

گزارش تمرین کامپیوتری:

در این تمرین یک CLI ماشین حساب با زبان پایتون طراحی کرده ایم که با اجرای برنامه و دادن کامند های مختلف از آن استفاده می کنیم که دستور ها را در منوی help می توان مشاهده کرد.

ورودی اعداد این ماشین حساب به صورت hex است و یک استک از اعداد ذخیره میکند که برای انجام چهار عمل اصلی به صورت پسوندی عمل می کند. یعنی ۲ عدد آخر استک را با operation ای که به آن می دهیم تبدیل به خروجی کرده و در استک مینویسد و آن را چاپ میکند.

در ضمن از آن جایی که  $m(x)$  گفته نشده بود همان که کتاب گرفته بود را به عنوان پیمانه گرفتیم.

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

عملیات جمع و منها :

در  $GF(2^8)$  هر دوی این ها نتیجه یکسان دارند) چرا که ضرایب ai ها در پیمانه ۲ اند و  $(-1 = 1)$ .

و برای محاسبه کافیسست دو عدد را با هم xor (bitwise) کنیم...

برای عملیت ضرب هم تابعی نوشتیم که تقریبا معادل رو کتاب برای محاسبه حاصل ضرب در میدان  $GF(2^8)$  است.

برای عمل تقسیم هم یک پارامتر متغیر را در بازه (0x00 , 0Xff) تغییر داده و در عدد اول ضرب میکنیم تا جایی که برابر عدد دوم شود. در این صورت در آن پله از حلقه مقدار آن عدد متغیر همان حاصل تقسیم عدد دوم به اول است.

توضیحات و نحوه اجرای کد تقریبا روشن است و با اجرای آن توضیحات فوق روشن تر خواهد شد.

