گزارش نهایی پروژه RSA

۰۱ مقدمه

رمزنگاری یکی از پایه‌های اصلی امنیت اطلاعات است که نقش مهمی در حفاظت از داده‌ها هنگام انتقال ایفا می‌کند. الگوریتم RSA، که در سال ۱۹۷۷ توسط ریوست، شامیر و آدلمن معرفی شد، یکی از پرکاربردترین روش‌های رمزنگاری نامتقارن است. این الگوریتم بر پایه دشواری تجزیه یک عدد بسیار بزرگ به عوامل اول خود استوار است و به دلیل امنیت بالا در حوزه‌هایی مانند بانکداری آنلاین، امضای دیجیتال و پروتکل‌های امنیتی مانند SSL/TLS به طور گسترده استفاده می‌شود.

۰۲ مبانی نظری الگوریتم RSA

الگوریتم RSA از مفاهیم ریاضی مانند نظریه اعداد و خواص اعداد اول بهره می‌برد. این الگوریتم از دو کلید استفاده می‌کند: کلید عمومی برای رمزنگاری و کلید خصوصی برای رمزگشایی. امنیت RSA به سختی مسئله لگاریتم گسسته و تجزیه اعداد بزرگ وابسته است. مراحل تولید کلید در RSA به شرح زیر است:

۱. انتخاب دو عدد اول بزرگ P و Q با استفاده از الگوریتم‌های تست اول بودن مانند میلر-رابین.

۲. محاسبه عدد N با استفاده از رابطه:

$$N = P \times Q$$

۳. محاسبه تابع اویلر:

$$\phi(N) = (P-1)(Q-1)$$

۴. انتخاب کلید عمومی e به‌گونه‌ای که:

$$1 < e < \phi(N) \quad \text{و} \quad \gcd(e, \phi(N)) = 1$$

۵. محاسبه کلید خصوصی d با استفاده از رابطه:

$$d \equiv e^{-1} \pmod{\phi(N)}$$

۰۱۰۲ الگوریتم میلر-رابین

الگوریتم میلر-رابین یک روش احتمالاتی برای تست اول بودن اعداد است که به دلیل سرعت و دقت بالا در تولید اعداد اول بزرگ مورد استفاده قرار می‌گیرد. این الگوریتم بر پایه قضیه کوچک فرما و ویژگی‌های اعداد اول عمل می‌کند. در این روش، عدد مورد نظر به‌صورت $n-1 = 2^k \cdot m$ نوشته می‌شود و سپس با انتخاب چند پایه تصادفی، بررسی می‌شود که آیا عدد رفتار یک عدد اول را دارد یا خیر. اگر عدد در چندین دور آزمایش، ویژگی‌های عدد اول را نشان دهد، با احتمال بسیار بالا اول است. این الگوریتم به‌ویژه برای اعداد بزرگ که در RSA استفاده می‌شوند، بسیار کارآمد است.

۳. فرآیند رمزنگاری و رمزگشایی

در الگوریتم RSA، فرآیند رمزنگاری و رمزگشایی به‌صورت زیر انجام می‌شود:

- **رمزنگاری:** پیام M (که به‌صورت عددی نمایش داده می‌شود) با استفاده از کلید عمومی e و عدد N به شکل زیر رمز می‌شود:

$$C = M^e \pmod{N}$$

- **رمزگشایی:** پیام رمز شده C با استفاده از کلید خصوصی d و عدد N به پیام اصلی بازمی‌گردد:

$$M = C^d \pmod{N}$$

۴. پیاده‌سازی در پایتون

در این پروژه، الگوریتم RSA با استفاده از زبان برنامه‌نویسی پایتون پیاده‌سازی شده است. مراحل اصلی پیاده‌سازی شامل موارد زیر است:

- تولید اعداد اول بزرگ با استفاده از الگوریتم میلر-رابین برای اطمینان از تصادفی بودن و امنیت کلیدها.
- محاسبه N و $\phi(N)$ بر اساس اعداد اول انتخاب‌شده.
- تولید کلید عمومی (e) و کلید خصوصی (d) با استفاده از الگوریتم اقلیدس توسعه‌یافته.
- پیاده‌سازی توابع رمزنگاری و رمزگشایی برای تبدیل پیام‌ها به حالت رمز شده و بازیابی پیام اصلی.

۵. نتایج اجرای برنامه

با اجرای برنامه، کاربر می‌تواند یک پیام عددی وارد کند و نسخه رمز شده آن را مشاهده کند. سپس، با استفاده از کلید خصوصی، پیام رمزگشایی شده و به شکل اصلی خود بازمی‌گردد. این فرآیند نشان‌دهنده صحت و دقت پیاده‌سازی الگوریتم RSA در این پروژه است. همچنین، استفاده از الگوریتم میلر-رابین برای تولید اعداد اول، سرعت و امنیت فرآیند تولید کلید را به‌طور قابل‌توجهی بهبود بخشیده است.

۶. نتیجه‌گیری

الگوریتم RSA به دلیل امنیت بالا و اتکا به دشواری تجزیه اعداد بزرگ به عوامل اول، یکی از مهم‌ترین روش‌های رمزنگاری کلید عمومی در جهان به شمار می‌رود. استفاده از الگوریتم میلر-رابین در تولید اعداد اول، کارایی و امنیت این الگوریتم را تقویت کرده است. RSA در حوزه‌های مختلفی مانند تبادل امن کلیدها، امضای دیجیتال و پروتکل‌های امنیتی اینترنت کاربرد گسترده‌ای دارد و همچنان یکی از ستون‌های اصلی امنیت دیجیتال است.