الگوریتم امضای ECDSA چیست؟

اگر به مبحث امنیت و رمزنگاری در دنیای کریپتوکارنسی علاقه داشته باشید، احتمالا تا به حال نام یکی از قوی‌ترین الگوریتم‌های رمزنگاری یعنی **الگوریتم امضای ECDSA** را شنیده‌اید. این الگوریتم یکی از قوی‌ترین و در عین حال بهینه‌ترین روش‌ها برای خلق یک امضای دیجیتال یا امضای اشنور و همچنین اعتبارسنجی تراکنش‌های شبکه و هویت فرد فرستند یا گیرنده یک پیام در بلاکچین است. در واقع الگوریتم امضای ECDSA از چند بخش بسیار حیاتی تحت عنوان کلید عمومی و خصوصی و همچنین یک منحنی بیضوی تشکیل شده است که به واسطه این چند مولفه، الگوریتم می‌تواند یک سازوکار قوی برای صحت سنجی تراکنش‌ها ارائه دهد.

امروزه سازوکار الگوریتم امضای ECDSA مزایای زیادی را با خود به همراه آورده و باعث شده تا اکوسیستم مالی این دنیای بزرگ با امنیت بیشتری با یک قدم بزرگ رو به جلو حرکت کند. اطلاع درباره سازوکار الگوریتم امضای ECDSA برای اعضای بازار ارز دیجیتال و همچنین کسانی که به مبحث امنیت و رمزنگاری داده‌ها توسط کامپیوترها علاقه‌مندند بسیار مفید است و به آن‌ها نگرشی جدید می‌دهد؛ از این رو وبسایت کیف پول من تصمیم دارد تا در این مقاله شما را با مفهوم و سازوکار الگوریتم امضای ECDSA آشنا کند و درباره مزایا و شیوه محاسبه آن اطلاعاتی را در اختیار شما قرار دهد.

مفهوم کلید خصوصی و کلید عمومی در رمزنگاری ارز دیجیتال

پیش از آنکه به توضیح درباره سازوکار الگوریتم امضای ECDSA بپردازیم، بهتر است با مفهوم کلید عمومی و خصوصی که ستون‌های ساخت این امضا هستند آشنا شویم. در واقع اصلی‌ترین تکنولوژی که هم اکنون در دنیای کریپتوکارنسی برای امنیت از آن استفاده می‌شود، رمزنگاری کلید عمومی (PKC) یا رمزنگاری نامتقارن است که از دو بخش کلید عمومی و خصوصی تشکیل می‌شود. هر عضوی از این شبکه یک کلید خصوصی و یک کلید عمومی دارد که از اولی برای امضای اطلاعات ارسالی و همچنین رمزنگاری تراکنش‌ها استفاده می‌کند و دومی را در اختیار اعضای دیگر اکوسیستم و گیرنده قرار می‌دهد. گیرنده نیز می‌تواند با استفاده از کلید عمومی فرد فرستنده صحت پیام را بسنجد.

الگوریتم امضای ECDSA چیست؟

حالا نوبت آن است که ببینیم الگوریتم امضای ECDSA چیست و چگونه می‌تواند با استفاده از کلیدهای عمومی و خصوصی این رمزنگاری را برای ما انجام دهد. **الگوریتم امضای ECDSA** مخفف عبارت لاتین Elliptic Curve Digital Signature Algorithm است که در زبان فارسی به معنای الگوریتم امضای دیجیتال منحنی بیضوی معنا می‌شود. این روش یکی از بهترین و امن‌ترین روش هاست و بر پایه استفاده از منحنی‌های بیضوی با مختصات‌های مختلف در صفحه دکارتی در ریاضیات بنا شده تا بتوانیم عبارات رمزنگاری کوتاه‌تری را تولید کنیم. سازوکار الگوریتم امضای

ECDSA برای ما یک امضای دیجیتالی تولید می‌کند تا به‌واسطه آن فرد گیرنده پیام پیام‌های ما را اعتبارسنجی کند و دریابد که فرستنده تراکنش، قطعا خود ما هستیم.

این امضای دیجیتال در اصل یک نوع سند دیجیتالی محسوب می‌شود که می‌توان در آن اطلاعاتی درباره صاحب کلید خصوصی و همچنین صادرکننده گواهی را یافت. اندازه این امضا به 256 بیت می‌رسد. این مقدار نسبت به الگوریتم‌های رمزنگاری دیگر که امضاهایی بسیار طولانی‌تر تولید می‌کنند بسیار به‌صرفه‌تر و سریع‌تر است؛ برای مثال، در الگوریتم RSA که یکی قوی‌ترین الگوریتم‌های رمزنگاری در دنیاست، امضای دیجیتال 3072 بیت دارد، در حالی که امنیتش از سازوکار الگوریتم امضای ECDSA کمتر است.

ساخت کلید عمومی و خصوصی در سازوکار الگوریتم امضای ECDSA

برای اینکه سازوکار الگوریتم امضای ECDSA را توضیح دهیم، ابتدا نیاز است بدانیم این الگوریتم چگونه کلیدهای خصوصی و عمومی مورد نیازش را به واسطه منحنی‌های بیضوی به دست می‌آورد. در ابتدای کار باید یک منحنی بیضوی مناسب انتخاب کرد. این منحنی مجموعه‌ای از نقاط مختلف را بر روی میدان مختصاتی ارائه می‌دهد که برای تولید کلید خصوصی و عمومی استفاده می‌شوند. سپس باید به صورت رندوم و تصادفی یک نقطه از این منحنی را انتخاب کرد. این نقطه که به‌عنوان G Point از آن یاد می‌شود به‌واسطه یک تابع به اسم G Generator تولید می‌شود. سپس باید یک عدد تصادفی انتخاب کرد که این عدد به‌عنوان کلید خصوصی ما مورد استفاده قرار می‌گیرد. حالا نوبت ساخت کلید عمومی است. در اصل کلید عمومی از ضرب عدد تصادفی کلید خصوصی در نقطه G Point به دست می‌آید.

مطلب پیشنهادی: کلید خصوصی و عمومی چیست؟

بعد از اینکه کلیدهای عمومی و خصوصی ساخته شد، وقت آن است که کلید خصوصی را در یک جای امن ذخیره کرده و کلید عمومی را برای استفاده در اختیار گیرنده قرار دهیم. به این ترتیب، مشخص می‌شود که کلید عمومی از کلید خصوصی به دست می‌آید؛ اما نقطه قوت ماجرا برعکس است. اینکه نمی‌توان کلید خصوصی را که همان شاخص امنیت ماست را از کلید عمومی به دست آورد. کلید عمومی تولید شده در اصل از یک x و y تشکیل شده است که می‌توان آن را به واسطه یک سری محاسبات با یک بیت فشرده سازی کرد و به یک عدد کوتاه‌تر رسید. به این ترتیب رمز سازوکار الگوریتم امضای ECDSA از رمزهای RSA کوتاه‌تر می‌شود.

نحوه رمزنگاری در سازوکار الگوریتم امضای ECDSA چطور است؟

بعد از اینکه کلیدهای عمومی و خصوصی را با اندازه‌های کوچک‌تر اما با امنیت بالا تولید کردیم، وقت آن است که به سراغ فرآیند سازوکار الگوریتم امضای ECDSA برویم. ابتدا پیامی که فرستنده می‌خواهد آن را بفرستد انتخاب می‌شود. این پیام می‌تواند شامل هر نوع داده‌ای از جمله متن یا داده دودویی. سپس این پیام باید امضا شود. برای اینکه وارد فرآیند ساخت امضا شویم ابتدا باید با استفاده از تابع هش، مقدار هش داده به دست آید. خروجی این تابع به‌عنوان ورودی توابع دیگر در مراحل بعدی استفاده می‌شود. حالا نوبت آن است که کلید خصوصی که انتخاب کردیم را وارد ماجرا کنیم.

کلید خصوصی و مقدار هش پیام با استفاده از یک سری محاسبات روی منحنی بیضوی، تبدیل به داده امضای دیجیتال می‌شوند. در واقع در سازوکار الگوریتم، امضای ECDSA شامل یک جفت عدد صحیح (r , s) است که بر اثر محاسباتی شامل توابع لگاریتم طبیعی ((Ln، mod n و هش (Hash) که بر روی داده کلید خصوصی و عمومی انجام می‌گیرد به دست می‌آید. حالا که امضای دیجیتال آماده شد، پیام به همراه امضا و کلید عمومی فرستاده می‌شود. در طرف دیگر نیز تاییدکننده می‌تواند با استفاده از کلید عمومی و یک سری محاسبات بر روی محنی بیضوی مربوطه مشخص کند که آیا پیام توسط خود شخص امضا شده است یا نه.

مطلب پیشنهادی: نحوه پیدا کردن کلید خصوصی

مزایای استفاده از سازوکار الگوریتم امضای ECDSA

سازوکار **الگوریتم امضای ECDSA** مزایای زیادی را همراه با خود برای شبکه‌های بلاکچینی به همراه آورده و همین مزایا باعث شده امروزه در خرید بیت کوین و دیگر رمزارزها، بلاکچین‌های مربوطه بتوانند با امنیت بیشتری به کار خود ادامه دهند. گوشه‌ای از مزایای ساز وکار الگوریتم امضای ECDSA عبارتند از:

- اندازه بسیار کوچک امضاهای تولیدی توسط این الگوریتم نسبت به الگوریتم‌های برتر رمزنگاری باعث می‌شود سرعت و کارایی شبکه افزایش زیادی داشته باشد.
- سازوکار الگوریتم امضای ECDSA با وجود اینکه بسیار کوچک است؛ اما امنیتی چند برابری را به شبکه هدیه می‌کند.
- از آنجایی که محاسبات در این نوع الگوریتم در تعداد کمتری صورت می‌گیرد و همچنین خروجی آن‌ها امضایی با حجم کمتر است؛ پس انرژی کمتری توسط سیستم‌های کامپیوتری برای رمزنگاری و رمزگشایی استفاده می‌شود و در نتیجه سیستم‌های متوسط نیز می‌توانند با شرکت در این فرآیند کمک بیشتری به امنیت شبکه بکنند.
- با استفاده از این الگوریتم، شخص ثالث به راحتی می‌تواند امضای دیجیتال را تایید کند بدون اینکه امنیت شبکه به خطر بیفتد.
- با استفاده از این الگوریتم امکان ساخت امضاهای دیجیتالی بی‌همتا برای هر جفت کلید عمومی و خصوصی ایجاد می‌شود.
- می‌توان با استفاده از این روش و تابع G Generator که در نقطه تصادفی کلید خصوصی ضرب می‌شود، تعداد نامحدودی کلید عمومی ساخت.
- با استفاده از روش الگوریتم امضای ECDSA حجم اطلاعات ذخیره شده در بلاکچین کاهش می‌یابد و به این ترتیب قراردادهای هوشمند و تراکنش‌ها ساده‌تر و سریع‌تر پردازش می‌شوند.
- این روش کدهای پشتیبان بسیار متنوعی از جمله Crypto++، Botan، Open SSL، Microsoft Crypto API، Bouncycastle و غیره دارد.
- با استفاده از سازوکار الگوریتم امضای ECDSA می‌توان کلید عمومی و همچنین امضا را از یک پیام امضا شده توسط فرستنده بازیابی کرد به این صورت که یک متغیر دیگر تحت عنوان v که نماینده امضای دیجیتال است به آن اضافه کنیم و فرمت را به شکل (به r, s, v) در بیاوریم.

سازوکار الگوریتم امضای ECDSA چه معایبی دارد؟

با اینکه **الگوریتم امضای ECDSA** مزایای بسیار زیادی را به همراه دارد؛ اما همچنان ضعف‌ها و معایبی به آن وارد است که در برخی زمینه‌ها استفاده کنندگان را ناکام می‌گذارد. از معایب این الگوریتم می‌توان به موارد زیر اشاره کرد:

- با اینکه این روش یکی از روش‌های سریع و دارای محاسباتی با تعداد کم است؛ اما همین محاسبات بسیار پیچیده هستند و می‌توانند در دستگاه‌هایی که منابع محدودی دارند مانند دستگاه‌های جانبی سیستم اینترنت اشیا مشکل تولید کنند و به سرانجام نرسند.
- در سازمان‌های کوچک این الگوریتم می‌تواند بهینه نباشد؛ چرا که برای مجهز کردن سیستم‌ها به منابع خوب نیازمند وقت و هزینه زیاد هستیم.
- برای اینکه بتوان توسط سازوکار الگوریتم امضای ECDSA امنیت خوبی برای شبکه به همراه آورد، نیاز داریم که کلیدهای خصوصی با اندازه بزرگ انتخاب کنیم که همین موضوع می‌تواند زمان محاسبه را بیشتر کند.
- چون الگوریتم به تولید اعداد تصادفی برای ایجاد یک امضای خوب نیازمند است. اگر این اعداد به درستی تولید نشوند ممکن است که امنیت ایجاد شده چندان مقاوم نباشد و در برابر حمله هکرها از بین برود.
- برای اینکه این الگوریتم بتواند به درستی کارخودش را انجام دهد نیاز است تا آن را با دقت و تخصص بسیار بالا پیاده سازی کرد؛ در غیر این صورت سیستم با ضعف امنیتی مواجه می‌شود.

- انتخاب منحنی‌های صحیح هم یکی از دشواری‌های پیاده سازی الگوریتم امضای ECDSA است.
- در مرحله تایید امضا نیز با دشواری روبه‌رو هستیم؛ چنانچه در این مرحله نیز نیاز داریم تا یک سری محاسبات انجام شود؛ در صورتی که ممکن است در الگوریتم‌های دیگر اینگونه نباشد.

با سازوکار الگوریتم امضای ECDSA، رمزنگاری را ایمن‌تر و کوتاه‌تر کنید!

سازوکار **الگوریتم امضای ECDSA** امروزه به یکی از قوی‌ترین و همچنین بهینه‌ترین روش‌های رمزنگاری داده به خصوص در بستر ارزهای دیجیتال تبدیل شده که به اکوسیستم کمک می‌کند با هزینه کمتر و سرعت بیشتر بتواند تراکنش‌ها را اعتبارسنجی کرده و نسبت به هویت فرستنده و گیرنده با حساسیت بیشتری رفتار کند. سازوکار این الگوریتم با اینکه تعداد محاسبات کمتری نسبت به الگوریتم‌های دیگر دارد؛ اما پیچیدگی آن بیشتر است و همچنین امضا و خروجی که تولید می‌کند با وجود امنیت بیشتر، طول کمتری نسبت به روش‌های دیگر رمزنگاری دارد.

اصلی‌ترین اجزای سازوکار الگوریتم امضای ECDSA نیز شامل یک کلید خصوصی، یک کلید عمومی، یک منحنی بیضوی مشخص و همچنین تعدادی از توابع ریاضی است. البته با اینکه این روش به‌عنوان یکی از روش‌های برتر در حوزه امنیت شناخته می‌شود؛ اما هنوز معایب و ایراداتی به آن وارد است که باعث می‌شود این روش نیاز به توسعه بیشتر داشته باشد. چنانچه دوست دارید که درباره الگوریتم‌های رمزنگاری بیشتر بدانید و مطالبی در خصوص امنیت شبکه کریپتوکارنسی مطالعه کنید می‌توانید به مقاله‌های دیگر سایت کیف پول من سری بزنید.