باسمه تعالی

گزارش تمرین کامپیوتری تمرین ۵ پوریا دادخواه – ۹۶۱۰۶۴۸۵

در این تمرین برنامه MixColumn را نوشته ایم که در آن بردار ورودی (A1,B2,C3,D4) را میگیرد و در ماتریس جایگشت که در کتاب و اسلاید های معرفی شده در GF(2^8) ضرب میکند.

ضرب تک تک ضرایب را با استفاده از تابع multGF2 که در تمرین های گذشته نوشتیم انجام میدهیم و جمع هم که صرفا xor می باشد.

نتیجه ضرب ماتریسی فوق داریم:

```
The MixColumn is :

83
54
E9
3A
```

سپس برای چک کردن درستی پاسخ ، بردار خروجی را درماتریس معکوس تبدیل Inv_MixColumn ضرب می کنیم . طبق انتظار حاصل همان بردار اولیه شد:

```
The Main Column was :

A1
B2
C3
D4
```

نهایتا برای میزان تاثیر یک بیت ورودی A1 را به A3 تغییر میدهیم:

```
The Changed MixColumn is :

87
56
EB
3C
```

همان طور که می بینیم

83 → 87

54 → 56

E9 → EB

3A → 3C

در مجموع در یک دور از اجرای الگوریتم ۴ بیت تغییر کرده است (هر کدام یک بیت)
