بررسی و تفاوت رمزنگاری متقارن و نامتقارن

رمزنگاری، مفهومی که شاید انسان‌ها از همان دوران طفولیت با آن آشنا می‌شوند! حال به یک امری تخصصی تبدیل شده که اهمیت آن بویژه در فضای سایبری که خطرات مختلفی داده‌های ما را تهدید می‌کند به وضوح برای تمامی کاربران دنیای سایبر و بازارهای مالی دیجیتالی روشن‌تر شده است. آیا در دوران طفولیت خاطرات خویش را به زبان رمزی یادداشت کرده‌اید؟ اگر چنین کاری را انجام نداده‌اید، احتمالا تاکنون از پاکت نامه برای ارسال نامه استفاده کرده‌اید.

تمامی این کارها با هدف تامین امینت اطلاعات صورت می‌گیرد. مسلما هنگامی که صحبت از بازارهای مالی همچون مارکت رمزارزی که در بستر اینترنت به وجود آمده‌اند به میان می‌آید، توجه غالب کاربران به سمت تامین امنیت این حوزه جلب می‌گردد. در حال حاضر الگوریتم‌های رمزنگاری را به دو نوع مهم رمزنگاری متقارن و نامتقارن تقسیم می‌کنند. احتمالا تاکنون مطالبی را در ارتباط با کلید عمومی و خصوصی در دنیای کریپتوکارنسی مطالعه کرده باشید. تمامی صحبت‌ها در شناخت کلید عمومی و خصوصی تراکنش‌های بلاک چینی رمزارزی به شناخت انواع رمزنگاری‌ها گره خورده است. با توجه به اهمیت شناخت رمزنگاری **متقارن** و **نامتقارن**، ما این مقاله از بلاگ **کیف پول من** را به بررسی مفاهیم و

تفاوت‌های این سیستم‌های رمزنگاری اختصاص داده‌ایم؛ اگر شما هم در این زمینه کنجکاو هستید تا انتهای این مطلب با ما همراه باشید.

مروری اجمالی بر مفهوم رمزنگاری

قبل از آن که به بررسی و تفاوت **رمزنگاری متقارن** و **نامتقارن** بپردازیم، ضرورت دارد نگاهی اجمالی به خود ماهیت مفهوم رمزگذاری داشته باشیم تا با دیدی روشن‌تر به مطالعه مطالبی بپردازید که در ادامه به آن‌ها پرداخته خواهد شد. رمزنگاری به بیان ساده، عبارت از روشی است که به منظور ویرایش اطلاعات به کار می‌رود و این ویرایش اطلاعات به گونه‌ای صورت می‌گیرد که منحصرا اشخاص مجاز قادر هستند اطلاعات موجود در آن را درک نمایند. به لحاظ فنی در فرآیند رمزنگاری، متن ساده به یک متن رمزی تبدیل می‌شود؛ به طوری که این داده‌های خوانا به گونه‌ای تغییر می‌کنند که در ظاهر غیرقابل فهم و تصادفی به نظر برسند. البته ناگفته نماند که الگوریتم‌های رمزنگاری برای انجام چنین کاری به کلید رمزنگاری (KEY) نیاز پیدا می‌کنند.

این کلیدهای رمزنگاری در واقع به مجموعه‌ای از مقادیر ریاضی اطلاق می‌شود که هم برای فرستنده داده رمزنگاری شده و هم برای گیرنده آن، آشنا است. تفاوت اصلی رمزنگاری متقارن و نامتقارن را می‌توان در همین استفاده از کلیدهای رمزنگاری شده جستجو کرد. در الگوریتم رمزنگاری متقارن از یک کلید به منظور اجرای توابع رمزنگاری و همچنین رمزگشایی آن استفاده می‌شود؛ اما در الگوریتم نامتقارن ما با دو کلید مواجه خواهیم بود، یک کلید برای رمزگذاری داده‌ها و کلید دیگر برای رمزگشایی آن‌ها مورد استفاده قرار می‌گیرد.

آشنایی با الگوریتم رمزنگاری متقارن

یکی از الگوریتم‌های مورد استفاده از رمزنگاری، **رمزنگاری متقارن** است که در آن ما از یک کلید واحد به منظور رمزگذاری (Encryption) و همچنین رمزگشایی داده‌ها (Decryption) استفاده می‌کنیم. در نظر فعالان حوزه رمزگذاری، این سیستم رمزنگاری قدیمی‌ترین و همچنین معروف‌ترین تکنیک رمزگذاری است. در این سیستم رمزنگاری کلید مخفی مورد استفاده می‌تواند یک کلمه، یک شماره یا حتی یک رشته که مجموعه‌ای از کاراکترها و اعداد که به وسیله یک تولید کننده عدد تصادفی امن ایجاد شده است، باشد. داده‌ها منطبق با قوانین حاکم بر این الگوریتم تغییر پیدا می‌کنند و طرفینی که داده‌ها در میان آن‌ها به صورت رمزنگاری شده مبادله می‌گردد، بایستی کلید را نیز مبادله نمایند تا بتوانند اطلاعات ارسالی و دریافتی را رمزگذاری و همچنین رمزگشایی کنند.

اگر داده رمزنگاری شده به شما ارسال گردد ولی شما کلید مخفی برای رمزگشایی آن را در اختیار نداشته باشید؛ در این حالت شما با متنی نامفهوم که قابل درک نیست، مواجه خواهید شد. ما در الگوریتم رمزنگاری متقارن با 4 مؤلفه روبه‌رو هستیم که به شرح زیر می‌باشند:

1. متن ساده (Plain Text): این متن ساده در واقع همان پیام اصلی قابل فهم است که نباید به وسیله اشخاص غیرمجاز دیده شود و به همین علت نیاز به رمزگذاری دارد.

2. کلید (Key): از کلید برای رمزگشایی پیام استفاده می‌شود و در واقع این کلید است که کلیه اطلاعات مربوط به سوئیچ‌ها و تعویض‌های رخ داده در پیام اصلی را در اختیار گیرنده قرار می‌دهد.

3. متن رمزنگاری شده (Cipher Text): داده مورد نظر شما پس از گذراندن فرآیند رمزگذاری، آماده ارسال می‌شود.

4. الگوریتم‌های رمزنگاری: در یک تعریف ساده از الگوریتم رمزنگاری می‌توان چنین گفت که این الگوریتم‌ها در واقع نوعی فرمول ریاضی هستند که به منظور تبدیل داده‌های سری به متن رمزنگاری شده مورد استفاده قرار می‌گیرند.

مطلب پیشنهادی : نحوه پیدا کردن کلید خصوصی

ناگفته نماند که هر چند الگوریتم رمزنگاری متقارن در مقایسه با رمزنگاری نامتقارن دارای قدمت بیشتری است؛ اما همچنان از آن به عنوان الگوریتمی که دارای سرعت بالایی می‌باشد، یاد می‌شود و در مقایسه با رمزنگاری نامتقارن بسیار کارآمدتر ظاهر شده است. اصولا در رمزنگاری نامتقارن، شبکه‌ها به دلیل مشکلات عملکردی، اندازه داده‌ها و همچنین استفاده از پردازنده‌های سنگین متحمل ضررهای قابل توجهی می‌شوند.

معرفی الگوریتم رمزنگاری نامتقارن (Asymmetric Cryptography)

رمزنگاری نامتقارن که از آن تحت عنوان رمزنگاری کلید عمومی نیز یاد می‌شود، در واقع نسخه پیشرفته‌تر رمزنگاری متقارن است. این روش رمزنگاری با توجه به ماهیت خاص خویش بسیار مورد توجه فناوری بلاک چینی قرار گرفته و از آن در ارتقا سطح امنیت شبکه‌ها و تراکنش‌ها استفاده می‌شود. این الگوریتم جدید رمزنگاری در واقع در سال 1977 میلادی به وسیله دو محقق به نام‌های مارتین هلمن (Martin Hellman) و ویتفیلد دیفی (Whitfield Diffie) در مقاله‌ای به نام «سویه‌های جدید در رمزنگاری» معرفی گردید. البته به نظر کارشناسان ما در **کیفپولمن**، می‌توان سابقه این شیوه خاص رمزنگاری را در زمانی دورتر، یعنی هنگامی که فردی به نام جیمز الیس (James Ellis) ایده چنین رمزنگاری را در دفتر مقر ارتباطی در سازمان اطلاعات و امنیت انگلیس مطرح کرده بود، جستجو کرد.

ما در رمزنگاری نامتقارن با یک جفت کلید مواجه هستیم که از این کلیدها تحت عنوان کلید عمومی (Public Key) و کلید خصوصی (Private Key) یاد می‌شود؛ در واقع در میان این کلیدها نوعی رابطه ریاضی وجود دارد که آن‌ها را در قالب یک جفت مرتبط به هم تعریف می‌کند. برای این که راحت‌تر با نحوه عملکرد این کلیدها ارتباط برقرار نمایید، به این مثال توجه کنید: تصور نمایید که شما دارای یک صندوقچه خاص هستید که این صندوقچه به دلیل محتویات آن بسیار برای شما مهم است و به همین دلیل یک قفل ویژه برای آن در نظر گرفته‌اید.

ویژه بودن این قفل در ویژگی آن که برای باز و بسته شدن به دو کلید نیاز دارد نهفته است و مکانیزم عملکردی خود این کلیدها نیز قضیه را جالب‌تر می‌کند؛ به طوری که اگر از کلید شماره 1 به منظور قفل کردن صندوقچه استفاده کرده باشید این صندوقچه فقط با استفاده از کلید شماره 2 باز می‌شود و بالعکس اگر از کلید شماره 2 برای چنین منظوری استفاده کرده باشید، منحصرا با استفاده از کلید شماره 1 قادر خواهید بود قفل این صندوقچه را باز کنید.

کاربرد ویژه‌ای که در مثال فوق برای کلیدهای شماره 1 و 2 ترسیم کردیم، دقیقا همان کاربردی است که در کلیدهای عمومی و خصوصی در الگوریتم رمزنگاری نامتقارن نیز وجود دارد. این مکانیزم ویژه رمزنگاری که برای پردازش به انرژی و زمان زیادی نیاز دارد، دقیقا همان چیزی است که ما به طور کلی در تکنولوژی نوظهور بلاک چینی، زیاد با آن مواجه می‌شویم.

ارتباط الگوریتم رمزنگاری نامتقارن با شبکه بلاک چین

امروزه بسیاری از تریدرها و معامله‌گران چنین تصور می‌کنند که الگوریتم رمزنگاری نامتقارن همزمان با ظهور فناوری بلاک چین به وجود آمده است؛ اما این در حالی است که سابقه ایجاد چنین الگوریتم رمزگذاری ویژه‌ای به چندین سال پیش از ظهور دنیای کریپتوکارنسی باز می‌گردد ولی شاید بتوان این تصور را چنین تصحیح کرد که با ظهور بلاک چین‌ها و همچنین محبوبیت استفاده از ارزهای دیجیتالی سبب شده تا استفاده از این الگوریتم نیز به معروفیت قابل توجهی دست یابد. تقریبا می‌توان چنین ادعا کرد که غالب رمزارزهای موجود در حال حاضر از روش رمزنگاری نامتقارن و ایجاد کلیدهای عمومی و خصوصی بهره می‌برند. در این فناوری، منظور از کلیدهای عمومی در واقع همان آدرس‌هایی است که رمزارزها را نگهداری می‌کنند و کلیه اعضای شبکه می‌توانند آن را مشاهده نمایند. به بیان دیگر، تریدرها می‌توانند این کلید عمومی را در اختیار دیگران قرار دهند تا آن‌ها به کمک آن بتوانند توکن و ارز دیجیتال به حساب دارنده کلید عمومی ارسال نمایند.

ناگفته نماند که از رمزنگاری نامتقارن به منظور ایجاد کیف پول‌های دیجیتالی و همچنین تراکنش‌های انجام یافته میان تریدرها نیز استفاده می‌شود. به بیان ساده‌تر، آدرسی که بیت کوین شما در آن قرار دارد یک کلید عمومی محسوب می‌شود؛ اما کدی که برای ارسال بیت کوین به آدرس دیگر از آن استفاده می‌کنید، یک آدرس یا کلید خصوصی است که این آدرس و کد غالبا چیزی در حدود 256 بیت اطلاعات ترکیبی از حروف و اعداد است.
برای درک بهتر به این مثال توجه کنید: تصور کنید احسان قصد دارد 5 بیت کوین به هادی ارسال کند، در این صورت احسان بیت کوین را با کلید عمومی هادی رمزنگاری کرده و ارسال می‌کند و در طرف دیگر نیز هادی می‌تواند با استفاده از کلید خصوصی خویش، داده ارسالی

را رمزگشایی نماید و دقیقا به همین علت است که الگوریتم رمزنگاری نامتقارن، در مقایسه با رمزنگاری متقارن امنیت بالاتری را ارائه می‌کند؛ چراکه حتی اگر افراد متعددی به کلید عمومی هادی دسترسی داشته باشند، باز هم قادر نخواهند بود داده‌های ارسالی را رمزگشایی کرده و در آن دخل و تصرف نمایند.

مطلب پیشنهادی : امنیت شبکه بلاک چین

تفاوت الگوریتم رمزنگاری متقارن و نامتقارن

احتمالا با مطالعه مطالب فوق تا حدودی متوجه تفاوت‌های موجود میان **رمزنگاری متقارن** و **نامتقارن** شده باشید و چنین تصور کنید که تفاوت اصلی موجود در این الگوریتم‌های رمزنگاری در تعداد کلیدهای رمزنگاری دخیل در آن نهفته است، به طوری که الگوریتم رمزنگاری متقارن از یک کلید استفاده می‌کند و این در حالی است که ما در رمزنگاری نامتقارن با دو کلید (عمومی و خصوصی) مواجه هستیم؛ اما این مسئله طرح شده، کل ماجرا نبوده و الگوریتم‌های رمزنگاری متقارن و نامتقارن از جهات متعددی با یکدیگر تفاوت دارد که در ادامه به بررسی تفصیلی آن‌ها می‌پردازیم:

تفاوت در طول کلیدها

الگوریتم‌های رمزنگاری متقارن و نامتقارن به لحاظ طول کلیدها نیز با هم تفاوت دارند. جالب است بدانید که طول این کلیدها براساس بیت اندازه‌گیری می‌شود که این مسئله ارتباط کاملا مستقیمی با سطح امنیت ارائه شده به وسیله این الگوریتم‌های رمزنگاری دارد. در رمزنگاری متقارن، عموما کلیدها به صورت کاملا تصادفی انتخاب شده و طول آن‌ها نیز به تناسب امنیت مورد نیاز، غالبا بر روی 128 یا 256 بیت تنظیم می‌شود؛ این در حالی است که ما در رمزنگاری نامتقارن با یک رابطه ریاضیاتی مابین کلیدهای عمومی و خصوصی مواجه هستیم. به بیان دیگر، میان این دو نوع کلید یک الگو ریاضیاتی برقرار است. با توجه به این نکته، برای آن که این الگو در معرض حملات و نفوذ هکرها قرار نگیرد، کلیدهای رمزنگاری نامتقارن را طولانی‌تر در نظر می‌گیرند؛ به همین علت ما در رمزنگاری نامتقارن با کلیدهای 2048 بیتی مواجه هستیم.

تفاوت در مزایا و معایب

هر کدام از دو نوع الگوریتم رمزنگاری متقارن و نامتقارن دارای مزایا و معایب خاص خویش هستند و همین مسئله نیز موجب تفاوت آن‌ها شده است. اصولا الگوریتم‌های رمزنگاری متقارن دارای سرعت بیشتری هستند و این مسئله را به این ویژگی خاص خود که به توان محاسباتی کمتری نیاز دارند، مدیون می‌باشند. ناگفته نماند با توجه به این نکته که در رمزنگاری متقارن ما از یک کلید واحد به منظور رمزگذاری و رمزگشایی بهره می‌بریم، در صورتی که این کلید در اختیار هر فردی قرار بگیرد به راحتی می‌تواند به اطلاعات ما دسترسی پیدا کند که طبیعتا چنین امری خطرات و تهدیدات امنیتی بالقوه‌ای را به همراه خواهد داشت.

در طرف دیگر، رمزنگاری نامتقارن با بهره‌گیری از کلید عمومی برای رمزگذاری و کلید خصوصی برای رمزگشایی این مشکل امنیتی را برطرف کرده است. هرچند که این الگوریتم رمزنگاری نیز به نوبه خود دارای نقاط ضعف قابل توجهی است و با توجه به طول بلندتر کلیدهای مورد استفاده در این الگوریتم رمزنگاری، این روش رمزنگاری به توان محاسباتی بالایی نیاز دارد و همین مسئله موجب کندی آن می‌شود.

تفاوت در کاربردها

با توجه به ویژگی‌های خاص هر کدام از الگوریتم‌های رمزنگاری متقارن و نامتقارن، کاربردهای متعددی را می‌توان برای هر یک از آن‌ها متصور بود. در رمزنگاری متقارن با توجه به سرعت این روش از آن در محافظت از اطلاعات در بسیاری از سیستم‌های رایانه‌ای مدرن مورد استفاده قرار می‌گیرد. از مثال‌بارزی که می‌توان برای کاربرد رمزنگاری متقارن مورد اشاره قرار داد، استفاده از استاندارد رمزنگاری AES به وسیله دولت ایالات متحده آمریکا به منظور رمزنگاری اطلاعات

مهم و محرمانه است. در طرف دیگر ماجرا که روش رمزنگاری نامتقارن قرار دارد، از آن غالبا در سیستم‌هایی کمک گرفته می‌شود که در این سیستم‌ها، تعداد قابل توجهی از کاربران بایستی پیام‌ها یا مجموعه‌ای اطلاعات را رمزگذاری و رمزگشایی نمایند. یکی از نمونه‌های بارز چنین سیستم‌هایی، ایمیل رمزنگاری شده است که در آن می‌توان با استفاده از کلید عمومی برای رمزگذاری و از کلید خصوصی برای رمزگشایی بهره برد.

الگوریتم‌های رمزنگاری متقارن و نامتقارن؛ غول‌های تامین امنیت اطلاعات

همان طور که در مطالب فوق مشاهده کردید، امروزه الگوریتم‌های رمزنگاری متقارن و نامتقارن نقش بسیاری کلیدی را در حفظ اطلاعات مهم و همچنین برقراری ارتباطات ایمن در دنیای دیجیتالی را ایفا می‌نمایند. هرچند که در نگاه کلی هر کدام از این دو الگوریتم مورد بحث بسیار مفید ظاهر شده‌اند؛ اما با توجه به ویژگی‌های خاص خود از مزایا و معایبی نیز برخوردار هستند. توصیه ما به آن دسته از مخاطبانی که به تازگی وارد دنیای کریپتوکارنسی شده‌اند و در میان اصطلاحات پیچیده این دنیای نوظهور سردرگم هستند، این است که حتما به سراغ بررسی عمقی چنین اصطلاحاتی بروند تا با دید بازتری به این دنیای جدید اعتماد کرده و سرمایه‌گذاری ایمنی را تجربه کنند. یکی از این اصطلاحات که ممکن است به هنگام مطالعه در ارتباط با دنیای کریپتوکارنسی با آن مواجه شوید، رمزنگاری متقارن و نامتقارن است که ما در این مقاله از **کیف پول من** به طور کامل به بررسی آن پرداختیم. در رمزنگاری متقارن از یک کلید واحد برای رمزگذاری و رمزگشایی استفاده می‌شود و این در حالی است که در رمزنگاری نامتقارن از کلید عمومی برای رمزگذاری و از کلید خصوصی برای رمزگشایی استفاده می‌شود. ناگفته نماند که اگر در ارتباط با مفهوم رمزنگاری متقارن و نامتقارن و همچنین تفاوت آن‌ها سوالی دارید که در این مقاله به آن اشاره نشده است، می‌توانید سوال خود را در بخش نظرات مطرح کنید تا کارشناسان ما در اسرع وقت به سوال شما پاسخ دهند.