RSA cryptography algorithm document

چگونگی کارکرد

کلیات

RSAشامل 4 مرحله است: ساخت کلید، توزیع کلید، رمزنگاری و رمزگشایی.

یک اصل اساسی در RSA این است که یافتن سه عدد صحیح مثبت بسیار بزرگ مانند e, n و dکه رابطه ی زیر برایشان بر قرار باشد، عملی است.

$$(m^d)^e \equiv m(\, mod\ n)$$

و با دانستن این که e و n و یا حتیm ، یافتن d می تواند بسیار مشکل باشد.

آراس‌ای به‌طور کلی از دو کلید تشکیل می‌شود. کلید عمومی و کلید خصوصی. کلید، عددی ثابت است که در محاسبات رمزنگاری استفاده می‌شود. کلید عمومی برای همه معلوم بوده و برای رمزنگاری پیام استفاده می‌شود. این پیام فقط توسط کلید خصوصی باز می‌شود. به بیان دیگر همه می‌توانند یک پیام را رمز کنند اما فقط صاحب کلید خصوصی می‌تواند پیام را باز کند و بخواند.

کلید عمومی توسط اعداد صحیح n و e نمایش داده میشود و کلید خصوصی، توسط عدد صحیح(d گرچه n در فرایند رمزگشایی هم استفاده می شود بنا بر این ممکن است قسمتی از کلید خصوصی هم در نظر گرفته شود).m، نمایان گر پیام است که از قبل توسط یک تکنیک خاص آماده شده است و در ادامه این تکنیک شرح داده شده است.

هر چند از لحاظ ریاضی کلیدهای عمومی و خصوصی با یکدیگر ارتباط دارند اما تقریباً محال است که کسی بتواند حتی با تجیهزات پیشرفته و صرف وقت زیاد با داشتن یکی از کلیدها، دیگری را تشخیص دهد. در واقع می‌توان گفت که با توجه به سطح دانش کنونی و سامانه‌های رایانه‌ای موجود، الگوریتم رمزنگاری و ارتباط میان کلیدها تقریباً غیرقابل شکستن است.

آراس‌ای مبتنی بر توان‌رسانی پیمانه‌ای است و از اعداد طبیعی خیلی بزرگ استفاده می‌کند. مستندات آراس‌ای تحت عنوان PKCS 1 استاندارد شده‌اند.

ساخت کلید

مراحل زیر برای ساخت کلید طی می‌شود:

1. دو عدد اول بزرگ pو qرا به صورت تصادفی بیابید به‌طوری‌که p != q

- برای اهداف امنیتی، pو q باید به صورت تصادفی انتخاب شوند، و در اندازه مشابه باشند اما طول آن ها در حد چند رقم متفاوت باشد تا تجزیه را کمی دشوار تر کند. اعداد صحیح اول می توانند به صورت کارآمد توسط یک تست اول بودن یافت شوند.
- pو q پنهان باقی می مانند.

2.عدد n را محاسبه کنید به‌طوری‌که n = pq

- nبه عنوان پیمانه برای هر دو کلید خصوصی و عمومی استفاده می شود. طول کلید، تعداد بیت هایn ، طول کلید را مشخص می کند.

3.تابع $\lambda\ (n)$ را محاسبه کنید که λ Carmichael function است . از آن جایی که n=pq، $\lambda\ (n) = lcm(lambda(p), lambda(q))$ و از آن جایی که p و q اول هستند، $\lambda\ (p) = \Phi(p) = p - 1$ و به همین روال $\lambda\ (q) = q - 1$.
بنابراین $\lambda\ (n) = lcm(p - 1, q - 1)$

- این مقدار مخفی باقی می ماند.
- مقدار lcm ممکن است از طریق الگوریتم اقلیدسی محاسبه شود، از آن جایی که

4.عدد eرا انتخاب کنید به‌طوری‌که $1<e<\lambda\ (n)$ و نسبت به $\lambda\ (n)$ اول باشد.

- عدد eبه عنوان توان کلید عمومی منتشر می‌شود.
- eبا داشتن تعداد کم بیت و وزن وزن همینگ کم، منجر به رمزگذاری کارآمد تری می شود. معمول ترین مقدار انتخاب شده برایe ، حدود عدد2^{16} یک که برابر با 65536 است می باشد. کوچک ترین و سریع ترین مقدار ممکن برای e ، عدد 3 است اما چنین مقدار کمی نشان داده است که در بعضی ساختار ها امنیت کم تری را ایجاد می کند.

5.عدد d که $d \equiv e^{-1} \pmod{\lambda(n)}$ را به دست بیاورید.

- عدد d به عنوان توان کلید خصوصی محافظت می‌شود.
- در واقع $de \equiv 1 \pmod{\lambda(n)}$ این مقدار می تواند به صورت کارآمدی توسط الگوریتم تعمیم یافته اقلیدس پیدا شود از آن جایی که d و $\lambda(n)$ اول هستند،این معادله یک فرمی از قضیه بزو است که در آن d یکی از ضریب ها است.

دو عدد اول می‌توانند توسط روش **پیدا کردن اعداد اول احتمالی** پیدا شوند.

- **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)،
  - $q^{-1} \bmod (p)$.
- 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.

توزیع کلید

فرض کنید که باب می خواهد اطلاعاتی را به آلیس بفرستد. اگر آن ها تصمیم بگیرند که از RSA استفاده کنند، باب باید کلید عمومی آلیس را برای رمز گذاری پیام بداند و آلیس باید از کلید خصوصی ای که در اختیار دارد استفاده کند تا پیام را رمزگشایی نماید. بنابر این برای این

که باب قادر باشد پیام رمز شده اش را ارسال کند، آلیس کلید عمومی (n,e) خود را تسط یک مسیر مطمئن ولی نه لزوما مخفی به باب منقل می کند. کلید خصوصی آلیس (d)هرگز منتقل نمی شود.

رمزنگاری پیام

حالا که باب کلید عمومی آلیس را دریافت کرد، قصد دارد پیام M را به توسط الگوریتم RSA به آلیس بفرستد. با باید پیام خود را در قالب یک عدد (m) در بیاورد به‌طوری‌که این فرایند برگشت‌پذیر بوده و روی آن توافق شده باشد و شناخته شده باشد. به این فرایند طرح لایه گذاری گفته می شود.عدد باب باید از n کوچک‌تر باشد. بدیهی است اگر پیام بزرگ‌تر از حد معمول باشد آن را در بسته‌های جداگانه می‌فرستیم. او اکنون عدد C را محاسبه می‌کند به‌طوری که

$$c = m^e \bmod n$$

این کار با استفاده از به توان رسانی پیمانه ای می تواند خیلی سریع انجام شود، حتی برای اعداد خیلی بزرگ.

حال باب می تواند c را به آلیس بفرستد و آلیس توسط کلید خصوصی اش آن را رمزگشایی کند و آن را بفهمد.

رمز گشایی پیام

آلیس c را دریافت کرده است و کلید خصوصی خود را در دسترس دارد. حال می تواند عدد m را که معادل پیام اصلی است از n، C و d بازیابی کند.

$$m = c^d \bmod n$$

نمونه

1. انتخاب دو عدد اول مانند:

$$q = 53 \quad \text{and } p = 61$$

2. محاسبه $n = pq$:

$$n = 61 * 53 = 3233$$

3. محاسبه تابع فی اویلر با ساخت $\varphi(n) = (p-1)(q-1)$ خواهدشد:

$\varphi(3233) = (61-1)(53-1)= 3120$

4. انتخاب هر عددی $1<e<3120$ که نسبت به ۳۱۲۰ اول باشد.

$e=17$ در نظر می‌گیریم

5. محاسبه d, the وارون ضربی (هم‌نهشتی) $e \pmod{\varphi(n)}$,

$d= 2753$

$e * d \bmod \varphi(n) =1$

$17 * 2753 \bmod 3120 =1$

کلید عمومی $(n = 3233,\ e =17)$ برای پیام m هست. بنابران تابع رمز به صورت زیر است:

$$c(m) = m^{17}\ mod\ 3233$$

کلید خصوصی $(d =2753)$ هست. برای متن رمز c تابع رمزگشایی به صورت زیر خواهد بود:

$$m(c) = c^{2753}\ mod\ 3233$$

برای نمونه در رمزنگاری $m =$ ۶۵, را حساب می‌کنیم.

$$c = 65^{17}\ mod\ 3233 = 2790$$

برای رمزگشایی $c =2790$ را حساب می‌کنیم.

$$m = 2790^{2753}\ mod\ 3233 = 65$$

امضای پیام

فرض کنید آلیس از کلید عمومی باب برای ارسال پیام رمزگذاری شده برای وی استفاده می کند. در این پیام، او می تواند ادعا کند که آلیس است، اما باب هیچ راهی برای تایید این که این پیام واقعا از طرف آلیس است ندارد، چرا که هر کس می تواند از کلید عمومی باب برای ارسال پیام

های رمز گذاری شده به وی استفاده کند. برای تایید منشاء پیام، می توان از **RSA** برای امضا کردن یک پیام استفاده کرد.

فرض کنید آلیس مایل است پیام امضا شده ای را به باب ارسال کند. او می تواند برای این کار از کلید خصوصی خود استفاده کند. برای این کار، او مقدار هش پیام مورد نظر خود را محاسبه می کند، آن را به توان **d** می رساند (در پیمانه ی **n**)(همان طور که هنگام رمزگشایی یک پیام این کار را انجام می دهد)و آن را به عنوان "امضا" به پیام خود الصاق می کند. هنگامی که باب این پیام امضا شده را دریافت می کند، او هم از همان تابع هش در رابطه با کلید عمومی آلیس استفاده می کند. او این امضا را به توان **e** (در پیمانه ی **m**)می رساند (همان طور که این کار را هنگام رمزگشایی یک پیام نیز انجام می دهد) و مقدار هش حاصل را با مقدار هش واقعی پیام مقایسه می کند. اگر این دو با هم توافق داشته باشند، او می داند که نویسده پیام کلید خصوصی آلیس را در اختیار داشته است و پیام از آن زمان دست نخورده باقی مانده است.

این روش به دلیل قوانین به توان رسانی، کار می کند:

$$h = hash(m)$$
$$(h^e)^d = h^{ed} = (h^d)^e \equiv h (\bmod n)$$

بنابر این ، کلید خصوصی می تواند برای:

1. رمزگشایی یک پیام که برای یک گیرنده فرستاده شده است، که می تواند توسط هر فردی که دارای کلید عمومی است، برای رمزنگاری استفاده شود.
2. رمزنگاری یک پیام که ممکن است توسط هر کس رمزگشایی شود، اما فقط توسط یک نفر می تواند رمزنگاری شود، این استفاده، امضای دیجیتال را ممکن می سازد.