Asymmetric Cryptography یا رمزنگاری غیرمتقارن

رمزنگاری غیرمتقارن همچنین به عنوان رمزنگاری کلید عمومی نیز شناخته می شود و از کلیدهای عمومی و خصوصی برای رمزنگاری و رمزگشایی داده استفاده می کند . کلیدها بزرگ و وسیع هستند و به صورت جفت کنار هم قرار می گیرند اما یکسان نمی باشند یا به عبارتی متقارن یا Symmetric نیستند.

در این جفت کلید ، یکی از کلیدها می تواند با همه به اشتراک گذاشته شود که به آن کلید عمومی یا Public Key می گویند.کلید دیگر از این جفت کلید به صورت محرمانه و پنهان باقی می ماند که به آن کلید خصوصی یا Private Key گویند.هر دو کلید می توانند برای رمزنگاری استفاده شوند ، روال کار به این صورت می باشد که : کلیدی که پیام ما را رمزنگاری می کند کلید مخالف آن نیز آن را رمزگشایی خواهد کرد .بسیاری از پروتکل ها مانند SSH، OpenPGP، S/MIME و SSL/TLS از رمزنگاری نامتقارن برای رمزنگاری و قابلیت امضاء دیجیتال (Digital Signature) استفاده می کنند و نیز برنامه های نرم افزاری مانند مرورگرها به برقراری یک ارتباط امن در بستر یک شبکه ناامن مثل اینترنت و ایجاد یک امضاء دیجیتال معتبر نیاز دارند .رمزنگاری نامتقارن آیتم هایی مانند محرمانگی اطلاعات ، درستی و امانت در داده ، صحت و اعتبار و انکار نشدن صحت مطالب را تضمین می کند. کاربران و سیستم ها نیاز دارند که مطمئن باشند اطلاعاتی که دریافت می کنند از طرف همان فرستنده ای باشد که ادعا می کند فرستنده اطلاعات است و این اطلاعات در طول مسیر جابه جا یا دستکاری نخواهد شد و یا به دست یک شخص ثالث نخواهد افتاد. در رمزنگاری ، مرجع صدور گواهی دیجیتال (Certificate Authority) به طور مخفف CA ، گواهی های دیجیتال یا گواهی های کلید عمومی را صادر می کند.

الگوریتم RSA (Rivest Shamir-Adleman)

یک سیستم رمزنگاری برای رمزنگاری کلید عمومی می باشد. در سال 1977 توسط Ron Rivest ,Adi Shamirو

Nard Adleman در موسسه ماساچوست مطرح شد . الگوریتم تولید کلید های private و public پیچیده ترین قسمت از RSAمی باشد. با استفاده از the Rabin-Miller Primality test که یک الگوریتم تست اعداد اول می باشد دو عدد اول بزرگ به نام های Pو q تولید می شود . از ضرب اعداد اول p , q عددی به نام n بدست می آید . این عدد توسط هر دو کلید publicو Private مورد استفاده قرار می گیرد و لینکی را بین کلیدهای عمومی و خصوصی برقرار می کند که طول آن به صورت بیت بیان می شود که طول کلید نامیده می شود.

در حالت کلی محاسبه کلید عمومی و خصوصی با محاسبات زیر انجام می گیرد:

۱. دو عدد اول بزرگ p و q را به صورت تصادفی بیابید به طوری که $p \neq q$.
۲. عدد n را محاسبه کنید به طوری که $n = pq$.
۳. تابع فی را محاسبه کنید به طوری که $\varphi(n) = (p-1)(q-1)$
۴. عدد e را انتخاب کنید به طوری که $1 < e < \varphi(n)$ و نسبت به $\varphi(n)$ اول باشد.
   - عدد e به عنوان توان کلید عمومی منتشر می‌شود.
۵. عدد d را طوری بیابید که $de \equiv 1 \pmod{\varphi(n)}$ (باقی‌مانده ضرب دو عدد d و e نسبت به $\varphi(n)$ برابر ۱ باشد، به صورت: $de = 1 + k\varphi(n)$ به ازای kهای طبیعی)
   - عدد d به عنوان توان کلید خصوصی محافظت می‌شود.

- دو عدد اول می‌توانند توسط روش **پیدا کردن اعداد اول احتمالی** پیدا شوند.
- معمولاً عدد عمومی (e) را در حدود 2^{16} انتخاب می‌کنند. البته بعضی از برنامه‌ها اعداد کوچکی را انتخاب می‌کنند که باعث سریعتر شدن و البته خطرات امنیتی در رمزنگاری می‌شود.
- **کلید عمومی** تشکیل می‌شود از:
  - عدد n (عدد مشترک)
  - عدد e (عدد عمومی)
- **کلید خصوصی** تشکیل می‌شود از:
  - عدد n (عدد مشترک)
  - عدد d (عدد خصوصی)
- کلید خصوصی به صورت‌های دیگری غیر از d ممکن است نگهداری شود.
  - p و q: اعداد اول برای ساختن کلید.
  - $d \mod (p-1)$ و $d \mod (q-1)$،
  - $q^{-1} \mod (p)$.
- در تمام مراحل باید اجزای کلید خصوصی سری نگه داشته شود، دو عدد p و q اگر به عنوان صورتی از کلید خصوصی نگهداری نشود بهتر است به شیوه‌ای امن نابود شوند. زیرا با این دو عدد تمام اعداد n و e، d قابل محاسبه خواهند بود.

با ذکر یک مثال به توضیح کاربرد رمزنگاری Asymmetric و استفاده از الگوریتم RSA می پردازیم .

یک مثال ساده از کاربرد رمزنگاری در ارسال و دریافت ایمیل برای نمونه Gmail

1. شما وارد سایت https://gmail.com می شوید که به وسیله پروتکل Https امن شده است
2. مرورگر شما به سرور Gmail.com وصل می شود و تقاضای یک کلید عمومی می دهد
3. سرور برای تولید کلید از الگوریتم RSA استفاده می کند
4. خروجی این الگوریتم جفت کلید عمومی و خصوصی خواهد بود
5. سرور کلید عمومی ساخته شده را برای ما می فرستد ولی کلید خصوصی را پیش خود نگه می دارد
6. مرورگر داده های ما را که می تواند شامل نام کاربری و رمز عبور باشد را بوسیله کلید عمومی رمزنگاری می کند و برای سرور سایت Gmailمی فرستد
7. داده های رمزگذاری شده با کلید عمومی به دست سرور سایت Gmailمی رسد

8. سرور سایت Gmail با کلید خصوصی ای که پیش خود نگه داشته بود داده را رمزگشایی می کند مثلا نام کاربری و رمز عبور شما را استخراج می کند
9. سرور سایت Gmail داده های استخراج شده را برای صحت آنها بررسی می کند
10. در صورت صحت داده ، سرور Gmailایمیل را به سیستم ما می فرستد(روال مجدد ولی برعکس اتفاق می افتد)
11. سرور Gmail از مرورگر سیستم ما تقاضای یک کلید عمومی می کند
12. مرورگر سیستم ما توسط الگوریتم RSA کلیدهای عمومی و خصوصی را تولید می کند و کلید عمومی را برای سرور Gmailمی فرستد
13. مرورگر سیستم ما کلید خصوصی را پیش خود نگه می دارد
14. سرور Gmail توسط کلید عمومی ای که مرورگر ما برایش فرستاده بود محتویات ایمیل ما را رمزنگاری می کند
15. محتویات ایمیل برایمان ارسال می شود و مرورگر سیستم ما توسط کلید خصوصی خود محتویات ایمیل را که به صورت رمز می باشد رمزگشایی می کند .

نکته : همیشه فرستنده داده از گیرنده خود تقاضای کلید عمومی می کند ، کلید عمومی در اینجا حکم یک گاوصندوق امن را دارد ، گیرنده پیام، گاوصندوق (کلید عمومی) را برای فرستنده می فرستد و کلید گاو صندوق (کلید خصوصی) را پیش خود نگه می دارد . فرستنده با کلید عمومی داده را رمزنگاری می کند (یعنی داخل گاوصندوق قرار می دهد)

و به سمت گیرنده می فرستد ، گیرنده با کلید خصوصی ای که داشت داده را باز می کند .

هرگاه جای فرستنده و گیرنده عوض شود روال تقاضای کلید عمومی از گیرنده همچنان پا برجاست.

مهتاب بکیان

کارشناس فنی شرکت آتنا