Question 1

MixColumns(])

begin

byte state [16];

state =in;

for col = 0 to 3 column size do

get currentColumn;

for row = 0 to 3 row size do

 tempVector[row] = (byte)

Multiply each column by c(x) = 03\*x^3 + 01\*x^2 + 01\*x + 2

End for

for row = 0 to 3 row size do

currentColumnrow = tempVector(byte)];

//Gets value of the multiplied result from the temp vector

end for

end for

Question 2

ffMultiply (byte a, byte b)

begin

byte c =0;

byte counter;

byte bit\_set;

for counter = 0 to 8 do

if (b&1) is not equal to zero

c^=a;

bit\_set = byte (a&0x80);

a is less than 1;

if bit\_set is not equal to zero

a^=0x1b

b is greater than or equal to 1

end for

return c;