a(8,6)=157;

a(8,7)=56;

a(8,8)=245;

a(8,9)=188;

a(8,10)=182;

a(8,11)=218;

a(8,12)=33;

a(8,13)=16;

a(8,14)=255;

a(8,15)=243;

a(8,16)=210;

a(9,1)=205;

a(9,2)=12;

a(9,3)=19;

a(9,4)=236;

a(9,5)=95;

a(9,6)=151;

a(9,7)=68;

a(9,8)=23;

a(9,9)=196;

a(9,10)=167;

a(9,11)=126;

a(9,12)=61;

a(9,13)=100;

a(9,14)=93;

a(9,15)=25;

a(9,16)=115;

a(10,1)=96;

a(10,2)=129;

a(10,3)=79;

a(10,4)=220;

a(10,5)=34;

a(10,6)=42;

a(10,7)=144;

a(10,8)=136;

a(10,9)=70;

a(10,10)=238;

a(10,11)=184;

a(10,12)=20;

a(10,13)=222;

a(10,14)=94;

a(10,15)=11;

a(10,16)=219;

a(11,1)=224;

a(11,2)=50;

a(11,3)=58;

a(11,4)=10;

a(11,5)=73;

a(11,6)=6;

a(11,7)=36;

a(11,8)=92;

a(11,9)=194;

a(11,10)=211;

a(11,11)=172;

a(11,12)=98;

a(11,13)=145;

a(11,14)=149;

a(11,15)=228;

a(11,16)=121;

a(12,1)=231;

a(12,2)=200;

a(12,3)=55;

a(12,4)=109;

a(12,5)=141;

a(12,6)=213;

a(12,7)=78;

a(12,8)=169;

a(12,9)=108;

a(12,10)=86;

a(12,11)=244;

a(12,12)=234;

a(12,13)=101;

a(12,14)=122;

a(12,15)=174;

a(12,16)=8;

a(13,1)=186;

a(13,2)=120;

a(13,3)=37;

a(13,4)=46;

a(13,5)=28;

a(13,6)=166;

a(13,7)=180;

a(13,8)=198;

a(13,9)=232;

a(13,10)=221;

a(13,11)=116;

a(13,12)=31;

a(13,13)=75;

a(13,14)=189;

a(13,15)=139;

a(13,16)=138;

a(14,1)=112;

a(14,2)=62;

a(14,3)=181;

a(14,4)=102;

a(14,5)=72;

a(14,6)=3;

a(14,7)=246;

a(14,8)=14;

a(14,9)=97;

a(14,10)=53;

a(14,11)=87;

a(14,12)=185;

a(14,13)=134;

a(14,14)=193;

a(14,15)=29;

a(14,16)=158;

a(15,1)=225;

a(15,2)=248;

a(15,3)=152;

a(15,4)=17;

a(15,5)=105;

a(15,6)=217;

a(15,7)=142;

a(15,8)=148;

a(15,9)=155;

a(15,10)=30;

a(15,11)=135;

a(15,12)=233;

a(15,13)=206;

a(15,14)=85;

a(15,15)=40;

a(15,16)=223;

a(16,1)=140;

a(16,2)=161;

a(16,3)=137;

a(16,4)=13;

a(16,5)=191;

a(16,6)=230;

a(16,7)=66;

a(16,8)=104;

a(16,9)=65;

a(16,10)=153;

a(16,11)=45;

a(16,12)=15;

a(16,13)=176;

a(16,14)=84;

a(16,15)=187;

a(16,16)=22;

temp=a(2,1);

a(2,1)=a(6,9);

a(6,9)=temp;

b=ones(10,1);

b(1,1)=hex2dec('01');

b(2,1)=hex2dec('02');

b(3,1)=hex2dec('04');

b(4,1)=hex2dec('08');

b(5,1)=hex2dec('10');

b(6,1)=hex2dec('20');

b(7,1)=hex2dec('40');

b(8,1)=hex2dec('80');

b(9,1)=hex2dec('1b');

b(10,1)=hex2dec('36');

round0=[26 135 183 147;12 84 8 12;36 147 14 83;242 188 67 13];

% W(0)

w\_0=ones(4,1);

for i=1:4

for j=1

w\_0(i,j)=round0(i,j);

end

end

% W(1)

w\_1=ones(4,1);

for i=1:4

for j=1

w\_1(i,j)=round0(i,j+1);

end

end

% W(2)

w\_2=ones(4,1);

for i=1:4

for j=1

w\_2(i,j)=round0(i,j+2);

end

end

% W(3)

w\_3=ones(4,1);

for i=1:4

for j=1

w\_3(i,j)=round0(i,j+3);

end

end

% Round 1

w\_3\_rot=ones(4,1);

temp=w\_3(1,1);

for i=1:3

for j=1

w\_3\_rot(i,j)=w\_3(i+1,j);

end

end

w\_3\_rot(4,1)=temp;

w\_3\_sub=ones(4,1);

for i=1:4

for j=1

d=bitand(w\_3\_rot(i,j),15);

e=bitshift(w\_3\_rot(i,j),-4);

d=d+1;

e=e+1;

w\_3\_sub(i,j)=a(e,d);

end

end

w\_3\_temp=w\_3\_sub;

w\_3\_temp(1,1)=bitxor(w\_3\_sub(1,1),b(1,1));

w\_4=ones(4,1);

for i=1:4

for j=1

w\_4(i,j)=bitxor(w\_0(i,j),w\_3\_temp(i,j));

end

end

disp(w\_4);

round1=ones(4,4);

for i=1:4

for j=1

round1(i,j)=w\_4(i,j);

end

end

for i=1:4

for j=2:4

if j==2

round1(i,j)=bitxor(round1(i,j-1),w\_1(i,j-1));

elseif j==3

round1(i,j)=bitxor(round1(i,j-1),w\_2(i,j-2));

elseif j==4

round1(i,j)=bitxor(round1(i,j-1),w\_3(i,j-3));

end

end

end

% Round 2

w\_7=ones(4,1);

for i=1:4

for j=1

w\_7(i,j)=round1(i,j+3);

end

end

w\_7\_rot=ones(4,1);

temp=w\_7(1,1);

for i=1:3

for j=1

w\_7\_rot(i,j)=w\_7(i+1,j);

end

end

w\_7\_rot(4,1)=temp;

w\_7\_sub=ones(4,1);

for i=1:4

for j=1

d=bitand(w\_7\_rot(i,j),15);

e=bitshift(w\_7\_rot(i,j),-4);

d=d+1;

e=e+1;

w\_7\_sub(i,j)=a(e,d);

end

end

w\_7\_temp=w\_7\_sub;

w\_7\_temp(1,1)=bitxor(w\_7\_sub(1,1),b(2,1));

w\_8=ones(4,1);

for i=1:4

for j=1

w\_8(i,j)=bitxor(w\_4(i,j),w\_7\_temp(i,j));

end

end

round2=ones(4,4);

for i=1:4

for j=1

round2(i,j)=w\_8(i,j);

end

end

for i=1:4

for j=2:4

if j==2

round2(i,j)=bitxor(round2(i,j-1),round1(i,j));

elseif j==3

round2(i,j)=bitxor(round2(i,j-1),round1(i,j));

elseif j==4

round2(i,j)=bitxor(round2(i,j-1),round1(i,j));

end

end

end

% Round 3

w\_11=ones(4,1);

for i=1:4

for j=1

w\_11(i,j)=round2(i,j+3);

end

end

w\_11\_rot=ones(4,1);

temp=w\_11(1,1);

for i=1:3

for j=1

w\_11\_rot(i,j)=w\_11(i+1,j);

end

end

w\_11\_rot(4,1)=temp;

w\_11\_sub=ones(4,1);

for i=1:4

for j=1

d=bitand(w\_11\_rot(i,j),15);

e=bitshift(w\_11\_rot(i,j),-4);

d=d+1;

e=e+1;

w\_11\_sub(i,j)=a(e,d);

end

end

w\_11\_temp=w\_11\_sub;

w\_11\_temp(1,1)=bitxor(w\_11\_sub(1,1),b(3,1));

w\_12=ones(4,1);

for i=1:4

for j=1

w\_12(i,j)=bitxor(w\_8(i,j),w\_11\_temp(i,j));

end

end

round3=ones(4,4);

for i=1:4

for j=1

round3(i,j)=w\_12(i,j);

end

end

for i=1:4

for j=2:4

if j==2

round3(i,j)=bitxor(round3(i,j-1),round2(i,j));

elseif j==3

round3(i,j)=bitxor(round3(i,j-1),round2(i,j));

elseif j==4

round3(i,j)=bitxor(round3(i,j-1),round2(i,j));

end

end

end

% Round 4

w\_15=ones(4,1);

for i=1:4

for j=1

w\_15(i,j)=round3(i,j+3);

end

end

w\_15\_rot=ones(4,1);

temp=w\_15(1,1);

for i=1:3

for j=1

w\_15\_rot(i,j)=w\_15(i+1,j);

end

end

w\_15\_rot(4,1)=temp;

disp(w\_15\_rot);

w\_15\_sub=ones(4,1);

for i=1:4

for j=1

d=bitand(w\_15\_rot(i,j),15);

e=bitshift(w\_15\_rot(i,j),-4);

d=d+1;

e=e+1;

w\_15\_sub(i,j)=a(e,d);

end

end

w\_15\_temp=w\_15\_sub;

w\_15\_temp(1,1)=bitxor(w\_15\_sub(1,1),b(4,1));

w\_16=ones(4,1);

for i=1:4

for j=1

w\_16(i,j)=bitxor(w\_12(i,j),w\_15\_temp(i,j));

end

end

round4=ones(4,4);

for i=1:4

for j=1

round4(i,j)=w\_16(i,j);

end

end

for i=1:4

for j=2:4

if j==2

round4(i,j)=bitxor(round4(i,j-1),round3(i,j));

elseif j==3

round4(i,j)=bitxor(round4(i,j-1),round3(i,j));

elseif j==4

round4(i,j)=bitxor(round4(i,j-1),round3(i,j));

end

end

end

% Round 5

w\_19=ones(4,1);

for i=1:4

for j=1

w\_19(i,j)=round4(i,j+3);

end

end

w\_19\_rot=ones(4,1);

temp=w\_19(1,1);

for i=1:3

for j=1

w\_19\_rot(i,j)=w\_19(i+1,j);

end

end

w\_19\_rot(4,1)=temp;

w\_19\_sub=ones(4,1);

for i=1:4

for j=1

d=bitand(w\_19\_rot(i,j),15);

e=bitshift(w\_19\_rot(i,j),-4);

d=d+1;

e=e+1;

w\_19\_sub(i,j)=a(e,d);

end

end

w\_19\_temp=w\_19\_sub;

w\_19\_temp(1,1)=bitxor(w\_19\_sub(1,1),b(5,1));

w\_20=ones(4,1);

for i=1:4

for j=1

w\_20(i,j)=bitxor(w\_16(i,j),w\_19\_temp(i,j));

end

end

round5=ones(4,4);

for i=1:4

for j=1

round5(i,j)=w\_20(i,j);

end

end

for i=1:4

for j=2:4

if j==2

round5(i,j)=bitxor(round5(i,j-1),round4(i,j));

elseif j==3

round5(i,j)=bitxor(round5(i,j-1),round4(i,j));

elseif j==4

round5(i,j)=bitxor(round5(i,j-1),round4(i,j));

end

end

end

% Round 6

w\_23=ones(4,1);

for i=1:4

for j=1

w\_23(i,j)=round5(i,j+3);

end

end

w\_23\_rot=ones(4,1);

temp=w\_23(1,1);

for i=1:3

for j=1

w\_23\_rot(i,j)=w\_23(i+1,j);

end

end

w\_23\_rot(4,1)=temp;

w\_23\_sub=ones(4,1);

for i=1:4

for j=1

d=bitand(w\_23\_rot(i,j),15);

e=bitshift(w\_23\_rot(i,j),-4);

d=d+1;

e=e+1;

w\_23\_sub(i,j)=a(e,d);

end

end

w\_23\_temp=w\_23\_sub;

w\_23\_temp(1,1)=bitxor(w\_23\_sub(1,1),b(6,1));

w\_24=ones(4,1);

for i=1:4

for j=1

w\_24(i,j)=bitxor(w\_20(i,j),w\_23\_temp(i,j));

end

end

round6=ones(4,4);

for i=1:4

for j=1

round6(i,j)=w\_24(i,j);

end

end

for i=1:4

for j=2:4

if j==2

round6(i,j)=bitxor(round6(i,j-1),round5(i,j));

elseif j==3

round6(i,j)=bitxor(round6(i,j-1),round5(i,j));

elseif j==4

round6(i,j)=bitxor(round6(i,j-1),round5(i,j));

end

end

end

% Round 7

w\_27=ones(4,1);

for i=1:4

for j=1

w\_27(i,j)=round6(i,j+3);

end

end

w\_27\_rot=ones(4,1);

temp=w\_27(1,1);

for i=1:3

for j=1

w\_27\_rot(i,j)=w\_27(i+1,j);

end

end

w\_27\_rot(4,1)=temp;

w\_27\_sub=ones(4,1);

for i=1:4

for j=1

d=bitand(w\_27\_rot(i,j),15);

e=bitshift(w\_27\_rot(i,j),-4);

d=d+1;

e=e+1;

w\_27\_sub(i,j)=a(e,d);

end

end

w\_27\_temp=w\_27\_sub;

w\_27\_temp(1,1)=bitxor(w\_27\_sub(1,1),b(7,1));

w\_28=ones(4,1);

for i=1:4

for j=1

w\_28(i,j)=bitxor(w\_24(i,j),w\_27\_temp(i,j));

end

end

round7=ones(4,4);

for i=1:4

for j=1

round7(i,j)=w\_28(i,j);

end

end

for i=1:4

for j=2:4

if j==2

round7(i,j)=bitxor(round7(i,j-1),round6(i,j));

elseif j==3

round7(i,j)=bitxor(round7(i,j-1),round6(i,j));

elseif j==4

round7(i,j)=bitxor(round7(i,j-1),round6(i,j));

end

end

end

% Round 8

w\_31=ones(4,1);

for i=1:4

for j=1

w\_31(i,j)=round7(i,j+3);

end

end

w\_31\_rot=ones(4,1);

temp=w\_31(1,1);

for i=1:3

for j=1

w\_31\_rot(i,j)=w\_31(i+1,j);

end

end

w\_31\_rot(4,1)=temp;

w\_31\_sub=ones(4,1);

for i=1:4

for j=1

d=bitand(w\_31\_rot(i,j),15);

e=bitshift(w\_31\_rot(i,j),-4);

d=d+1;

e=e+1;

w\_31\_sub(i,j)=a(e,d);

end

end

w\_31\_temp=w\_31\_sub;

w\_31\_temp(1,1)=bitxor(w\_31\_sub(1,1),b(8,1));

w\_32=ones(4,1);

for i=1:4

for j=1

w\_32(i,j)=bitxor(w\_28(i,j),w\_31\_temp(i,j));

end

end

round8=ones(4,4);

for i=1:4

for j=1

round8(i,j)=w\_32(i,j);

end

end

for i=1:4

for j=2:4

if j==2

round8(i,j)=bitxor(round8(i,j-1),round7(i,j));

elseif j==3

round8(i,j)=bitxor(round8(i,j-1),round7(i,j));

elseif j==4

round8(i,j)=bitxor(round8(i,j-1),round7(i,j));

end

end

end

% Round 9

w\_35=ones(4,1);

for i=1:4

for j=1

w\_35(i,j)=round8(i,j+3);

end

end

w\_35\_rot=ones(4,1);

temp=w\_35(1,1);

for i=1:3

for j=1

w\_35\_rot(i,j)=w\_35(i+1,j);

end

end

w\_35\_rot(4,1)=temp;

w\_35\_sub=ones(4,1);

for i=1:4

for j=1

d=bitand(w\_35\_rot(i,j),15);

e=bitshift(w\_35\_rot(i,j),-4);

d=d+1;

e=e+1;

w\_35\_sub(i,j)=a(e,d);

end

end

w\_35\_temp=w\_35\_sub;

w\_35\_temp(1,1)=bitxor(w\_35\_sub(1,1),b(9,1));

w\_36=ones(4,1);

for i=1:4

for j=1

w\_36(i,j)=bitxor(w\_32(i,j),w\_35\_temp(i,j));

end

end

round9=ones(4,4);

for i=1:4

for j=1

round9(i,j)=w\_36(i,j);

end

end

for i=1:4

for j=2:4

if j==2

round9(i,j)=bitxor(round9(i,j-1),round8(i,j));

elseif j==3

round9(i,j)=bitxor(round9(i,j-1),round8(i,j));

elseif j==4

round9(i,j)=bitxor(round9(i,j-1),round8(i,j));

end

end

end

% Round 9

w\_39=ones(4,1);

for i=1:4

for j=1

w\_39(i,j)=round9(i,j+3);

end

end

w\_39\_rot=ones(4,1);

temp=w\_39(1,1);

for i=1:3

for j=1

w\_39\_rot(i,j)=w\_39(i+1,j);

end

end

w\_39\_rot(4,1)=temp;

w\_39\_sub=ones(4,1);

for i=1:4

for j=1

d=bitand(w\_39\_rot(i,j),15);

e=bitshift(w\_39\_rot(i,j),-4);

d=d+1;

e=e+1;

w\_39\_sub(i,j)=a(e,d);

end

end

w\_39\_temp=w\_39\_sub;

w\_39\_temp(1,1)=bitxor(w\_39\_sub(1,1),b(10,1));

w\_40=ones(4,1);

for i=1:4

for j=1

w\_40(i,j)=bitxor(w\_36(i,j),w\_39\_temp(i,j));

end

end

round10=ones(4,4);

for i=1:4

for j=1

round10(i,j)=w\_40(i,j);

end

end

for i=1:4

for j=2:4

if j==2

round10(i,j)=bitxor(round10(i,j-1),round9(i,j));

elseif j==3

round10(i,j)=bitxor(round10(i,j-1),round9(i,j));

elseif j==4

round10(i,j)=bitxor(round10(i,j-1),round9(i,j));

end

end

end

if roundin==0

roundout=round0;

elseif roundin==1

roundout=round1;

elseif roundin==2

roundout=round2;

elseif roundin==3

roundout=round3;

elseif roundin==4

roundout=round4;

elseif roundin==5

roundout=round5;

elseif roundin==6

roundout=round6;

elseif roundin==7

roundout=round7;

elseif roundin==8

roundout=round8;

elseif roundin==9

roundout=round9;

elseif roundin==10;

roundout=round10;

end

end

% MadC Function and name as MadC.m

function [ temp ] = MadC( a,b )

%UNTITLED2 Summary of this function goes here

% Detailed explanation goes here

if a==1

temp=b;

elseif a==2

if(b>=128)

mad\_1=bitshift(b,1);

mad\_1=bitxor(mad\_1,27);

elseif(b<128)

mad\_1=bitshift(b,1);

end

if(mad\_1>255)

mad\_1=bitxor(mad\_1,256);

end

temp=mad\_1;

elseif a==3

if(b>=128)

mad\_2=bitshift(b,1);

mad\_2=bitxor(mad\_2,27);

elseif(b<128)

mad\_2=bitshift(b,1);

end

if(mad\_2>255)

mad\_2=bitxor(mad\_2,256);

end

temp3\_1=mad\_2;

temp3\_2=b;

temp=bitxor(temp3\_1,temp3\_2);

end

% MC Function and name as MC.m

function [ mc ] = MC( sr )

%UNTITLED6 Summary of this function goes here

% Detailed explanation goes here

mc\_pre=[2 3 1 1;1 2 3 1;1 1 2 3;3 1 1 2];

a=mc\_pre;

b=sr;

temp1=MadC(a(1,1),b(1,1));

temp2=MadC(a(1,2),b(2,1));

temp3=MadC(a(1,3),b(3,1));

temp4=MadC(a(1,4),b(4,1));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(1,1)=temp1;

temp1=MadC(a(1,1),b(1,2));

temp2=MadC(a(1,2),b(2,2));

temp3=MadC(a(1,3),b(3,2));

temp4=MadC(a(1,4),b(4,2));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(1,2)=temp1;

temp1=MadC(a(1,1),b(1,3));

temp2=MadC(a(1,2),b(2,3));

temp3=MadC(a(1,3),b(3,3));

temp4=MadC(a(1,4),b(4,3));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(1,3)=temp1;

temp1=MadC(a(1,1),b(1,4));

temp2=MadC(a(1,2),b(2,4));

temp3=MadC(a(1,3),b(3,4));

temp4=MadC(a(1,4),b(4,4));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(1,4)=temp1;

temp1=MadC(a(2,1),b(1,1));

temp2=MadC(a(2,2),b(2,1));

temp3=MadC(a(2,3),b(3,1));

temp4=MadC(a(2,4),b(4,1));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(2,1)=temp1;

temp1=MadC(a(2,1),b(1,2));

temp2=MadC(a(2,2),b(2,2));

temp3=MadC(a(2,3),b(3,2));

temp4=MadC(a(2,4),b(4,2));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(2,2)=temp1;

temp1=MadC(a(2,1),b(1,3));

temp2=MadC(a(2,2),b(2,3));

temp3=MadC(a(2,3),b(3,3));

temp4=MadC(a(2,4),b(4,3));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(2,3)=temp1;

temp1=MadC(a(2,1),b(1,4));

temp2=MadC(a(2,2),b(2,4));

temp3=MadC(a(2,3),b(3,4));

temp4=MadC(a(2,4),b(4,4));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(2,4)=temp1;

temp1=MadC(a(3,1),b(1,1));

temp2=MadC(a(3,2),b(2,1));

temp3=MadC(a(3,3),b(3,1));

temp4=MadC(a(3,4),b(4,1));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(3,1)=temp1;

temp1=MadC(a(3,1),b(1,2));

temp2=MadC(a(3,2),b(2,2));

temp3=MadC(a(3,3),b(3,2));

temp4=MadC(a(3,4),b(4,2));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(3,2)=temp1;

temp1=MadC(a(3,1),b(1,3));

temp2=MadC(a(3,2),b(2,3));

temp3=MadC(a(3,3),b(3,3));

temp4=MadC(a(3,4),b(4,3));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(3,3)=temp1;

temp1=MadC(a(3,1),b(1,4));

temp2=MadC(a(3,2),b(2,4));

temp3=MadC(a(3,3),b(3,4));

temp4=MadC(a(3,4),b(4,4));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(3,4)=temp1;

temp1=MadC(a(4,1),b(1,1));

temp2=MadC(a(4,2),b(2,1));

temp3=MadC(a(4,3),b(3,1));

temp4=MadC(a(4,4),b(4,1));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(4,1)=temp1;

temp1=MadC(a(4,1),b(1,2));

temp2=MadC(a(4,2),b(2,2));

temp3=MadC(a(4,3),b(3,2));

temp4=MadC(a(4,4),b(4,2));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(4,2)=temp1;

temp1=MadC(a(4,1),b(1,3));

temp2=MadC(a(4,2),b(2,3));

temp3=MadC(a(4,3),b(3,3));

temp4=MadC(a(4,4),b(4,3));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(4,3)=temp1;

temp1=MadC(a(4,1),b(1,4));

temp2=MadC(a(4,2),b(2,4));

temp3=MadC(a(4,3),b(3,4));

temp4=MadC(a(4,4),b(4,4));

temp1=bitxor(temp1,temp2);

temp1=bitxor(temp1,temp3);

temp1=bitxor(temp1,temp4);

c(4,4)=temp1;

mc=c;

end

% Function s\_box and save as s\_box.m

function [ out ] = s\_box(i,j)

%UNTITLED3 Summary of this function goes here

% Detailed explanation goes here

% S-BOX and it's modified form

s\_box=ones(16,16);

s\_box(1,1)=99;

s\_box(1,2)=124;

s\_box(1,3)=119;

s\_box(1,4)=123;

s\_box(1,5)=242;

s\_box(1,6)=107;

s\_box(1,7)=111;

s\_box(1,8)=197;

s\_box(1,9)=48;

s\_box(1,10)=1;

s\_box(1,11)=103;

s\_box(1,12)=43;

s\_box(1,13)=254;

s\_box(1,14)=215;

s\_box(1,15)=171;

s\_box(1,16)=118;

s\_box(2,1)=202;

s\_box(2,2)=130;

s\_box(2,3)=201;

s\_box(2,4)=125;

s\_box(2,5)=250;

s\_box(2,6)=89;

s\_box(2,7)=71;

s\_box(2,8)=240;

s\_box(2,9)=173;

s\_box(2,10)=212;

s\_box(2,11)=162;

s\_box(2,12)=175;

s\_box(2,13)=156;

s\_box(2,14)=164;

s\_box(2,15)=114;

s\_box(2,16)=192;

s\_box(3,1)=183;

s\_box(3,2)=253;

s\_box(3,3)=147;

s\_box(3,4)=38;

s\_box(3,5)=54;

s\_box(3,6)=63;

s\_box(3,7)=247;

s\_box(3,8)=204;

s\_box(3,9)=52;

s\_box(3,10)=165;

s\_box(3,11)=229;

s\_box(3,12)=241;

s\_box(3,13)=113;

s\_box(3,14)=216;

s\_box(3,15)=49;

s\_box(3,16)=21;

s\_box(4,1)=4;

s\_box(4,2)=199;

s\_box(4,3)=35;

s\_box(4,4)=195;

s\_box(4,5)=24;

s\_box(4,6)=150;

s\_box(4,7)=5;

s\_box(4,8)=154;

s\_box(4,9)=7;

s\_box(4,10)=18;

s\_box(4,11)=128;

s\_box(4,12)=226;

s\_box(4,13)=235;

s\_box(4,14)=39;

s\_box(4,15)=178;

s\_box(4,16)=117;

s\_box(5,1)=9;

s\_box(5,2)=131;

s\_box(5,3)=44;

s\_box(5,4)=26;

s\_box(5,5)=27;

s\_box(5,6)=110;

s\_box(5,7)=90;

s\_box(5,8)=160;

s\_box(5,9)=82;

s\_box(5,10)=59;

s\_box(5,11)=214;

s\_box(5,12)=179;

s\_box(5,13)=41;

s\_box(5,14)=227;

s\_box(5,15)=47;

s\_box(5,16)=132;

s\_box(6,1)=83;

s\_box(6,2)=209;

s\_box(6,3)=0;

s\_box(6,4)=237;

s\_box(6,5)=32;

s\_box(6,6)=252;

s\_box(6,7)=177;

s\_box(6,8)=91;

s\_box(6,9)=106;

s\_box(6,10)=203;

s\_box(6,11)=190;

s\_box(6,12)=57;

s\_box(6,13)=74;

s\_box(6,14)=76;

s\_box(6,15)=88;

s\_box(6,16)=207;

s\_box(7,1)=208;

s\_box(7,2)=239;

s\_box(7,3)=170;

s\_box(7,4)=251;

s\_box(7,5)=67;

s\_box(7,6)=77;

s\_box(7,7)=51;

s\_box(7,8)=133;

s\_box(7,9)=69;

s\_box(7,10)=249;

s\_box(7,11)=2;

s\_box(7,12)=127;

s\_box(7,13)=80;

s\_box(7,14)=60;

s\_box(7,15)=159;

s\_box(7,16)=168;

s\_box(8,1)=81;

s\_box(8,2)=163;

s\_box(8,3)=64;

s\_box(8,4)=143;

s\_box(8,5)=146;

s\_box(8,6)=157;

s\_box(8,7)=56;

s\_box(8,8)=245;

s\_box(8,9)=188;

s\_box(8,10)=182;

s\_box(8,11)=218;

s\_box(8,12)=33;

s\_box(8,13)=16;

s\_box(8,14)=255;

s\_box(8,15)=243;

s\_box(8,16)=210;

s\_box(9,1)=205;

s\_box(9,2)=12;

s\_box(9,3)=19;

s\_box(9,4)=236;

s\_box(9,5)=95;

s\_box(9,6)=151;

s\_box(9,7)=68;

s\_box(9,8)=23;

s\_box(9,9)=196;

s\_box(9,10)=167;

s\_box(9,11)=126;

s\_box(9,12)=61;

s\_box(9,13)=100;

s\_box(9,14)=93;

s\_box(9,15)=25;

s\_box(9,16)=115;

s\_box(10,1)=96;

s\_box(10,2)=129;

s\_box(10,3)=79;

s\_box(10,4)=220;

s\_box(10,5)=34;

s\_box(10,6)=42;

s\_box(10,7)=144;

s\_box(10,8)=136;

s\_box(10,9)=70;

s\_box(10,10)=238;

s\_box(10,11)=184;

s\_box(10,12)=20;

s\_box(10,13)=222;

s\_box(10,14)=94;

s\_box(10,15)=11;

s\_box(10,16)=219;

s\_box(11,1)=224;

s\_box(11,2)=50;

s\_box(11,3)=58;

s\_box(11,4)=10;

s\_box(11,5)=73;

s\_box(11,6)=6;

s\_box(11,7)=36;

s\_box(11,8)=92;

s\_box(11,9)=194;

s\_box(11,10)=211;

s\_box(11,11)=172;

s\_box(11,12)=98;

s\_box(11,13)=145;

s\_box(11,14)=149;

s\_box(11,15)=228;

s\_box(11,16)=121;

s\_box(12,1)=231;

s\_box(12,2)=200;

s\_box(12,3)=55;

s\_box(12,4)=109;

s\_box(12,5)=141;

s\_box(12,6)=213;

s\_box(12,7)=78;

s\_box(12,8)=169;

s\_box(12,9)=108;

s\_box(12,10)=86;

s\_box(12,11)=244;

s\_box(12,12)=234;

s\_box(12,13)=101;

s\_box(12,14)=122;

s\_box(12,15)=174;

s\_box(12,16)=8;

s\_box(13,1)=186;

s\_box(13,2)=120;

s\_box(13,3)=37;

s\_box(13,4)=46;

s\_box(13,5)=28;

s\_box(13,6)=166;

s\_box(13,7)=180;

s\_box(13,8)=198;

s\_box(13,9)=232;

s\_box(13,10)=221;

s\_box(13,11)=116;

s\_box(13,12)=31;

s\_box(13,13)=75;

s\_box(13,14)=189;

s\_box(13,15)=139;

s\_box(13,16)=138;

s\_box(14,1)=112;

s\_box(14,2)=62;

s\_box(14,3)=181;

s\_box(14,4)=102;

s\_box(14,5)=72;

s\_box(14,6)=3;

s\_box(14,7)=246;

s\_box(14,8)=14;

s\_box(14,9)=97;

s\_box(14,10)=53;

s\_box(14,11)=87;

s\_box(14,12)=185;

s\_box(14,13)=134;

s\_box(14,14)=193;

s\_box(14,15)=29;

s\_box(14,16)=158;

s\_box(15,1)=225;

s\_box(15,2)=248;

s\_box(15,3)=152;

s\_box(15,4)=17;

s\_box(15,5)=105;

s\_box(15,6)=217;

s\_box(15,7)=142;

s\_box(15,8)=148;

s\_box(15,9)=155;

s\_box(15,10)=30;

s\_box(15,11)=135;

s\_box(15,12)=233;

s\_box(15,13)=206;

s\_box(15,14)=85;

s\_box(15,15)=40;

s\_box(15,16)=223;

s\_box(16,1)=140;

s\_box(16,2)=161;

s\_box(16,3)=137;

s\_box(16,4)=13;

s\_box(16,5)=191;

s\_box(16,6)=230;

s\_box(16,7)=66;

s\_box(16,8)=104;

s\_box(16,9)=65;

s\_box(16,10)=153;

s\_box(16,11)=45;

s\_box(16,12)=15;

s\_box(16,13)=176;

s\_box(16,14)=84;

s\_box(16,15)=187;

s\_box(16,16)=22;

temp=s\_box(2,1);

s\_box(2,1)=s\_box(6,9);

s\_box(6,9)=temp;

out=s\_box(i,j);

end

% Function SR and name as SR.m

function [ sr ] = SR( bs )

%UNTITLED5 Summary of this function goes here

% Detailed explanation goes here

sr=bs;

for i=2:4

if(i==2)

for j=1:4

if(j==4)

sr(i,j)=bs(i,j-3);

else

sr(i,j)=bs(i,j+1);

end

end

end

if(i==3)

for j=1:4

if((j==3)||(j==4))

sr(i,j)=bs(i,j-2);

else

sr(i,j)=bs(i,j+2);

end

end

end

if(i==4)

for j=1:4

if((j==2)||(j==3)||(j==4))

sr(i,j)=bs(i,j-1);

else

sr(i,j)=bs(i,j+3);

end

end

end

end

end