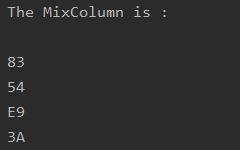
باسمه تعالی

گزارش تمرین کامپیوتری تمرین 5 پوریا دادخواه – 96106485

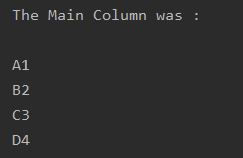
در این تمرین برنامه MixColumn را نوشته ایم که در آن بردار ورودی (A1,B2,C3,D4) را میگیرد و در ماتریس جایگشت که در کتاب و اسلاید های معرفی شده در GF(2^8) ضرب میکند.

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.

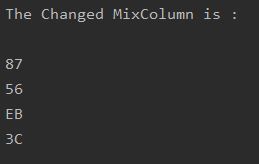
نتیجه ضرب ماتریسی فوق داریم:



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



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



همان طور که می بینیم

83 🡪 87

54 🡪 56

E9 🡪 EB

3A 🡪 3C

در مجموع در یک دور از اجرای الگوریتم 4 بیت تغییر کرده است ( هر کدام یک بیت)

\*\* تمرین این سری تا موعد مقرر ( ساعت 12 ظهر پنچ شنبه) تحویل داده شده بود ، فقط گزارش تمرین کامپیوتری در آن ضمیمه نشده بود و این نسخه صرفا توضیح تمرین کامپیوتری اضافه شد که محتوای خاص و پیچیده ای هم ندارد چرا که اکثر توضیحات در کد به صورت کامنت توضیح داده شده بود) بنابراین خواهشمندم به عنوان تحویل با تاخیر محاسبه نشود. با تشکر فراوان