پروژه پایانی گسسته

طراحی شده توسط صدرا نصراله و سید محمد حسین هاشمی دانا

در ابتدا در تابع generate_large_prime دو عددی در بازه 16bits میسازیم(برای اینکه ما اسکی کد را رمز گذاری میکنیم و خب عدد اول ما در این بازه کارساز است) و با استفاده از الگوریتم میلر رابین-که با استفاده از هم نهشتی و قضیه فرما ثابت می شود-استفاده میکنیم و تا ۴۰ بار این آزمون را انجام داده تا بسیار خطای این الگوریتم پایین بیاید سپس بار دیگر این مراحل را برای عدد دوم هم انجام داده و مطمئن میشویم که عدد های ما مساوی هم نیستند و پس از آن عدد n را که بر حسب p و q به دست آمده است و phi که تعداد اعداد کوچک تر از n که نسبت به آن اول هم هستند پیدا میکنیم حال ما n و phi را داریم و می توانیم سراغ پیدا کردن e و d برویم که e مساوی است با عددی که بین phi و ۲ است و بر phi اول است و d هم عددی است که ضرب در e باقی مانده آن بر phi مساوی یک باشد وقتی این دو را پیدا کردیم حال میرویم سراغ بخش اصلی کد که گرفتن مسیج از کاربر پیدا کردن کد اسکی هر قسمت آن و فرستادن هر کدام از آنها برای رمز گذاری با کلید های عمومی مان و رمزگشایی با کلید خصوصی مان و دوباره تبدیل کد اسکی به حروف و چاپ پیام رمز گذاری شده

این کد از نظر امنیتی مشکلی نخواهد داشت چون دو عدد اول بزرگ هستند و در نتیجه n عدد بزرگی خواهد بود

اگر n کوچک باشد ما مشکل امنیتی خواهیم داشت و بعد از رمز کردن دیگر نمی‌توانیم با کلید خصوصی به پیام اولیه برسیم زیرا این الگوریتم RSA برای اعدادی جوابگو هست که کوچک تر از n باشند و برای اعداد بزرگ تر از آن به مشکل امنیتی برخورد می‌کند.