



دانشکده مهندسی کامپیوتر

استاد درس: دکتر ابوالفضل دیانت

بهار ۱۴۰۳

## تمرین ایتريم

امنیت سیستم های کامپیوتری

گزارش تمرین

ستاره باباجانی - ملیکا محمدی فخار

۹۹۵۲۲۰۸۶-۹۹۵۲۱۱۰۹



## ۱ سوال اول

در الگوریتم RSA، کلید عمومی به صورت  $(e, n)$  تعریف می شود و پیام  $m$  با استفاده از این کلید عمومی به وسیله این فرمول رمزگذاری می شود:

$$C \equiv m^e \pmod{n} \quad 0 < m < n$$

در اینجا، اگر  $(m, n)$  برابر با ۱ باشد یعنی  $m$  و  $n$  نسبت به هم اول هستند. این ویژگی اهمیت زیادی دارد و به آن نیاز داریم. اگر  $m$  و  $n$  نسبت به هم اول نباشند، به این معناست که  $m$  و  $n$  دارای عوامل مشترکی هستند و ممکن است با تحلیل مسائل مرتبه ی کوچکتر مانند الگوریتم اقلیدس برای محاسبه  $\gcd$ ، حمله کننده بتواند به سادگی پیام رمزگذاری شده را باز کند. هرچند که در ادامه و طبق اسلاید ۴۰ و ۴۱ فصل سوم، طی مقاله Rivest و Shamir و Adleman نشان داده شده که حتی اگر  $m$  و  $n$  نسبت به هم اول نباشند نیز رابطه فوق برقرار است.

## ۲ سوال دوم

میدانیم در RSA پارامتر رمزگذاری  $e$  باید شرط زیر را ارضا کند و در آن برقرار باشد.

$$1 = \gcd(e, \phi(n)) = \gcd(e, (p-1)(q-1))$$

در RSA اعداد اول  $p, q$  متمایز هستند، بنابراین حداقل یکی از آنها فرد است. و در موارد بهتر هردو فرد هستند. بنابراین توان رمزگذاری  $e$  هرگز نمی تواند یک عدد صحیح زوج باشد. زیرا دیگر شرط فوق برقرار نمی ماند و کوچکترین مضرب مشترک دو عدد زوج میدانیم یک نیست و حداقل ۲ میباشد. معمولاً برای انتخاب  $e$ ، عددی اول بزرگ و بدون مشترک اول با تعداد اعداد اولیه کوچکتر استفاده می شود. عدد ۶۵۵۳۷ به عنوان یک انتخاب معمولی برای  $e$  در الگوریتم RSA به کار می رود، چرا که این عدد بزرگ و معتدل است و با اکثر اعداد اول کوچک مشترک اول ندارد.

## ۳ سوال سوم

الگوریتم RSA یکی از الگوریتم های رمزنگاری و امضای دیجیتال محبوب است که بر اساس مسائل محاسباتی مرتبه ی بزرگ مانند مسئله ی عددی اول برپایه ی عملیات ریاضیاتی استوار است. در RSA، دو عدد اول به نام اعداد فرما (Prime Numbers) به عنوان کلیدهای اصلی برای ایجاد کلیدهای عمومی و خصوصی استفاده می شوند. اعداد فرما به دو عدد اول گفته می شوند که در الگوریتم RSA برای تولید کلیدها به کار می روند. این دو عدد عبارتند از:

پارامتر اول  $(p)$ : یک عدد اول که به عنوان یکی از اعداد اصلی در تشکیل کلیدهای RSA استفاده می شود. پارامتر دوم  $(q)$ : یک عدد اول دیگر که نیز به عنوان یکی از اعداد اصلی در تشکیل کلیدها در الگوریتم RSA به کار می رود. سپس از این دو عدد، مقداری به نام ماژول (modulus) تولید می شود که با ضرب دو عدد اول به دست می آید:

$$n = p \times q$$

این مقدار  $n$  به عنوان پارامتر ماژول در کلیدهای RSA استفاده می شود. سپس از مقدار  $n$ ، اعداد دیگری



برای تولید کلیدهای عمومی و خصوصی محاسبه می‌شوند. تولید کلیدهای عمومی و خصوصی در RSA از مبانی نظری تئوری اعداد اول، مختصات و معادلات دیوفانتی استفاده می‌کند. اعداد فرما در اینجا نقش اساسی دارند و امنیت الگوریتم به زیاد بودن اندازه این اعداد فرما مرتبط است، زیرا با افزایش اندازه اعداد فرما، پیچیدگی فرآیند شکستن کلیدها افزایش می‌یابد.

## ۴ سوال چهارم

الگوریتم RSA از عملیات به توان رسانی برای تولید کلیدها و رمزگذاری/رمزگشایی پیام‌ها استفاده می‌کند. در اینجا چند نمونه الگوریتم بهینه برای این عملیات در محیط پیمانانه ای ذکر می‌شود:

### ۱.۴ Square-and-Multiply

این الگوریتم برای به توان رساندن اعداد صحیح به توانهای دیگر استفاده می‌شود. با این الگوریتم می‌توان به سرعت توانهای بزرگتر را محاسبه کرد.  
- این الگوریتم از تقسیم و حاصلضرب برای سریعتر به توان رساندن اعداد استفاده می‌کند.  
- با تجزیه توان به صورت دودویی، هر بیت را از چپ به راست می‌خواند و با توجه به بیت، مراحل از محاسبه را انجام می‌دهد.  
- این الگوریتم به توانهای بزرگ به صورت کارآمد می‌پردازد.  
کاربرد در RSA: در محاسبات RSA، عددی را به توان دلخواه (معمولاً تابع اقتدار عدد پایه) می‌رساند که در کلیدهای عمومی و خصوصی به کار می‌رود.

### ۲.۴ Montgomery Exponentiation

این الگوریتم نیز برای به توان رساندن سریع اعداد در محیط پیمانانه ای استفاده می‌شود و به خصوص برای اعداد بزرگ مؤلفه فرد.  
این الگوریتم از یک عمل تبدیل خاص برای اجتناب از تقسیم و استفاده از ضرب متوالی به منظور افزایش سرعت استفاده می‌کند.  
کاربرد در RSA: در محاسبات RSA، معمولاً از اعداد بزرگ و مؤلفه فرد استفاده می‌شود، بنابراین الگوریتم Exponentiation Montgomery بهینه است.

### ۳.۴ Sliding Window Exponentiation

این الگوریتم نیز یک ترکیب از Square-and-Multiply با بهینه‌سازی‌های اضافی است که برای سرعت بخشیدن به محاسبات به توان رساندن اعداد مورد استفاده قرار می‌گیرد.  
- توان دلخواه را به صورت باینری جدا می‌کند و بر اساس بیت‌های مجموعه شده، محاسبات را انجام می‌دهد.  
- با استفاده از پنجره‌های متغیر، این الگوریتم می‌تواند به صورت موثرتری با توان‌های بزرگ کار کند.



کاربرد در RSA: در محاسبات RSA، این الگوریتم می تواند به سرعت توانهای بزرگتر را محاسبه کرده و در عملیات کلیدی مورد استفاده قرار گیرد.

## ۵ سوال پنجم

اثربخشی سیستم های رمزنگاری کلید عمومی به غیرقابل حل بودن (محاسباتی و نظری) برخی مسائل ریاضی مانند فاکتورسازی اعداد صحیح بستگی دارد. حل این مشکلات زمان بر است، اما معمولاً سریعتر از امتحان کردن همه کلیدهای ممکن با brute force است. بنابراین، کلیدهای نامتقارن برای مقاومت برابر در برابر حمله باید طولانی تر از کلیدهای الگوریتم متقارن باشند. متداول ترین روش ها در برابر کامپیوترهای کوانتومی به اندازه کافی قدرتمند در آینده ضعیف فرض می شوند. کلیدهای RSA ۱۰۲۴ بیتی از نظر قدرت معادل کلیدهای متقارن ۸۰ بیتی، و کلیدهای RSA ۲۰۴۸ بیتی با کلیدهای بلوکی ۱۱۲ بیتی معادل می باشند.

## ۶ سوال ششم

RSA یک الگوریتم رمزنگاری اسقاطی است که بر اساس مسائل اعداد اول بزرگ استوار است. فرایند تولید اعداد اول در RSA به شکل زیر است:

- ۱) انتخاب دو عدد اول بزرگ  $(p, q)$ : و ابتدا دو عدد اول بزرگ و مختلف به صورت تصادفی انتخاب می شوند. این دو عدد باید بسیار بزرگ باشند تا فرایند فاکتورگیری (تجزیه به عوامل اول) برای یک شخص ثالث زمان بر شود.
- ۲) محاسبه مقدار  $N$ : مقدار  $N$  برابر با حاصلضرب دو عدد اول  $p$  و  $q$  می شود:  $N = p \times q$  این مقدار  $N$  برای ایجاد کلیدهای رمزنگاری و رمزگشایی در الگوریتم RSA استفاده می شود.
- ۳) محاسبه تابع فای آیلر (Euler's Totient Function):  
تابع فای آیلر  $\phi(N)$  از رابطه زیر محاسبه می شود:  $\phi(N) = (p-1)(q-1)$   
این تابع مهم است زیرا تاثیر مستقیم در انتخاب کلیدهای رمزنگاری دارد.
- ۴) انتخاب عددی برای کلید عمومی  $(e)$ :  
عددی که با تابع فای آیلر نسبتی اول باشد، به عنوان کلید عمومی انتخاب می شود. معمولاً اعدادی از خانواده اعداد اول مانند ۳، ۵، ۷، ۱۱، ۱۳، ۱۷، ۱۹، ۲۳، ۲۹، ۳۱، ۳۷، ۴۱، ۴۳، ۴۷، ۵۳، ۵۹، ۶۷، ۷۱، ۷۳، ۷۹، ۸۳، ۸۹، ۹۷، ۱۰۱، ۱۰۳، ۱۰۷، ۱۰۹، ۱۱۳، ۱۲۷، ۱۳۱، ۱۳۷، ۱۳۹، ۱۴۳، ۱۴۹، ۱۵۷، ۱۶۳، ۱۶۷، ۱۷۳، ۱۷۹، ۱۸۷، ۱۹۱، ۱۹۳، ۱۹۷، ۲۱۱، ۲۲۳، ۲۲۷، ۲۲۹، ۲۳۳، ۲۳۹، ۲۴۱، ۲۴۷، ۲۵۱، ۲۵۷، ۲۶۳، ۲۶۹، ۲۷۱، ۲۷۳، ۲۷۹، ۲۸۱، ۲۸۷، ۲۹۱، ۲۹۳، ۲۹۷، ۳۱۱، ۳۱۳، ۳۱۷، ۳۳۱، ۳۳۷، ۳۳۹، ۳۴۱، ۳۴۷، ۳۴۹، ۳۵۳، ۳۵۹، ۳۶۷، ۳۷۱، ۳۷۳، ۳۷۹، ۳۸۱، ۳۸۷، ۳۹۱، ۳۹۳، ۳۹۷، ۴۱۱، ۴۱۳، ۴۱۷، ۴۳۱، ۴۳۷، ۴۳۹، ۴۴۱، ۴۴۷، ۴۴۹، ۴۵۳، ۴۵۹، ۴۶۷، ۴۷۱، ۴۷۳، ۴۷۹، ۴۸۱، ۴۸۷، ۴۹۱، ۴۹۳، ۴۹۷، ۵۱۱، ۵۱۳، ۵۱۷، ۵۳۱، ۵۳۷، ۵۳۹، ۵۴۱، ۵۴۷، ۵۴۹، ۵۵۳، ۵۵۹، ۵۶۷، ۵۷۱، ۵۷۳، ۵۷۹، ۵۸۱، ۵۸۷، ۵۹۱، ۵۹۳، ۵۹۷، ۶۱۱، ۶۱۳، ۶۱۷، ۶۳۱، ۶۳۷، ۶۳۹، ۶۴۱، ۶۴۷، ۶۴۹، ۶۵۳، ۶۵۹، ۶۶۷، ۶۷۱، ۶۷۳، ۶۷۹، ۶۸۱، ۶۸۷، ۶۹۱، ۶۹۳، ۶۹۷، ۷۱۱، ۷۱۳، ۷۱۷، ۷۳۱، ۷۳۷، ۷۳۹، ۷۴۱، ۷۴۷، ۷۴۹، ۷۵۳، ۷۵۹، ۷۶۷، ۷۷۱، ۷۷۳، ۷۷۹، ۷۸۱، ۷۸۷، ۷۹۱، ۷۹۳، ۷۹۷، ۸۱۱، ۸۱۳، ۸۱۷، ۸۳۱، ۸۳۷، ۸۳۹، ۸۴۱، ۸۴۷، ۸۴۹، ۸۵۳، ۸۵۹، ۸۶۷، ۸۷۱، ۸۷۳، ۸۷۹، ۸۸۱، ۸۸۷، ۸۹۱، ۸۹۳، ۸۹۷، ۹۱۱، ۹۱۳، ۹۱۷، ۹۳۱، ۹۳۷، ۹۳۹، ۹۴۱، ۹۴۷، ۹۴۹، ۹۵۳، ۹۵۹، ۹۶۷، ۹۷۱، ۹۷۳، ۹۷۹، ۹۸۱، ۹۸۷، ۹۹۱، ۹۹۳، ۹۹۷، ۱۰۱۱، ۱۰۱۳، ۱۰۱۷، ۱۰۳۱، ۱۰۳۷، ۱۰۳۹، ۱۰۴۱، ۱۰۴۷، ۱۰۴۹، ۱۰۵۳، ۱۰۵۹، ۱۰۶۷، ۱۰۷۱، ۱۰۷۳، ۱۰۷۹، ۱۰۸۱، ۱۰۸۷، ۱۰۹۱، ۱۰۹۳، ۱۰۹۷، ۱۱۱۱، ۱۱۱۳، ۱۱۱۷، ۱۱۳۱، ۱۱۳۷، ۱۱۳۹، ۱۱۴۱، ۱۱۴۷، ۱۱۴۹، ۱۱۵۳، ۱۱۵۹، ۱۱۶۷، ۱۱۷۱، ۱۱۷۳، ۱۱۷۹، ۱۱۸۱، ۱۱۸۷، ۱۱۹۱، ۱۱۹۳، ۱۱۹۷، ۱۲۱۱، ۱۲۱۳، ۱۲۱۷، ۱۲۳۱، ۱۲۳۷، ۱۲۳۹، ۱۲۴۱، ۱۲۴۷، ۱۲۴۹، ۱۲۵۳، ۱۲۵۹، ۱۲۶۷، ۱۲۷۱، ۱۲۷۳، ۱۲۷۹، ۱۲۸۱، ۱۲۸۷، ۱۲۹۱، ۱۲۹۳، ۱۲۹۷، ۱۳۱۱، ۱۳۱۳، ۱۳۱۷، ۱۳۳۱، ۱۳۳۷، ۱۳۳۹، ۱۳۴۱، ۱۳۴۷، ۱۳۴۹، ۱۳۵۳، ۱۳۵۹، ۱۳۶۷، ۱۳۷۱، ۱۳۷۳، ۱۳۷۹، ۱۳۸۱، ۱۳۸۷، ۱۳۹۱، ۱۳۹۳، ۱۳۹۷، ۱۴۱۱، ۱۴۱۳، ۱۴۱۷، ۱۴۳۱، ۱۴۳۷، ۱۴۳۹، ۱۴۴۱، ۱۴۴۷، ۱۴۴۹، ۱۴۵۳، ۱۴۵۹، ۱۴۶۷، ۱۴۷۱، ۱۴۷۳، ۱۴۷۹، ۱۴۸۱، ۱۴۸۷، ۱۴۹۱، ۱۴۹۳، ۱۴۹۷، ۱۵۱۱، ۱۵۱۳، ۱۵۱۷، ۱۵۳۱، ۱۵۳۷، ۱۵۳۹، ۱۵۴۱، ۱۵۴۷، ۱۵۴۹، ۱۵۵۳، ۱۵۵۹، ۱۵۶۷، ۱۵۷۱، ۱۵۷۳، ۱۵۷۹، ۱۵۸۱، ۱۵۸۷، ۱۵۹۱، ۱۵۹۳، ۱۵۹۷، ۱۶۱۱، ۱۶۱۳، ۱۶۱۷، ۱۶۳۱، ۱۶۳۷، ۱۶۳۹، ۱۶۴۱، ۱۶۴۷، ۱۶۴۹، ۱۶۵۳، ۱۶۵۹، ۱۶۶۷، ۱۶۷۱، ۱۶۷۳، ۱۶۷۹، ۱۶۸۱، ۱۶۸۷، ۱۶۹۱، ۱۶۹۳، ۱۶۹۷، ۱۷۱۱، ۱۷۱۳، ۱۷۱۷، ۱۷۳۱، ۱۷۳۷، ۱۷۳۹، ۱۷۴۱، ۱۷۴۷، ۱۷۴۹، ۱۷۵۳، ۱۷۵۹، ۱۷۶۷، ۱۷۷۱، ۱۷۷۳، ۱۷۷۹، ۱۷۸۱، ۱۷۸۷، ۱۷۹۱، ۱۷۹۳، ۱۷۹۷، ۱۸۱۱، ۱۸۱۳، ۱۸۱۷، ۱۸۳۱، ۱۸۳۷، ۱۸۳۹، ۱۸۴۱، ۱۸۴۷، ۱۸۴۹، ۱۸۵۳، ۱۸۵۹، ۱۸۶۷، ۱۸۷۱، ۱۸۷۳، ۱۸۷۹، ۱۸۸۱، ۱۸۸۷، ۱۸۹۱، ۱۸۹۳، ۱۸۹۷، ۱۹۱۱، ۱۹۱۳، ۱۹۱۷، ۱۹۳۱، ۱۹۳۷، ۱۹۳۹، ۱۹۴۱، ۱۹۴۷، ۱۹۴۹، ۱۹۵۳، ۱۹۵۹، ۱۹۶۷، ۱۹۷۱، ۱۹۷۳، ۱۹۷۹، ۱۹۸۱، ۱۹۸۷، ۱۹۹۱، ۱۹۹۳، ۱۹۹۷، ۲۰۱۱، ۲۰۱۳، ۲۰۱۷، ۲۰۳۱، ۲۰۳۷، ۲۰۳۹، ۲۰۴۱، ۲۰۴۷، ۲۰۴۹، ۲۰۵۳، ۲۰۵۹، ۲۰۶۷، ۲۰۷۱، ۲۰۷۳، ۲۰۷۹، ۲۰۸۱، ۲۰۸۷، ۲۰۹۱، ۲۰۹۳، ۲۰۹۷، ۲۱۱۱، ۲۱۱۳، ۲۱۱۷، ۲۱۳۱، ۲۱۳۷، ۲۱۳۹، ۲۱۴۱، ۲۱۴۷، ۲۱۴۹، ۲۱۵۳، ۲۱۵۹، ۲۱۶۷، ۲۱۷۱، ۲۱۷۳، ۲۱۷۹، ۲۱۸۱، ۲۱۸۷، ۲۱۹۱، ۲۱۹۳، ۲۱۹۷، ۲۲۱۱، ۲۲۱۳، ۲۲۱۷، ۲۲۳۱، ۲۲۳۷، ۲۲۳۹، ۲۲۴۱، ۲۲۴۷، ۲۲۴۹، ۲۲۵۳، ۲۲۵۹، ۲۲۶۷، ۲۲۷۱، ۲۲۷۳، ۲۲۷۹، ۲۲۸۱، ۲۲۸۷، ۲۲۹۱، ۲۲۹۳، ۲۲۹۷، ۲۳۱۱، ۲۳۱۳، ۲۳۱۷، ۲۳۳۱، ۲۳۳۷، ۲۳۳۹، ۲۳۴۱، ۲۳۴۷، ۲۳۴۹، ۲۳۵۳، ۲۳۵۹، ۲۳۶۷، ۲۳۷۱، ۲۳۷۳، ۲۳۷۹، ۲۳۸۱، ۲۳۸۷، ۲۳۹۱، ۲۳۹۳، ۲۳۹۷، ۲۴۱۱، ۲۴۱۳، ۲۴۱۷، ۲۴۳۱، ۲۴۳۷، ۲۴۳۹، ۲۴۴۱، ۲۴۴۷، ۲۴۴۹، ۲۴۵۳، ۲۴۵۹، ۲۴۶۷، ۲۴۷۱، ۲۴۷۳، ۲۴۷۹، ۲۴۸۱، ۲۴۸۷، ۲۴۹۱، ۲۴۹۳، ۲۴۹۷، ۲۵۱۱، ۲۵۱۳، ۲۵۱۷، ۲۵۳۱، ۲۵۳۷، ۲۵۳۹، ۲۵۴۱، ۲۵۴۷، ۲۵۴۹، ۲۵۵۳، ۲۵۵۹، ۲۵۶۷، ۲۵۷۱، ۲۵۷۳، ۲۵۷۹، ۲۵۸۱، ۲۵۸۷، ۲۵۹۱، ۲۵۹۳، ۲۵۹۷، ۲۶۱۱، ۲۶۱۳، ۲۶۱۷، ۲۶۳۱، ۲۶۳۷، ۲۶۳۹، ۲۶۴۱، ۲۶۴۷، ۲۶۴۹، ۲۶۵۳، ۲۶۵۹، ۲۶۶۷، ۲۶۷۱، ۲۶۷۳، ۲۶۷۹، ۲۶۸۱، ۲۶۸۷، ۲۶۹۱، ۲۶۹۳، ۲۶۹۷، ۲۷۱۱، ۲۷۱۳، ۲۷۱۷، ۲۷۳۱، ۲۷۳۷، ۲۷۳۹، ۲۷۴۱، ۲۷۴۷، ۲۷۴۹، ۲۷۵۳، ۲۷۵۹، ۲۷۶۷، ۲۷۷۱، ۲۷۷۳، ۲۷۷۹، ۲۷۸۱، ۲۷۸۷، ۲۷۹۱، ۲۷۹۳، ۲۷۹۷، ۲۸۱۱، ۲۸۱۳، ۲۸۱۷، ۲۸۳۱، ۲۸۳۷، ۲۸۳۹، ۲۸۴۱، ۲۸۴۷، ۲۸۴۹، ۲۸۵۳، ۲۸۵۹، ۲۸۶۷، ۲۸۷۱، ۲۸۷۳، ۲۸۷۹، ۲۸۸۱، ۲۸۸۷، ۲۸۹۱، ۲۸۹۳، ۲۸۹۷، ۲۹۱۱، ۲۹۱۳، ۲۹۱۷، ۲۹۳۱، ۲۹۳۷، ۲۹۳۹، ۲۹۴۱، ۲۹۴۷، ۲۹۴۹، ۲۹۵۳، ۲۹۵۹، ۲۹۶۷، ۲۹۷۱، ۲۹۷۳، ۲۹۷۹، ۲۹۸۱، ۲۹۸۷، ۲۹۹۱، ۲۹۹۳، ۲۹۹۷، ۳۰۱۱، ۳۰۱۳، ۳۰۱۷، ۳۰۳۱، ۳۰۳۷، ۳۰۳۹، ۳۰۴۱، ۳۰۴۷، ۳۰۴۹، ۳۰۵۳، ۳۰۵۹، ۳۰۶۷، ۳۰۷۱، ۳۰۷۳، ۳۰۷۹، ۳۰۸۱، ۳۰۸۷، ۳۰۹۱، ۳۰۹۳، ۳۰۹۷، ۳۱۱۱، ۳۱۱۳، ۳۱۱۷، ۳۱۳۱، ۳۱۳۷، ۳۱۳۹، ۳۱۴۱، ۳۱۴۷، ۳۱۴۹، ۳۱۵۳، ۳۱۵۹، ۳۱۶۷، ۳۱۷۱، ۳۱۷۳، ۳۱۷۹، ۳۱۸۱، ۳۱۸۷، ۳۱۹۱، ۳۱۹۳، ۳۱۹۷، ۳۲۱۱، ۳۲۱۳، ۳۲۱۷، ۳۲۳۱، ۳۲۳۷، ۳۲۳۹، ۳۲۴۱، ۳۲۴۷، ۳۲۴۹، ۳۲۵۳، ۳۲۵۹، ۳۲۶۷، ۳۲۷۱، ۳۲۷۳، ۳۲۷۹، ۳۲۸۱، ۳۲۸۷، ۳۲۹۱، ۳۲۹۳، ۳۲۹۷، ۳۳۱۱، ۳۳۱۳، ۳۳۱۷، ۳۳۳۱، ۳۳۳۷، ۳۳۳۹، ۳۳۴۱، ۳۳۴۷، ۳۳۴۹، ۳۳۵۳، ۳۳۵۹، ۳۳۶۷، ۳۳۷۱، ۳۳۷۳، ۳۳۷۹، ۳۳۸۱، ۳۳۸۷، ۳۳۹۱، ۳۳۹۳، ۳۳۹۷، ۳۴۱۱، ۳۴۱۳، ۳۴۱۷، ۳۴۳۱، ۳۴۳۷، ۳۴۳۹، ۳۴۴۱، ۳۴۴۷، ۳۴۴۹، ۳۴۵۳، ۳۴۵۹، ۳۴۶۷، ۳۴۷۱، ۳۴۷۳، ۳۴۷۹، ۳۴۸۱، ۳۴۸۷، ۳۴۹۱، ۳۴۹۳، ۳۴۹۷، ۳۵۱۱، ۳۵۱۳، ۳۵۱۷، ۳۵۳۱، ۳۵۳۷، ۳۵۳۹، ۳۵۴۱، ۳۵۴۷، ۳۵۴۹، ۳۵۵۳، ۳۵۵۹، ۳۵۶۷، ۳۵۷۱، ۳۵۷۳، ۳۵۷۹، ۳۵۸۱، ۳۵۸۷، ۳۵۹۱، ۳۵۹۳، ۳۵۹۷، ۳۶۱۱، ۳۶۱۳، ۳۶۱۷، ۳۶۳۱، ۳۶۳۷، ۳۶۳۹، ۳۶۴۱، ۳۶۴۷، ۳۶۴۹، ۳۶۵۳، ۳۶۵۹، ۳۶۶۷، ۳۶۷۱، ۳۶۷۳، ۳۶۷۹، ۳۶۸۱، ۳۶۸۷، ۳۶۹۱، ۳۶۹۳، ۳۶۹۷، ۳۷۱۱، ۳۷۱۳، ۳۷۱۷، ۳۷۳۱، ۳۷۳۷، ۳۷۳۹، ۳۷۴۱، ۳۷۴۷، ۳۷۴۹، ۳۷۵۳، ۳۷۵۹، ۳۷۶۷، ۳۷۷۱، ۳۷۷۳، ۳۷۷۹، ۳۷۸۱، ۳۷۸۷، ۳۷۹۱، ۳۷۹۳، ۳۷۹۷، ۳۸۱۱، ۳۸۱۳، ۳۸۱۷، ۳۸۳۱، ۳۸۳۷، ۳۸۳۹، ۳۸۴۱، ۳۸۴۷، ۳۸۴۹، ۳۸۵۳، ۳۸۵۹، ۳۸۶۷، ۳۸۷۱، ۳۸۷۳، ۳۸۷۹، ۳۸۸۱، ۳۸۸۷، ۳۸۹۱، ۳۸۹۳، ۳۸۹۷، ۳۹۱۱، ۳۹۱۳، ۳۹۱۷، ۳۹۳۱، ۳۹۳۷، ۳۹۳۹، ۳۹۴۱، ۳۹۴۷، ۳۹۴۹، ۳۹۵۳، ۳۹۵۹، ۳۹۶۷، ۳۹۷۱، ۳۹۷۳، ۳۹۷۹، ۳۹۸۱، ۳۹۸۷، ۳۹۹۱، ۳۹۹۳، ۳۹۹۷، ۴۰۱۱، ۴۰۱۳، ۴۰۱۷، ۴۰۳۱، ۴۰۳۷، ۴۰۳۹، ۴۰۴۱، ۴۰۴۷، ۴۰۴۹، ۴۰۵۳، ۴۰۵۹، ۴۰۶۷، ۴۰۷۱، ۴۰۷۳، ۴۰۷۹، ۴۰۸۱، ۴۰۸۷، ۴۰۹۱، ۴۰۹۳، ۴۰۹۷، ۴۱۱۱، ۴۱۱۳، ۴۱۱۷، ۴۱۳۱، ۴۱۳۷، ۴۱۳۹، ۴۱۴۱، ۴۱۴۷، ۴۱۴۹، ۴۱۵۳، ۴۱۵۹، ۴۱۶۷، ۴۱۷۱، ۴۱۷۳، ۴۱۷۹، ۴۱۸۱، ۴۱۸۷، ۴۱۹۱، ۴۱۹۳، ۴۱۹۷، ۴۲۱۱، ۴۲۱۳، ۴۲۱۷، ۴۲۳۱، ۴۲۳۷، ۴۲۳۹، ۴۲۴۱، ۴۲۴۷، ۴۲۴۹، ۴۲۵۳، ۴۲۵۹، ۴۲۶۷، ۴۲۷۱، ۴۲۷۳، ۴۲۷۹، ۴۲۸۱، ۴۲۸۷، ۴۲۹۱، ۴۲۹۳، ۴۲۹۷، ۴۳۱۱، ۴۳۱۳، ۴۳۱۷، ۴۳۳۱، ۴۳۳۷، ۴۳۳۹، ۴۳۴۱، ۴۳۴۷، ۴۳۴۹، ۴۳۵۳، ۴۳۵۹، ۴۳۶۷، ۴۳۷۱، ۴۳۷۳، ۴۳۷۹، ۴۳۸۱، ۴۳۸۷، ۴۳۹۱، ۴۳۹۳، ۴۳۹۷، ۴۴۱۱، ۴۴۱۳، ۴۴۱۷، ۴۴۳۱، ۴۴۳۷، ۴۴۳۹، ۴۴۴۱، ۴۴۴۷، ۴۴۴۹، ۴۴۵۳، ۴۴۵۹، ۴۴۶۷، ۴۴۷۱، ۴۴۷۳، ۴۴۷۹، ۴۴۸۱، ۴۴۸۷، ۴۴۹۱، ۴۴۹۳، ۴۴۹۷، ۴۵۱۱، ۴۵۱۳، ۴۵۱۷، ۴۵۳۱، ۴۵۳۷، ۴۵۳۹، ۴۵۴۱، ۴۵۴۷، ۴۵۴۹، ۴۵۵۳، ۴۵۵۹، ۴۵۶۷، ۴۵۷۱، ۴۵۷۳، ۴۵۷۹، ۴۵۸۱، ۴۵۸۷، ۴۵۹۱، ۴۵۹۳، ۴۵۹۷، ۴۶۱۱، ۴۶۱۳، ۴۶۱۷، ۴۶۳۱، ۴۶۳۷، ۴۶۳۹، ۴۶۴۱، ۴۶۴۷، ۴۶۴۹، ۴۶۵۳، ۴۶۵۹، ۴۶۶۷، ۴۶۷۱، ۴۶۷۳، ۴۶۷۹، ۴۶۸۱، ۴۶۸۷، ۴۶۹۱، ۴۶۹۳، ۴۶۹۷، ۴۷۱۱، ۴۷۱۳، ۴۷۱۷، ۴۷۳۱، ۴۷۳۷، ۴۷۳۹، ۴۷۴۱، ۴۷۴۷، ۴۷۴۹، ۴۷۵۳، ۴۷۵۹، ۴۷۶۷، ۴۷۷۱، ۴۷۷۳، ۴۷۷۹، ۴۷۸۱، ۴۷۸۷، ۴۷۹۱، ۴۷۹۳، ۴۷۹۷، ۴۸۱۱، ۴۸۱۳، ۴۸۱۷، ۴۸۳۱، ۴۸۳۷، ۴۸۳۹، ۴۸۴۱، ۴۸۴۷، ۴۸۴۹، ۴۸۵۳، ۴۸۵۹، ۴۸۶۷، ۴۸۷۱، ۴۸۷۳، ۴۸۷۹، ۴۸۸۱، ۴۸۸۷، ۴۸۹۱، ۴۸۹۳، ۴۸۹۷، ۴۹۱۱، ۴۹۱۳، ۴۹۱۷، ۴۹۳۱، ۴۹۳۷، ۴۹۳۹، ۴۹۴۱، ۴۹۴۷، ۴۹۴۹، ۴۹۵۳، ۴۹۵۹، ۴۹۶۷، ۴۹۷۱، ۴۹۷۳، ۴۹۷۹، ۴۹۸۱، ۴۹۸۷، ۴۹۹۱، ۴۹۹۳، ۴۹۹۷، ۵۰۱۱، ۵۰۱۳، ۵۰۱۷، ۵۰۳۱، ۵۰۳۷، ۵۰۳۹، ۵۰۴۱، ۵۰۴۷، ۵۰۴۹، ۵۰۵۳، ۵۰۵۹، ۵۰۶۷، ۵۰۷۱، ۵۰۷۳، ۵۰۷۹، ۵۰۸۱، ۵۰۸۷، ۵۰۹۱، ۵۰۹۳، ۵۰۹۷، ۵۱۱۱، ۵۱۱۳، ۵۱۱۷، ۵۱۳۱، ۵۱۳۷، ۵۱۳۹، ۵۱۴۱، ۵۱۴۷، ۵۱۴۹، ۵۱۵۳، ۵۱۵۹، ۵۱۶۷، ۵۱۷۱، ۵۱۷۳، ۵۱۷۹، ۵۱۸۱، ۵۱۸۷، ۵۱۹۱، ۵۱۹۳، ۵۱۹۷، ۵۲۱۱، ۵۲۱۳، ۵۲۱۷، ۵۲۳۱، ۵۲۳۷، ۵۲۳۹، ۵۲۴۱، ۵۲۴۷، ۵۲۴۹، ۵۲۵۳، ۵۲۵۹، ۵۲۶۷، ۵۲۷۱، ۵۲۷۳، ۵۲۷۹، ۵۲۸۱، ۵۲۸۷، ۵۲۹۱، ۵۲۹۳، ۵۲۹۷، ۵۳۱۱، ۵۳۱۳، ۵۳۱۷، ۵۳۳۱، ۵۳۳۷، ۵۳۳۹، ۵۳۴۱، ۵۳۴۷، ۵۳۴۹، ۵۳۵۳، ۵۳۵۹، ۵۳۶۷، ۵۳۷۱، ۵۳۷۳، ۵۳۷۹، ۵۳۸۱، ۵۳۸۷، ۵۳۹۱، ۵۳۹۳، ۵۳۹۷، ۵۴۱۱، ۵۴۱۳، ۵۴۱۷، ۵۴۳۱، ۵۴۳۷، ۵۴۳۹، ۵۴۴۱، ۵۴۴۷، ۵۴۴۹، ۵۴۵۳، ۵۴۵۹، ۵۴۶۷، ۵۴۷۱، ۵۴۷۳، ۵۴۷۹، ۵۴۸۱، ۵۴۸۷، ۵۴۹۱، ۵۴۹۳، ۵۴۹۷، ۵۵۱۱، ۵۵۱۳، ۵۵۱۷، ۵۵۳۱، ۵۵۳۷، ۵۵۳۹، ۵۵۴۱، ۵۵۴۷، ۵۵۴۹، ۵۵۵۳، ۵۵۵۹، ۵۵۶۷، ۵۵۷۱، ۵۵۷۳، ۵۵۷۹، ۵۵۸۱، ۵۵۸۷، ۵۵۹۱، ۵۵۹۳، ۵۵۹۷، ۵۶۱۱، ۵۶۱۳، ۵۶۱۷، ۵۶۳۱، ۵۶۳۷، ۵۶۳۹، ۵۶۴۱، ۵۶۴۷، ۵۶۴۹، ۵۶۵۳، ۵۶۵۹، ۵۶۶۷، ۵۶۷۱، ۵۶۷۳، ۵۶۷۹، ۵۶۸۱، ۵۶۸۷، ۵۶۹۱، ۵۶۹۳، ۵۶۹۷، ۵۷۱۱، ۵۷۱۳، ۵۷۱۷، ۵۷۳۱، ۵۷۳۷، ۵۷۳۹، ۵۷۴۱، ۵۷۴۷، ۵۷۴۹، ۵۷۵۳، ۵۷۵۹، ۵۷۶۷، ۵۷۷۱، ۵۷۷۳، ۵۷۷۹، ۵۷۸۱، ۵۷۸۷، ۵۷۹۱، ۵۷۹۳، ۵۷۹۷، ۵۸۱۱، ۵۸۱۳، ۵۸۱۷، ۵۸۳۱، ۵۸۳۷، ۵۸۳۹، ۵۸۴۱، ۵۸۴۷، ۵۸۴۹، ۵۸۵۳، ۵۸۵۹، ۵۸۶۷، ۵۸۷۱، ۵۸۷۳، ۵۸۷۹، ۵۸۸۱، ۵۸۸۷، ۵۸۹۱، ۵۸۹۳، ۵۸۹۷، ۵۹۱۱، ۵۹۱۳، ۵۹۱۷، ۵۹۳۱، ۵۹۳۷، ۵۹۳۹، ۵۹۴۱، ۵۹۴۷،



الگوریتم به صورت خلاصه به شرح زیر است:

(۱) انتخاب یک محدوده:

ابتدا یک بازه از اعداد صحیح بزرگ انتخاب می شود. این بازه ممکن است بسیار وسیع باشد.

(۲) استفاده از الگوریتم اراتوستن:

از الگوریتم اراتوستن برای تولید اعداد اول در این بازه استفاده می شود. این الگوریتم به این صورت عمل می کند که ابتدا یک لیست از اعداد از ۲ تا حداکثر عدد در بازه ایجاد می شود. سپس اعداد غیراول از لیست حذف می شوند.

(۳) انتخاب تصادفی:

از میان اعداد اول بازه، دو عدد اول تصادفی  $p$  و  $q$  انتخاب می شوند. این دو عدد به عنوان اعداد اول  $p$  و  $q$  برای الگوریتم RSA استفاده می شوند.

(۴) بررسی اندازه اعداد انتخابی:

اعداد انتخابی باید بسیار بزرگ باشند تا فرآیند فاکتورگیری توسط حمله های کلید عمومی مانند حمله فاکتورگیری Fermat-Kraitichik کارایی نداشته باشد.