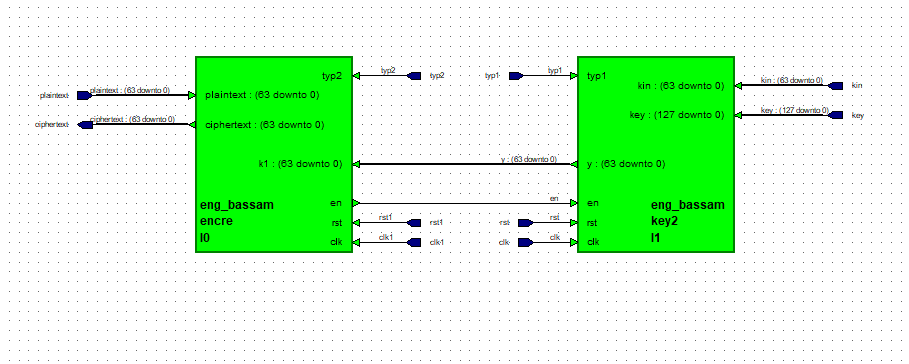
***Encryption and Decryption***

***First encryption:***



Code of encryption :

-- hds header\_start

--

-- VHDL Architecture eng\_bassam.test2.rtl

--

-- Created:

-- by - ahmed.UNKNOWN (AHMEDSAMY)

-- at - 21:49:07 02/12/2019

--

-- Generated by Mentor Graphics' HDL Designer(TM) 2001.5 (Build 170)

--

-- hds header\_end

LIBRARY ieee;

USE ieee.std\_logic\_1164.all;

USE ieee.std\_logic\_arith.all;

ENTITY encre IS

-- Declarations

port(

plaintext,k1 :in std\_logic\_vector(63 downto 0);

--k2 :in std\_logic\_vector(15 downto 0);

clk,rst : std\_logic;

typ2 : in std\_logic;

en : out std\_logic;

ciphertext : out std\_logic\_vector(63 downto 0)

);

END encre ;

-- hds interface\_end

ARCHITECTURE rtl OF encre IS

signal data,ciphertext\_temp :std\_logic\_vector(63 downto 0);

signal rest:unsigned (7 downto 0);

type S\_array is array (0 to 3) of std\_logic\_vector(15 downto 0);

signal S\_All : S\_array;

type K\_array is array (0 to 17) of std\_logic\_vector(63 downto 0);

signal k\_All : K\_array;

signal count,m,finish,control:NATURAL;

BEGIN

process(clk)

BEGIN

if (count = 16) then

if (finish = 0) then

ciphertext <= S\_All(3) & S\_All(2) & S\_All(1) & S\_All(0);

-- en <= '1';

finish <= finish +1;

--elsif (finish = 1) then

-- ciphertext <= ciphertext\_temp xor k1 ;

-- finish <= finish +1;

-- en <= '0';

end if;

end if ;

if (rst='1')then

if (typ2 = '1') then

rest <= (others =>'0') after 3700 ns;

count <= 0 after 3700 ns;

m <= 0 after 3700 ns;

finish <= 0 after 3700 ns;

en <= '1' after 3700 ns;

control <= 0 after 3700 ns;

end if ;

elsif(rest=0)then

--k\_All(m) <= k1;

en <= '0';

rest<=rest+1;

-------------------------------------------------------------------------------

elsif(rest=1)then

for k in 0 to 48 loop

if (m = 17) then

rest<=rest+1;

m <= m+1;

elsif(m < 17)then

if (control = 0) then

k\_All(m) <= k1;

control <= control +1 ;

m <= m+1;

elsif (control = 1) then

if (m <17) then

en <= '1';

end if;

control <= control +1;

elsif (control = 2) then

en <= '0';

control <= 0;

end if;

end if;

end loop;

---------------------------------------------------------------------------------------------

elsif(rest=2)then

m <= 0 ;

rest<=rest+1;

---------------------------------------------------------------------------------------------

elsif(rest=3)then

data <= plaintext xor k\_All(m);

rest<=rest+1;

elsif(rest=4)then

S\_All(0) <= data(15 downto 0);

S\_All(1) <= data(31 downto 16);

S\_All(2) <= data(47 downto 32);

S\_All(3) <= data(63 downto 48);

m <= m + 1;

rest<=rest+1;

elsif (count < 16) then

if (rest=5+count\*4) then

rest<=rest+1;

for i in 0 to 3 loop

if (S\_All(i)(3 downto 0) = "0000")then S\_All(i)(3 downto 0)<= "0010";

elsif (S\_All(i)(3 downto 0) = "0001")then S\_All(i)(3 downto 0)<= "0011";

elsif (S\_All(i)(3 downto 0) = "0010")then S\_All(i)(3 downto 0)<= "0000";

elsif (S\_All(i)(3 downto 0) = "0011")then S\_All(i)(3 downto 0)<= "0001";

elsif (S\_All(i)(3 downto 0) = "0100")then S\_All(i)(3 downto 0)<= "1011";

elsif (S\_All(i)(3 downto 0) = "0101")then S\_All(i)(3 downto 0)<= "1110";

elsif (S\_All(i)(3 downto 0) = "0110")then S\_All(i)(3 downto 0)<= "1010";

elsif (S\_All(i)(3 downto 0) = "0111")then S\_All(i)(3 downto 0)<= "1101";

elsif (S\_All(i)(3 downto 0) = "1000")then S\_All(i)(3 downto 0)<= "1111";

elsif (S\_All(i)(3 downto 0) = "1001")then S\_All(i)(3 downto 0)<= "1100";

elsif (S\_All(i)(3 downto 0) = "1010")then S\_All(i)(3 downto 0)<= "0110";

elsif (S\_All(i)(3 downto 0) = "1011")then S\_All(i)(3 downto 0)<= "0100";

elsif (S\_All(i)(3 downto 0) = "1100")then S\_All(i)(3 downto 0)<= "1001";

elsif (S\_All(i)(3 downto 0) = "1101")then S\_All(i)(3 downto 0)<= "0111";

elsif (S\_All(i)(3 downto 0) = "1110")then S\_All(i)(3 downto 0)<= "0101";

elsif (S\_All(i)(3 downto 0) = "1111")then S\_All(i)(3 downto 0)<= "1000";

end if ;

------------------------------------------4 to 7 ----------------------------------------------------

if (S\_All(i)(7 downto 4) = "0000")then S\_All(i)(7 downto 4)<= "1101";

elsif (S\_All(i)(7 downto 4) = "0001")then S\_All(i)(7 downto 4)<= "0011";

elsif (S\_All(i)(7 downto 4) = "0010")then S\_All(i)(7 downto 4)<= "0101";

elsif (S\_All(i)(7 downto 4) = "0011")then S\_All(i)(7 downto 4)<= "0001";

elsif (S\_All(i)(7 downto 4) = "0100")then S\_All(i)(7 downto 4)<= "1110";

elsif (S\_All(i)(7 downto 4) = "0101")then S\_All(i)(7 downto 4)<= "0010";

elsif (S\_All(i)(7 downto 4) = "0110")then S\_All(i)(7 downto 4)<= "1010";

elsif (S\_All(i)(7 downto 4) = "0111")then S\_All(i)(7 downto 4)<= "1111";

elsif (S\_All(i)(7 downto 4) = "1000")then S\_All(i)(7 downto 4)<= "1001";

elsif (S\_All(i)(7 downto 4) = "1001")then S\_All(i)(7 downto 4)<= "1000";

elsif (S\_All(i)(7 downto 4) = "1010")then S\_All(i)(7 downto 4)<= "0110";

elsif (S\_All(i)(7 downto 4) = "1011")then S\_All(i)(7 downto 4)<= "1100";

elsif (S\_All(i)(7 downto 4) = "1100")then S\_All(i)(7 downto 4)<= "1011";

elsif (S\_All(i)(7 downto 4) = "1101")then S\_All(i)(7 downto 4)<= "0000";

elsif (S\_All(i)(7 downto 4) = "1110")then S\_All(i)(7 downto 4)<= "0100";

elsif (S\_All(i)(7 downto 4) = "1111")then S\_All(i)(7 downto 4)<= "0111";

end if ;

------------------------------------------8 to 11 ----------------------------------------------------

if (S\_All(i)(11 downto 8) = "0000")then S\_All(i)(11 downto 8)<= "0111";

elsif (S\_All(i)(11 downto 8) = "0001")then S\_All(i)(11 downto 8)<= "0101";

elsif (S\_All(i)(11 downto 8) = "0010")then S\_All(i)(11 downto 8)<= "0011";

elsif (S\_All(i)(11 downto 8) = "0011")then S\_All(i)(11 downto 8)<= "0010";

elsif (S\_All(i)(11 downto 8) = "0100")then S\_All(i)(11 downto 8)<= "1101";

elsif (S\_All(i)(11 downto 8) = "0101")then S\_All(i)(11 downto 8)<= "0001";

elsif (S\_All(i)(11 downto 8) = "0110")then S\_All(i)(11 downto 8)<= "1011";

elsif (S\_All(i)(11 downto 8) = "0111")then S\_All(i)(11 downto 8)<= "0000";

elsif (S\_All(i)(11 downto 8) = "1000")then S\_All(i)(11 downto 8)<= "1001";

elsif (S\_All(i)(11 downto 8) = "1001")then S\_All(i)(11 downto 8)<= "1000";

elsif (S\_All(i)(11 downto 8) = "1010")then S\_All(i)(11 downto 8)<= "1111";

elsif (S\_All(i)(11 downto 8) = "1011")then S\_All(i)(11 downto 8)<= "0110";

elsif (S\_All(i)(11 downto 8) = "1100")then S\_All(i)(11 downto 8)<= "1110";

elsif (S\_All(i)(11 downto 8) = "1101")then S\_All(i)(11 downto 8)<= "0100";

elsif (S\_All(i)(11 downto 8) = "1110")then S\_All(i)(11 downto 8)<= "1100";

elsif (S\_All(i)(11 downto 8) = "1111")then S\_All(i)(11 downto 8)<= "1010";

end if ;

------------------------------------------12 to 15 ----------------------------------------------------

if (S\_All(i)(15 downto 12) = "0000")then S\_All(i)(15 downto 12)<= "0100";

elsif (S\_All(i)(15 downto 12) = "0001")then S\_All(i)(15 downto 12)<= "1011";

elsif (S\_All(i)(15 downto 12) = "0010")then S\_All(i)(15 downto 12)<= "0111";

elsif (S\_All(i)(15 downto 12) = "0011")then S\_All(i)(15 downto 12)<= "1101";

elsif (S\_All(i)(15 downto 12) = "0100")then S\_All(i)(15 downto 12)<= "0000";

elsif (S\_All(i)(15 downto 12) = "0101")then S\_All(i)(15 downto 12)<= "1100";

elsif (S\_All(i)(15 downto 12) = "0110")then S\_All(i)(15 downto 12)<= "1001";

elsif (S\_All(i)(15 downto 12) = "0111")then S\_All(i)(15 downto 12)<= "0010";

elsif (S\_All(i)(15 downto 12) = "1000")then S\_All(i)(15 downto 12)<= "1110";

elsif (S\_All(i)(15 downto 12) = "1001")then S\_All(i)(15 downto 12)<= "0110";

elsif (S\_All(i)(15 downto 12) = "1010")then S\_All(i)(15 downto 12)<= "1111";

elsif (S\_All(i)(15 downto 12) = "1011")then S\_All(i)(15 downto 12)<= "0001";

elsif (S\_All(i)(15 downto 12) = "1100")then S\_All(i)(15 downto 12)<= "0101";

elsif (S\_All(i)(15 downto 12) = "1101")then S\_All(i)(15 downto 12)<= "0011";

elsif (S\_All(i)(15 downto 12) = "1110")then S\_All(i)(15 downto 12)<= "1000";

elsif (S\_All(i)(15 downto 12) = "1111")then S\_All(i)(15 downto 12)<= "1010";

end if ;

end loop;

elsif(rest=6+count\*4)then

for r in 0 to 3 loop

S\_All(r) <=S\_All(r)(15)&S\_All(r)(11)&S\_All(r)(7)&S\_All(r)(3)&S\_All(r)(14)&S\_All(r)(10)&S\_All(r)(6)&S\_All(r)(2)&S\_All(r)(13)&S\_All(r)(9)&S\_All(r)(5)&S\_All(r)(1)&S\_All(r)(12)&S\_All(r)(8)&S\_All(r)(4)&S\_All(r)(0);

end loop;

rest<=rest+1;

elsif(rest=7+count\*4)then

if (count <16) then

S\_All(3) <= S\_All(3) xor S\_All(2) xor S\_All(1) xor S\_All(0) xor k\_All(m)(63 downto 48);

S\_All(2) <= S\_All(2) xor k\_All(m)(47 downto 32);

S\_All(1) <= S\_All(1) xor k\_All(m)(31 downto 16);

S\_All(0) <= S\_All(0) xor k\_All(m)(15 downto 0);

end if;

rest<=rest+1;

elsif(rest=8+count\*4)then

if (count <15) then

S\_All(0) <= S\_All(3);

S\_All(1) <= S\_All(0);

S\_All(2) <= S\_All(1);

S\_All(3) <= S\_All(2);

end if;

m <= m+1;

rest<=rest+1;

count <= count+1;

end if ;

end if ;

end process;

END rtl;

Code of generation key :

-- hds header\_start

--

-- VHDL Architecture eng\_bassam.first\_key.rtl

--

-- Created:

-- by - ahmed.UNKNOWN (AHMEDSAMY)

-- at - 11:25:09 02/21/2019

--

-- Generated by Mentor Graphics' HDL Designer(TM) 2001.5 (Build 170)

--

-- hds header\_end

LIBRARY ieee;

USE ieee.std\_logic\_1164.all;

USE ieee.std\_logic\_arith.all;

ENTITY key2 IS

-- Declarations

port (

key : in std\_logic\_vector(127 downto 0);

kin : in std\_logic\_vector(63 downto 0);

en,typ1 : in std\_logic;

clk,rst : std\_logic;

y: out std\_logic\_vector(63 downto 0)

);

END key2 ;

-- hds interface\_end

ARCHITECTURE rtl OF key2 IS

signal k1,k2 :std\_logic\_vector(63 downto 0);

signal rest:unsigned (7 downto 0);

type t\_array is array (0 to 16) of std\_logic\_vector(63 downto 0);

signal K\_All : t\_array;

signal count,m,o :NATURAL;

BEGIN

process(clk)

BEGIN

if ((en = '1') ) then

if (typ1 = '1') then

y <= K\_All(o);

if ( o < 17) then

o <= o + 1;

end if ;

elsif (typ1 = '0' ) then

y <= K\_All(o);

if ( o < 17) then

o <= o + 1;

end if ;

end if ;

end if;

if (rst = '1') then

--y <=key(127 downto 64);

count <= 0 ;

K\_All(0) <= key(127 downto 64);

K\_All(1) <= key(63 downto 0);

m <= 2;

o <= 0;

rest<= (others =>'0');

elsif (rest = 0 ) then

k1 <= key(127 downto 64);

k2 <= key(63 downto 0);

--y <= key(63 downto 0);

rest <= rest +1 ;

elsif (count < 15) then

if (rest = 1+count\*4) then

k1 <= k1(40 downto 0)&k1(63 downto 41);

k2 <= k2 xor kin ;

rest <= rest +1 ;

elsif (rest = 2+count\*4) then

k1 <=k1 xor k2 ;

k2 <= k2(22 downto 0) & k2(63 downto 23);

rest <= rest +1 ;

elsif (rest = 3+count\*4) then

rest<=rest+1;

----------------------------------------S1-----------------------------------------------------------

for i in 0 to 7 loop

if (k2 ((3+(i\*8)) downto (i\*8)) = "0000") then k2 ((3+(i\*8)) downto (i\*8)) <= "0010";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "0001") then k2 ((3+(i\*8)) downto (i\*8)) <= "0011";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "0010") then k2 ((3+(i\*8)) downto (i\*8)) <= "0000";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "0011") then k2 ((3+(i\*8)) downto (i\*8)) <= "0001";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "0100") then k2 ((3+(i\*8)) downto (i\*8)) <= "1011";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "0101") then k2 ((3+(i\*8)) downto (i\*8)) <= "1110";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "0110") then k2 ((3+(i\*8)) downto (i\*8)) <= "1010";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "0111") then k2 ((3+(i\*8)) downto (i\*8)) <= "1101";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "1000") then k2 ((3+(i\*8)) downto (i\*8)) <= "1111";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "1001") then k2 ((3+(i\*8)) downto (i\*8)) <= "1100";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "1010") then k2 ((3+(i\*8)) downto (i\*8)) <= "0110";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "1011") then k2 ((3+(i\*8)) downto (i\*8)) <= "0100";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "1100") then k2 ((3+(i\*8)) downto (i\*8)) <= "1001";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "1101") then k2 ((3+(i\*8)) downto (i\*8)) <= "0111";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "1110") then k2 ((3+(i\*8)) downto (i\*8)) <= "0101";

elsif (k2 ((3+(i\*8)) downto (i\*8)) = "1111") then k2 ((3+(i\*8)) downto (i\*8)) <= "1000";

end if ;

-----------------------------------------S2-----------------------------------------------------------

if (k2 ((7+(i\*8)) downto (4+(i\*8))) = "0000") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "1101";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "0001") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "0011";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "0010") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "0101";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "0011") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "0001";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "0100") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "1110";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "0101") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "0010";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "0110") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "1010";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "0111") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "1111";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "1000") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "1001";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "1001") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "1000";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "1010") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "0110";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "1011") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "1100";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "1100") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "1011";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "1101") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "0000";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "1110") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "0100";

elsif (k2 ((7+(i\*8)) downto (4+(i\*8))) = "1111") then k2 ((7+(i\*8)) downto (4+(i\*8))) <= "0111";

end if ;

------------------------------------------S3-------------------------------------------------------

if (k1 ((3+(i\*8)) downto (i\*8)) = "0000") then k1 ((3+(i\*8)) downto (i\*8)) <= "0111";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "0001") then k1 ((3+(i\*8)) downto (i\*8)) <= "0101";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "0010") then k1 ((3+(i\*8)) downto (i\*8)) <= "0011";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "0011") then k1 ((3+(i\*8)) downto (i\*8)) <= "0010";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "0100") then k1 ((3+(i\*8)) downto (i\*8)) <= "1101";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "0101") then k1 ((3+(i\*8)) downto (i\*8)) <= "0001";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "0110") then k1 ((3+(i\*8)) downto (i\*8)) <= "1011";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "0111") then k1 ((3+(i\*8)) downto (i\*8)) <= "0000";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "1000") then k1 ((3+(i\*8)) downto (i\*8)) <= "1001";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "1001") then k1 ((3+(i\*8)) downto (i\*8)) <= "1000";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "1010") then k1 ((3+(i\*8)) downto (i\*8)) <= "1111";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "1011") then k1 ((3+(i\*8)) downto (i\*8)) <= "0110";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "1100") then k1 ((3+(i\*8)) downto (i\*8)) <= "1110";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "1101") then k1 ((3+(i\*8)) downto (i\*8)) <= "0100";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "1110") then k1 ((3+(i\*8)) downto (i\*8)) <= "1100";

elsif (k1 ((3+(i\*8)) downto (i\*8)) = "1111") then k1 ((3+(i\*8)) downto (i\*8)) <= "1010";

end if ;

------------------------------------------S4-------------------------------------------------------

if (k1 ((7+(i\*8)) downto (4+(i\*8))) = "0000") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "0100";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "0001") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "1011";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "0010") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "0111";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "0011") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "1101";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "0100") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "0000";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "0101") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "1100";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "0110") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "1001";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "0111") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "0010";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "1000") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "1110";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "1001") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "0110";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "1010") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "1111";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "1011") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "0001";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "1100") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "0101";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "1101") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "0011";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "1110") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "1000";

elsif (k1 ((7+(i\*8)) downto (4+(i\*8))) = "1111") then k1 ((7+(i\*8)) downto (4+(i\*8))) <= "1010";

end if ;

end loop;

elsif (rest = 4+count\*4) then

--y <= k1;

K\_All(m) <= k1;

m <= m + 1;

rest <=rest+1;

count <= count +1;

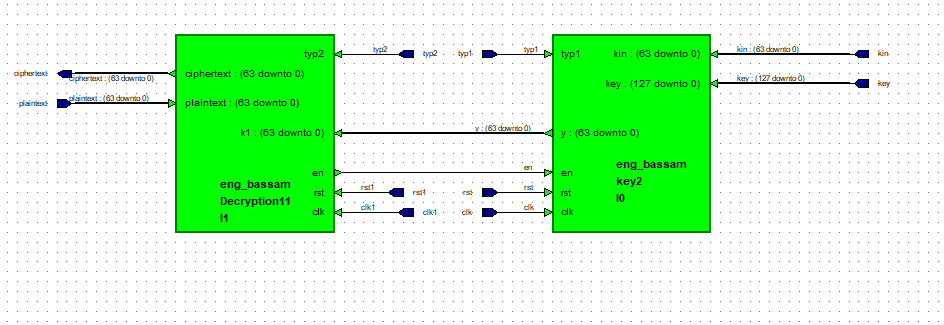
end if;

end if;

end process;

END rtl;

***Second decryption :***



***Code of decryption :***

-- hds header\_start

--

-- VHDL Architecture eng\_bassam.test2.rtl

--

-- Created:

-- by - ahmed.UNKNOWN (AHMEDSAMY)

-- at - 21:49:07 02/12/2019

--

-- Generated by Mentor Graphics' HDL Designer(TM) 2001.5 (Build 170)

--

-- hds header\_end

LIBRARY ieee;

USE ieee.std\_logic\_1164.all;

USE ieee.std\_logic\_arith.all;

ENTITY Decryption11 IS

-- Declarations

port(

plaintext,k1 :in std\_logic\_vector(63 downto 0);

--k2 :in std\_logic\_vector(15 downto 0);

clk,rst : std\_logic;

typ2 : in std\_logic;

en : out std\_logic;

ciphertext : out std\_logic\_vector(63 downto 0)

);

END Decryption11 ;

-- hds interface\_end

ARCHITECTURE rtl OF Decryption11 IS

signal data,ciphertext\_temp :std\_logic\_vector(63 downto 0);

signal rest:unsigned (7 downto 0);

type S\_array is array (0 to 3) of std\_logic\_vector(15 downto 0);

signal S\_All : S\_array;

type K\_array is array (0 to 16) of std\_logic\_vector(63 downto 0);

signal k\_All : K\_array;

signal count,m,finish,p\_invers,control:NATURAL;

BEGIN

process(clk)

BEGIN

if (count = 16) then

if (finish = 0) then

ciphertext\_temp <= S\_All(3) & S\_All(2) & S\_All(1) & S\_All(0);

finish <= finish +1;

-- en <= '1';

elsif (finish = 1) then

ciphertext <= ciphertext\_temp xor k\_All(m) ;

finish <= finish +1;

-- en <= '0';

end if;

end if ;

if (rst='1')then

if (typ2 = '0') then

rest <= (others =>'0') after 3700 ns;

count <= 0 after 3700 ns;

m <= 0 after 3700 ns;

finish <= 0 after 3700 ns;

p\_invers<= 0 after 3700 ns;

control <= 0 after 3700 ns;

en <= '1' after 3700 ns;

end if ;

--------------------------------------------------------------------------------------------------------------------------

elsif(rest=0)then

en <= '0';

rest<=rest+1;

--------------------------------------------------------------------------------------------------------------------------

elsif(rest=1)then

for k in 0 to 48 loop

if (m = 17) then

rest<=rest+1;

m <= m+1;

elsif(m < 17)then

if (control = 0) then

k\_All(m) <= k1;

control <= control +1 ;

m <= m+1;

elsif (control = 1) then

if (m <17) then

en <= '1';

end if;

control <= control +1;

elsif (control = 2) then

en <= '0';

control <= 0;

end if;

end if;

end loop;

----------------------------------------------------------------------------------------------------------------

elsif(rest=2)then

m <= 16;

S\_All(0)<=plaintext(15 downto 0);

S\_All(1)<=plaintext(31 downto 16);

S\_All(2)<=plaintext(47 downto 32);

S\_All(3)<=plaintext(63 downto 48);

rest<=rest+1;

-------------------------------------------------------------------------------------------------------------------

elsif(rest=3)then

S\_All(0)<= S\_All(0) xor k\_All(m)(15 downto 0);

S\_All(1)<= S\_All(1) xor k\_All(m)(31 downto 16);

S\_All(2)<= S\_All(2) xor k\_All(m)(47 downto 32);

S\_All(3)<= S\_All(3) xor k\_All(m)(63 downto 48);

rest<=rest+1;

-----------------------------------------------------------------------------------------------------------------

elsif(rest=4)then

m <= m -1;

S\_All(3)<= S\_All(3) xor S\_All(2) xor S\_All(1) xor S\_All(0);

rest<=rest+1;

---------------------------------------------------------------------------------------------------------------

elsif (count < 16) then

if (rest=5+count\*4) then

rest<=rest+1;

for r in 0 to 3 loop

S\_All(r) <=S\_All(r)(15)&S\_All(r)(11)&S\_All(r)(7)&S\_All(r)(3)&S\_All(r)(14)&S\_All(r)(10)&S\_All(r)(6)&S\_All(r)(2)&S\_All(r)(13)&S\_All(r)(9)&S\_All(r)(5)&S\_All(r)(1)&S\_All(r)(12)&S\_All(r)(8)&S\_All(r)(4)&S\_All(r)(0);

end loop;

--------------------------------------------------------------------------------------------------------------------

elsif(rest=6+count\*4)then

for i in 0 to 3 loop

if (S\_All(i)(3 downto 0) = "0000")then S\_All(i)(3 downto 0)<= "0010";

elsif (S\_All(i)(3 downto 0) = "0001")then S\_All(i)(3 downto 0)<= "0011";

elsif (S\_All(i)(3 downto 0) = "0010")then S\_All(i)(3 downto 0)<= "0000";

elsif (S\_All(i)(3 downto 0) = "0011")then S\_All(i)(3 downto 0)<= "0001";

elsif (S\_All(i)(3 downto 0) = "0100")then S\_All(i)(3 downto 0)<= "1011";

elsif (S\_All(i)(3 downto 0) = "0101")then S\_All(i)(3 downto 0)<= "1110";

elsif (S\_All(i)(3 downto 0) = "0110")then S\_All(i)(3 downto 0)<= "1010";

elsif (S\_All(i)(3 downto 0) = "0111")then S\_All(i)(3 downto 0)<= "1101";

elsif (S\_All(i)(3 downto 0) = "1000")then S\_All(i)(3 downto 0)<= "1111";

elsif (S\_All(i)(3 downto 0) = "1001")then S\_All(i)(3 downto 0)<= "1100";

elsif (S\_All(i)(3 downto 0) = "1010")then S\_All(i)(3 downto 0)<= "0110";

elsif (S\_All(i)(3 downto 0) = "1011")then S\_All(i)(3 downto 0)<= "0100";

elsif (S\_All(i)(3 downto 0) = "1100")then S\_All(i)(3 downto 0)<= "1001";

elsif (S\_All(i)(3 downto 0) = "1101")then S\_All(i)(3 downto 0)<= "0111";

elsif (S\_All(i)(3 downto 0) = "1110")then S\_All(i)(3 downto 0)<= "0101";

elsif (S\_All(i)(3 downto 0) = "1111")then S\_All(i)(3 downto 0)<= "1000";

end if ;

------------------------------------------4 to 7 ----------------------------------------------------

if (S\_All(i)(7 downto 4) = "0000")then S\_All(i)(7 downto 4)<= "1101";

elsif (S\_All(i)(7 downto 4) = "0001")then S\_All(i)(7 downto 4)<= "0011";

elsif (S\_All(i)(7 downto 4) = "0010")then S\_All(i)(7 downto 4)<= "0101";

elsif (S\_All(i)(7 downto 4) = "0011")then S\_All(i)(7 downto 4)<= "0001";

elsif (S\_All(i)(7 downto 4) = "0100")then S\_All(i)(7 downto 4)<= "1110";

elsif (S\_All(i)(7 downto 4) = "0101")then S\_All(i)(7 downto 4)<= "0010";

elsif (S\_All(i)(7 downto 4) = "0110")then S\_All(i)(7 downto 4)<= "1010";

elsif (S\_All(i)(7 downto 4) = "0111")then S\_All(i)(7 downto 4)<= "1111";

elsif (S\_All(i)(7 downto 4) = "1000")then S\_All(i)(7 downto 4)<= "1001";

elsif (S\_All(i)(7 downto 4) = "1001")then S\_All(i)(7 downto 4)<= "1000";

elsif (S\_All(i)(7 downto 4) = "1010")then S\_All(i)(7 downto 4)<= "0110";

elsif (S\_All(i)(7 downto 4) = "1011")then S\_All(i)(7 downto 4)<= "1100";

elsif (S\_All(i)(7 downto 4) = "1100")then S\_All(i)(7 downto 4)<= "1011";

elsif (S\_All(i)(7 downto 4) = "1101")then S\_All(i)(7 downto 4)<= "0000";

elsif (S\_All(i)(7 downto 4) = "1110")then S\_All(i)(7 downto 4)<= "0100";

elsif (S\_All(i)(7 downto 4) = "1111")then S\_All(i)(7 downto 4)<= "0111";

end if ;

------------------------------------------8 to 11 ----------------------------------------------------

if (S\_All(i)(11 downto 8) = "0000")then S\_All(i)(11 downto 8)<= "0111";

elsif (S\_All(i)(11 downto 8) = "0001")then S\_All(i)(11 downto 8)<= "0101";

elsif (S\_All(i)(11 downto 8) = "0010")then S\_All(i)(11 downto 8)<= "0011";

elsif (S\_All(i)(11 downto 8) = "0011")then S\_All(i)(11 downto 8)<= "0010";

elsif (S\_All(i)(11 downto 8) = "0100")then S\_All(i)(11 downto 8)<= "1101";

elsif (S\_All(i)(11 downto 8) = "0101")then S\_All(i)(11 downto 8)<= "0001";

elsif (S\_All(i)(11 downto 8) = "0110")then S\_All(i)(11 downto 8)<= "1011";

elsif (S\_All(i)(11 downto 8) = "0111")then S\_All(i)(11 downto 8)<= "0000";

elsif (S\_All(i)(11 downto 8) = "1000")then S\_All(i)(11 downto 8)<= "1001";

elsif (S\_All(i)(11 downto 8) = "1001")then S\_All(i)(11 downto 8)<= "1000";

elsif (S\_All(i)(11 downto 8) = "1010")then S\_All(i)(11 downto 8)<= "1111";

elsif (S\_All(i)(11 downto 8) = "1011")then S\_All(i)(11 downto 8)<= "0110";

elsif (S\_All(i)(11 downto 8) = "1100")then S\_All(i)(11 downto 8)<= "1110";

elsif (S\_All(i)(11 downto 8) = "1101")then S\_All(i)(11 downto 8)<= "0100";

elsif (S\_All(i)(11 downto 8) = "1110")then S\_All(i)(11 downto 8)<= "1100";

elsif (S\_All(i)(11 downto 8) = "1111")then S\_All(i)(11 downto 8)<= "1010";

end if ;

------------------------------------------12 to 15 ----------------------------------------------------

if (S\_All(i)(15 downto 12) = "0000")then S\_All(i)(15 downto 12)<= "0100";

elsif (S\_All(i)(15 downto 12) = "0001")then S\_All(i)(15 downto 12)<= "1011";

elsif (S\_All(i)(15 downto 12) = "0010")then S\_All(i)(15 downto 12)<= "0111";

elsif (S\_All(i)(15 downto 12) = "0011")then S\_All(i)(15 downto 12)<= "1101";

elsif (S\_All(i)(15 downto 12) = "0100")then S\_All(i)(15 downto 12)<= "0000";

elsif (S\_All(i)(15 downto 12) = "0101")then S\_All(i)(15 downto 12)<= "1100";

elsif (S\_All(i)(15 downto 12) = "0110")then S\_All(i)(15 downto 12)<= "1001";

elsif (S\_All(i)(15 downto 12) = "0111")then S\_All(i)(15 downto 12)<= "0010";

elsif (S\_All(i)(15 downto 12) = "1000")then S\_All(i)(15 downto 12)<= "1110";

elsif (S\_All(i)(15 downto 12) = "1001")then S\_All(i)(15 downto 12)<= "0110";

elsif (S\_All(i)(15 downto 12) = "1010")then S\_All(i)(15 downto 12)<= "1111";

elsif (S\_All(i)(15 downto 12) = "1011")then S\_All(i)(15 downto 12)<= "0001";

elsif (S\_All(i)(15 downto 12) = "1100")then S\_All(i)(15 downto 12)<= "0101";

elsif (S\_All(i)(15 downto 12) = "1101")then S\_All(i)(15 downto 12)<= "0011";

elsif (S\_All(i)(15 downto 12) = "1110")then S\_All(i)(15 downto 12)<= "1000";

elsif (S\_All(i)(15 downto 12) = "1111")then S\_All(i)(15 downto 12)<= "1010";

end if ;

end loop;

rest<=rest+1;

---------------------------------------------------------------------------------------------------------

elsif(rest=7+count\*4)then

if (count <15) then

S\_All(3) <= S\_All(3) xor k\_All(m)(47 downto 32);

S\_All(2) <= S\_All(2) xor k\_All(m)(31 downto 16);

S\_All(1) <= S\_All(1) xor k\_All(m)(15 downto 0);

end if;

rest<=rest+1;

-------------------------------------------------------------------------------------------------------

elsif(rest=8+count\*4)then

if (count <15) then

S\_All(3) <= S\_All(3) xor S\_All(2) xor S\_All(1) xor S\_All(0) xor k\_All(m)(63 downto 48);

S\_All(2) <= S\_All(3);

S\_All(1) <= S\_All(2);

S\_All(0) <= S\_All(1);

rest<=rest+1;

m <= m -1;

end if;

count <= count+1;

end if ;

end if ;

end process;

END rtl;