سیدمحمدرضا حسینی - 97243129

سیدعباس میرقاسمی - 97243068

در این تمرین یک سیستم کامل برای اجرای هم طراحی رمزنگاری به شیوه RSA را پیاده سازی کردیم.

با توجه به اینکه در صورت تمرین اعلام شده بود باید از شیوه memory-mapped برای برقراری ارتباط میان سخت افزار و نرم افزار استفاده کنیم ما از همین شیوه memory-mapped استفاده کردیم و مانند مثال کتاب آدرس هایی از حافظه را انتخاب کردیم تا میان سخت افزار و نرم افزار بتوانیم ارتباطی ایجاد کنیم. همچنین طبق مثال کتاب تعریف های حافظه نیز در کد gezel انجام شد. همچنین متغیرهای volatile نیز در سمت نرم‌افزار تعریف کردیم که با استفاده از اشاره گر به خانه های حافظه متناظر با آن اشاره می کرد. حال فقط نیاز داشتیم تا یک پروتکل ارتباطی بین سخت افزار و نرم افزار را طراحی و پیاده سازی کنیم. در این حالت ما باید به سخت افزار به هنگام آماده شدن دیتا در نرم‌افزار اطلاع بدهیم تا پارامترهای ورودی بگیرد به همین علت نیز پورتی به نام req قرار دادیم تا این آماده شدن دیتا را به سخت افزار اطلاع بدهد. حال بعد از خواندن پارامترهای ورودی از حافظه نیاز بود تا ورودی داده شده را رمزگذاری کنیم و بعد از آن نیز آن را رمز گشایی کنیم تا زمانی که خروجی های ما شامل cipher و plaint که حاصل از رمزگذاری و رمزگشایی هستند آماده شوند لازم است تا بخش نرم‌افزاری صبر کند. برای همین یک پورت دیگر نیز به نام ack میان سخت افزار و نرم افزار تعریف کردیم تا بر اساس وضعیتی که ماشین حالت سخت افزار تعیین می‌کند نرم افزار صبر کند تا نتایج آماده شود و در خانه های حافظه قرار بگیرد. همچنین برای سادگی تمام ورودی هایی که لازم بود از طریق نرم افزار به سخت افزار داده شود را نیز به صورت جدا در حافظه قرارداد دادیم. برای اجرای ما دو بخش مجزا برای اجرا داشتیم. یک بخش کد c و تبدیل آن به یک برنامه برای کد fdl. و بخش دیگر اجرای کد fdl و خروجی گرفتن از آن.

از دستورهای زیر برای این کار استفاده کردیم:

arm-linux-gcc -static main.c -o main

gplatform model.fdl

همچنین برای اجرای این برنامه نیاز به نصب برنامه هایی در سیستم عامل بود که ما آن را انجام دادیم و در نهایت یک ایمیج داکری برای ساده تر شدن وضعیتمان ایجاد کردیم تا راحت تر بتوانیم کد های مان را کامپایل و اجرا کنیم:

ایمیج داکری ایجاد شده:

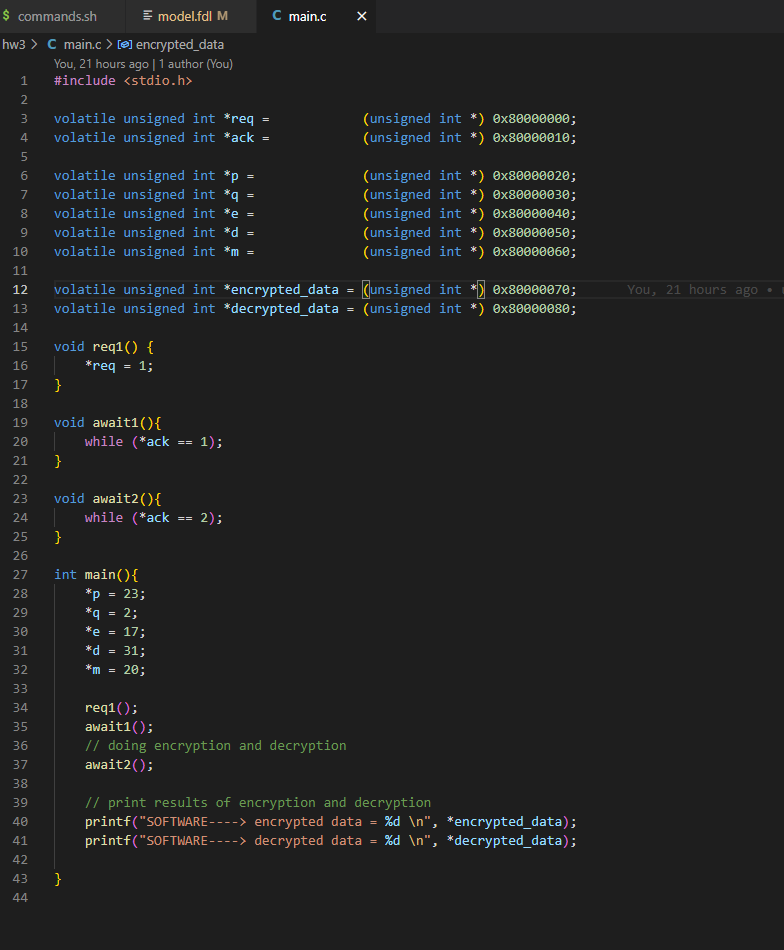
samirghasemi/gezel:3.1.1

docker run -it -v $HOME/Documents/gezel:/opt/src samirghasemi/gezel:3.1.1

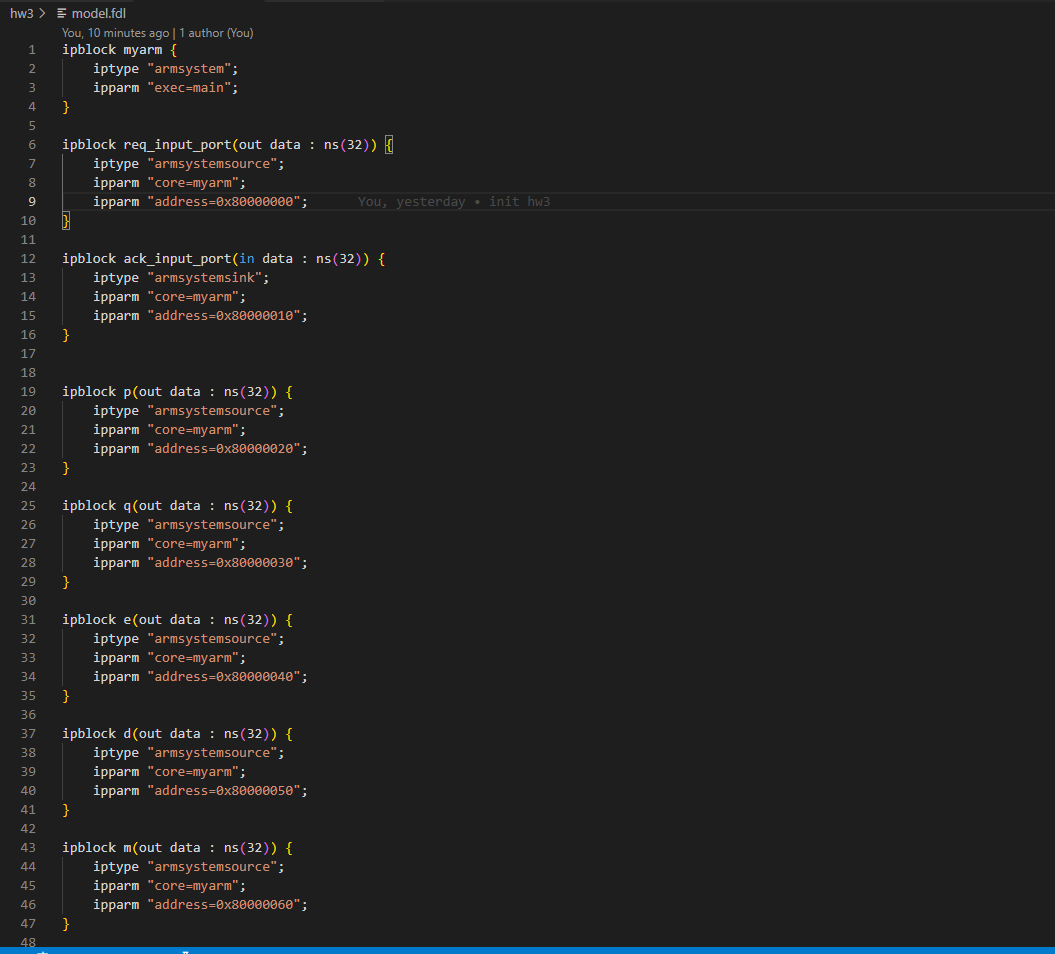
نکته:

کد fdl و کد c به صورت کامل کامنت گذاری شده است. این فایل ها نیز به پیوست خدمت تان ارسال میگردد.

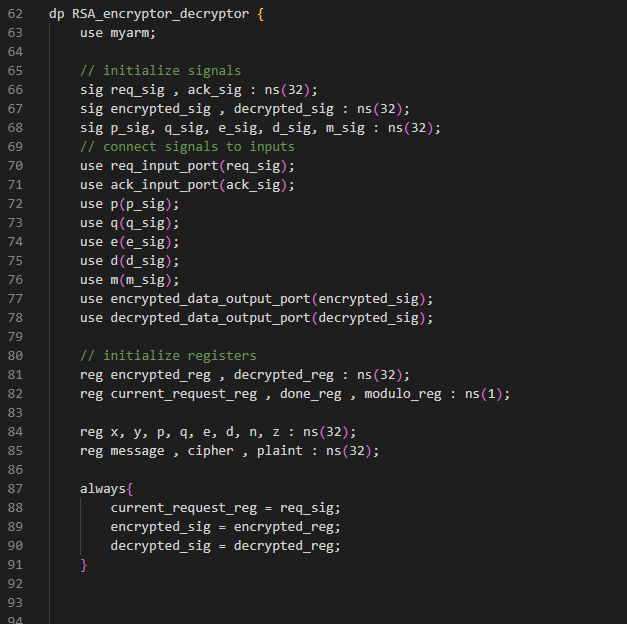
کد c



کد fdl:

بخشی از پیاده سازی ipblock برای اختصاص حافظه مشترک بین سخت افزار و نرم افزار

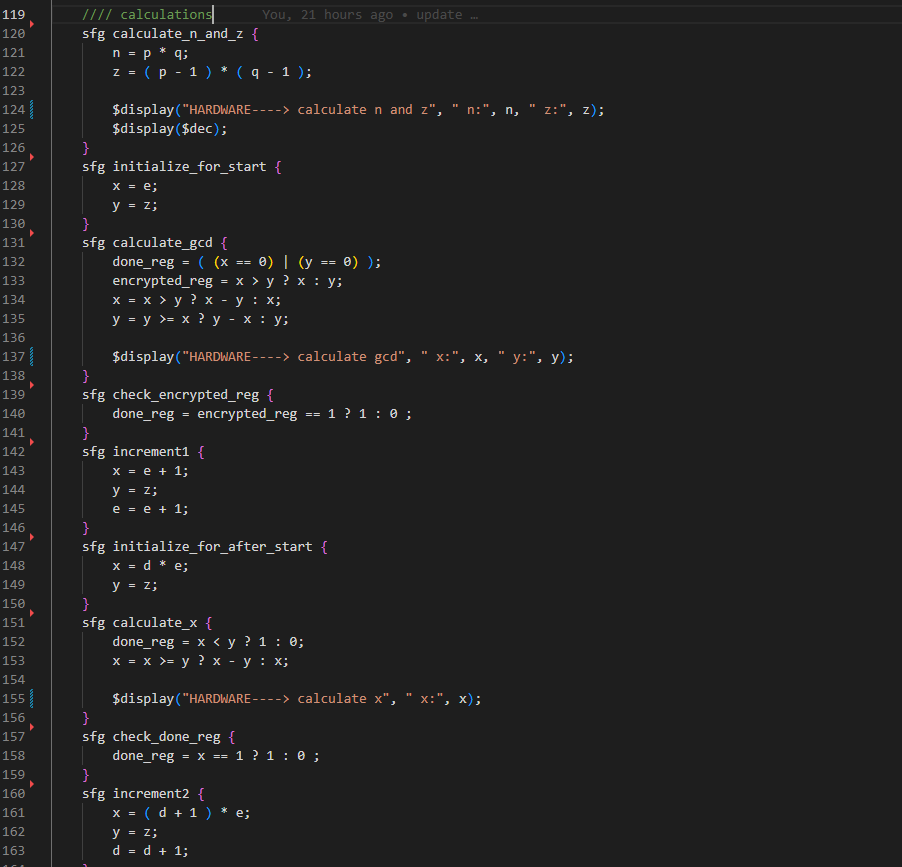
اتصالات اولیه:



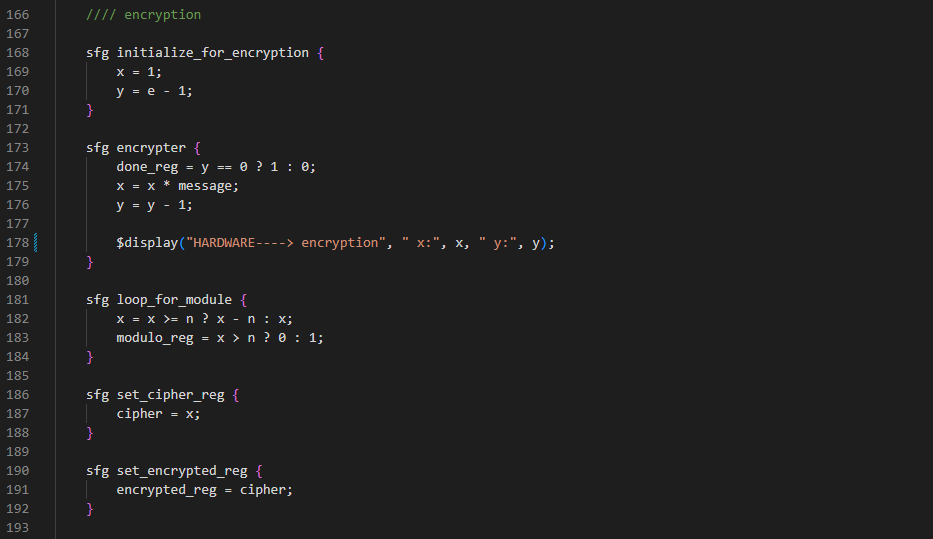
Sfg برای مقداردهی ack ها و خواندن دیتا اولیه از روی پورت ها:



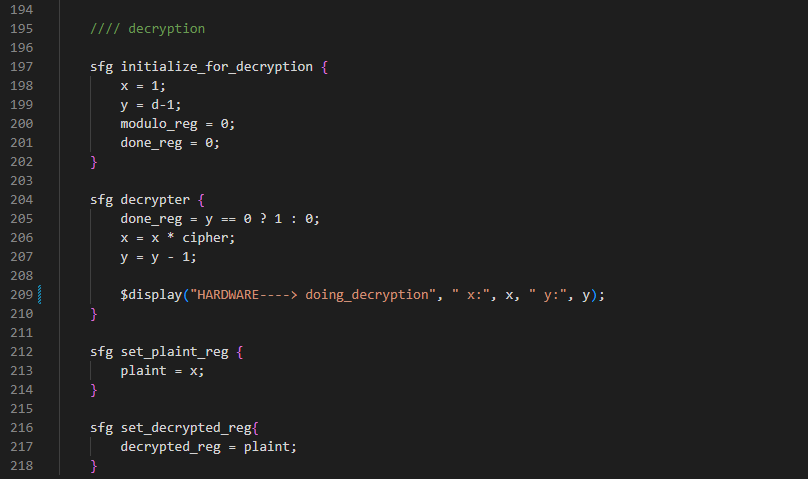
Sfg برای انجام محاسبات اولیه در رمزگذاری و رمزگشایی



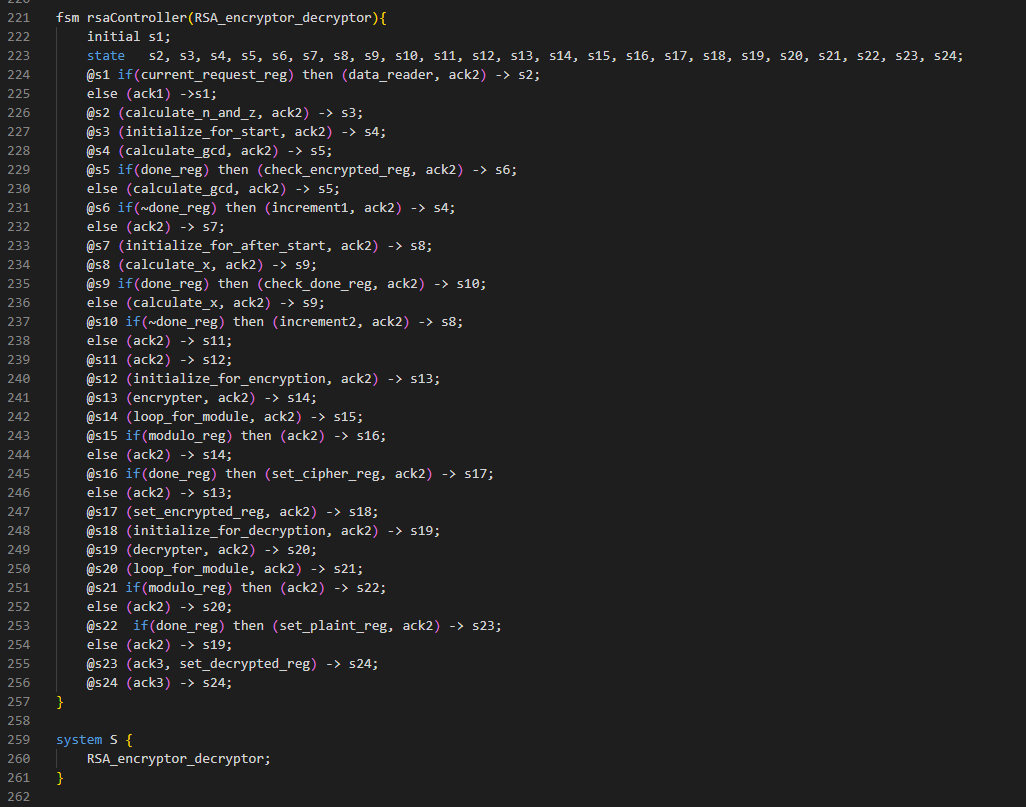
Sfg های بخش رمزگذاری:



Sfg های بخش رمزگشایی



بخش state ها:



خروجی های شبیه سازی شده به شرح زیر می باشند:

