

```
`include "timescale.v"
```

```
module byte_mixcolumn(a,b,c,d,outx,outy);
```

```
input [7:0] a,b,c,d;
```

```
output [7:0] outx, outy;
```

```
reg [7:0] outx, outy;
```

```
function [7:0] xtime;
```

```
input [7:0] in;
```

```
reg [3:0] xtime_t;
```

```
begin
```

```
    xtime[7:5] = in[6:4];
```

```
    xtime_t[3] = in[7];
```

```
    xtime_t[2] = in[7];
```

```
    xtime_t[1] = 0;
```

```
    xtime_t[0] = in[7];
```

```
    xtime[4:1] = xtime_t^in[3:0];
```

```
    xtime[0] = in[7];
```

```
end
```

```
endfunction
```

```
reg [7:0] w1,w2,w3,w4,w5,w6,w7,w8,outx_var;
```

```
always @ (a, b, c, d)
```

```
begin
```

```
    w1 = a ^b;
```

```
    w2 = a ^c;
```

```
    w3 = c ^d;
```

```
    w4 = xtime(w1);
```

```
    w5 = xtime(w3);
```

```
    w6 = w2 ^w4 ^w5;
```

```
    w7 = xtime(w6);
```

```
    w8 = xtime(w7);
```

```
    outx_var = b^w3^w4;
```

```
    outx=outx_var;
```

```
    outy=w8^outx_var;
```

```
end
```

```
endmodule
```