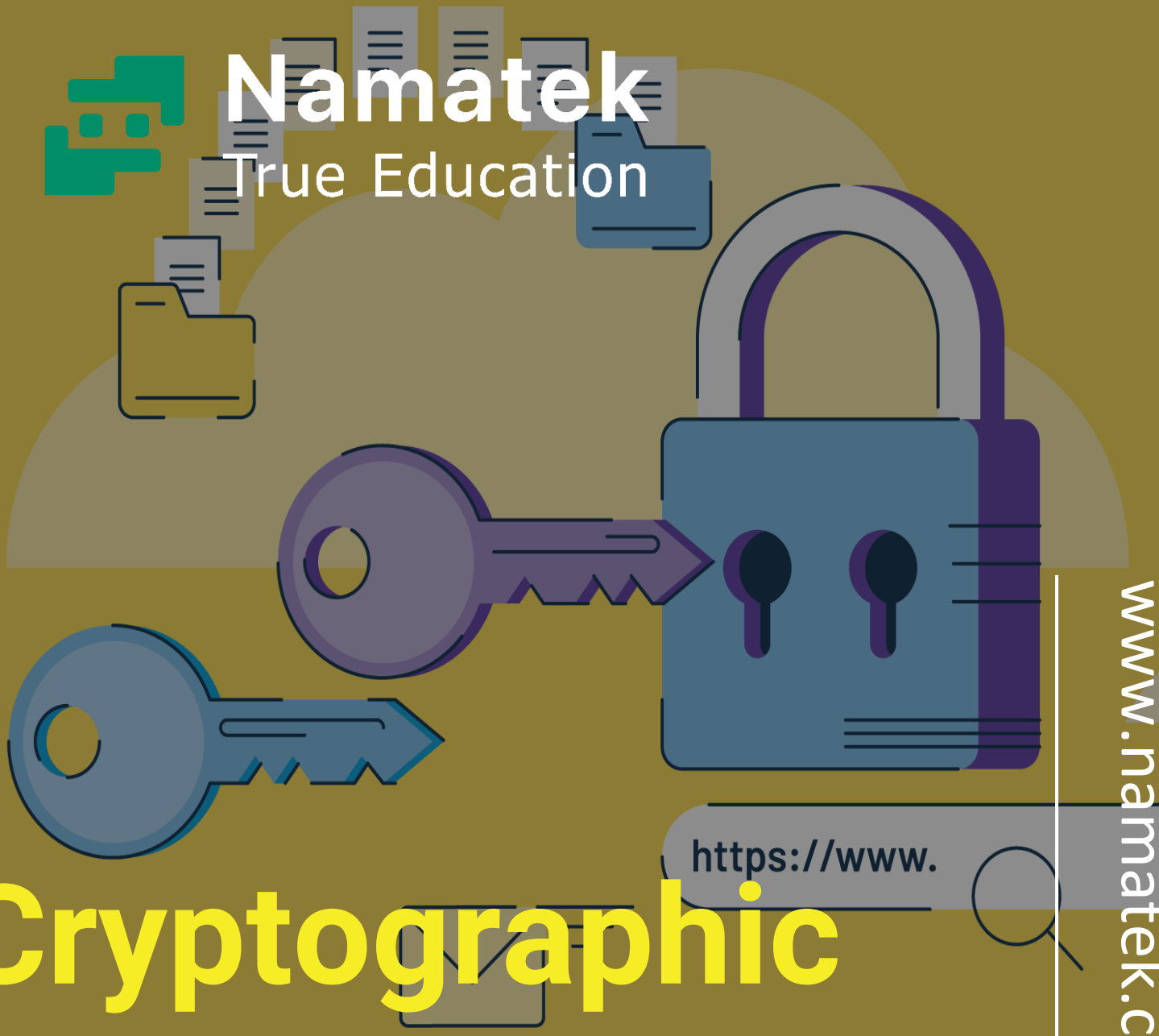
Namatek
True Education



Cryptographic Algorithm

الگوریتم رمزنگاری

www.namatek.com

فهرست مطالب

به کار گیری الگوریتم رمزنگاری برای تبادل هر نوع داده در بستر اینترنت امری ضروری است. بدون استفاده از این الگوریتم ها نمی توان امنیت جریان اطلاعات در بستر اینترنت را تضمین کرد. در نتیجه شرایط برای سو استفاده از اطلاعات شخصی کاربران و شرکت ها کاملا هموار می شود.

در این مطلب قصد داریم به معرفی انواع الگوریتم های رمزنگاری و بررسی تفاوت های آن ها بپردازیم. دعوت می کنیم تا پایان با ما همراه باشید.

الگوریتم رمزنگاری چیست؟

وقتی متنی را روی کاغذ می نویسید و قصد دارید بدون آن که دیگران به متن دسترسی پیدا کنند، آن را در اختیار فرد خاصی قرار دهید، چه می کنید؟ معمولا برگه ها را داخل پاکت هایی قرار داده و با چسب یا هر ابزار دیگری مهر و موم می کنید.

اگر تجربه نوشتن چک داشته باشید هم حتما با چسب های نواری که روی مبلغ می چسبانند، آشنا هستید. روش های مختلفی برای حفاظت از اطلاعات به صورت فیزیکی وجود دارد که هر کدام مزایا و معایب خود را دارند.

در دنیای مجازی اینترنت نیز برای جلوگیری از دسترسی دیگران به اطلاعات شخصی کاربران باید از روش های خاصی استفاده شود.

این جا دقیقا نقطه عطفی است که پای الگوریتم رمزنگاری (Cryptographic Algorithm) به میان می آید.

الگوریتم های رمزنگاری روش هایی برای محافظت از اطلاعات کاربران در بستر اینترنت هستند. منطق حاکم بر آن ها نسبتا ساده است.

پس از ارسال داده از سوی فرستنده در بستر اینترنت، الگوریتم ها اقدام به رمزگذاری آن ها می کنند. به عبارت دیگر داده ها از فرمت قابل خواندن و تشخیص به فرمت غیر قابل خواندن و ناشناس تبدیل می شوند.

در ادامه وقتی داده ها به مقصد می رسند، بار دیگر الگوریتم ها اقدام به رمزگشایی آن ها می کنند. به این معنی که داده ها از فرمت غیر قابل خواندن به صورت خوانا و قابل فهم تبدیل می شوند.

برای این که حلقه ارتباطی فوق بین گیرنده و فرستنده شکل بگیرد، از کلید رمزنگاری استفاده می شود. این کلید صرفا برای گیرنده و فرستنده اطلاعات قابل شناسایی است و دیگران نمی توانند به ماهیت آن پی ببرند.

در نتیجه الگوریتم های رمزنگاری به کمک این کلیدها ماموریت حفاظت از جریان داده در بستر اینترنت را انجام می دهند.

اجزای تشکیل دهنده الگوریتم های رمزنگاری

الگوریتم های رمزنگاری به چند دسته تقسیم می شوند که در بخش بعدی آن ها را معرفی می کنیم. اما ماهیت رمزگذاری (Encryption) در زمان ارسال و رمزگشایی (Decryption) هنگام دریافت اطلاعات در تمام آن ها مشترک است.

الگوریتم های رمزنگاری با استفاده از رشته ای از اعداد و حروف که به صورت تصادفی انتخاب می شوند، داده ها را رمزگذاری و رمزگشایی می کنند.

فارغ از این که درباره چه نوعی از الگوریتم رمزنگاری صحبت می کنیم، چند جزء اصلی در شکل گیری آن ها نقش دارند که در این بخش به آن ها می پردازیم.

متن شفاف (Clear Text)

متن شفاف را با نام متن ساده (Plain Text) نیز می شناسند.

منظور متن الزاما نوشته نیست؛ بلکه هر نوع داده ای مانند تصاویر، ویدیو و... را نیز شامل می شود.

پیامی که از سوی فرستنده برای گیرنده ارسال می شود و نیاز به رمزنگاری دارد را تحت عنوان متن شفاف می شناسند.

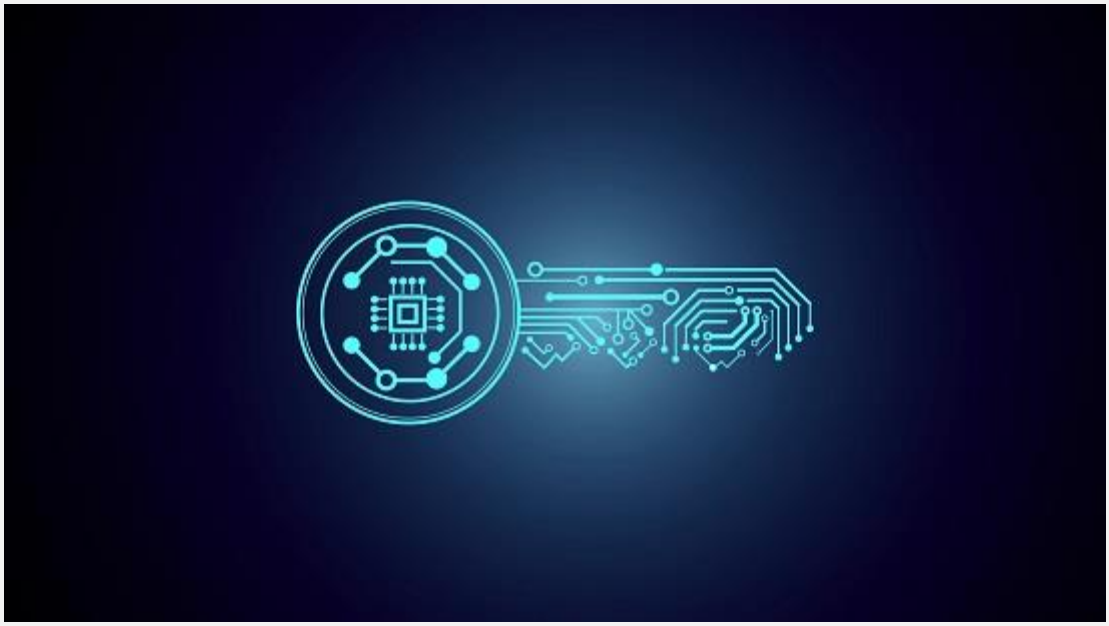
در حالت عادی این پیام قابل فهم است و باید با استفاده از الگوریتم آن را به حالت غیر قابل فهم تبدیل کرد.

کلید رمزنگاری (Cryptography Key)

کلید ابزار اصلی پیاده سازی الگوریتم رمزنگاری برای تبادل اطلاعات ایمن در بستر اینترنت به حساب می آید. متن شفاف با استفاده از کلید رمزنگاری به متن رمزنگاری شده تبدیل می شود.

هنگام تحویل داده به مقصد نیز متن رمزنگاری شده به کمک کلید به متن شفاف تبدیل می شود. اگر دیگران به کلید رمزنگاری دست پیدا کنند، عملا به تمام داده ها دسترسی خواهند داشت؛ بنابراین تاکید می شود که فرستنده ها و گیرنده ها در نگهداری از کلیدهای رمزنگاری بسیار حساس باشند.

کلیدهای رمزنگاری به دو دسته عمومی و خصوصی تقسیم می شوند که در ادامه بیشتر به توضیح در این باره می پردازیم.



متن رمزنگاری شده (Cipher Text)

متن شفاف پس از ارسال با استفاده از کلید رمزنگاری به متن رمزنگاری شده تبدیل می شود. این متن به صورت رمزگذاری شده و غیر قابل فهم ارسال می شود.

داده های تصادفی زیادی در متن رمزنگاری شده وجود دارد که آن را برای کسانی که کلید را در اختیار ندارند، غیر قابل فهم می کند.

انواع الگوریتم رمزنگاری

تا این جا با مفهوم رمزنگاری آشنا شدیم. بدیهی است که اهمیت اطلاعاتی که در بستر اینترنت جابجا می شوند، یکسان نیست.

گاهی اوقات با اطلاعات ساده ای سروکار داریم که حتی اگر دیگران به آن ها دسترسی هم پیدا کنند، مشکلی به وجود نمی آید؛ اما در مواقعی با داده های حساس مانند اطلاعات مالی افراد و شرکت ها مواجه هستیم.

کوچک ترین دسترسی به این اطلاعات از سوی سودجویان، مشکلات متعددی را به دنبال خواهد داشت.

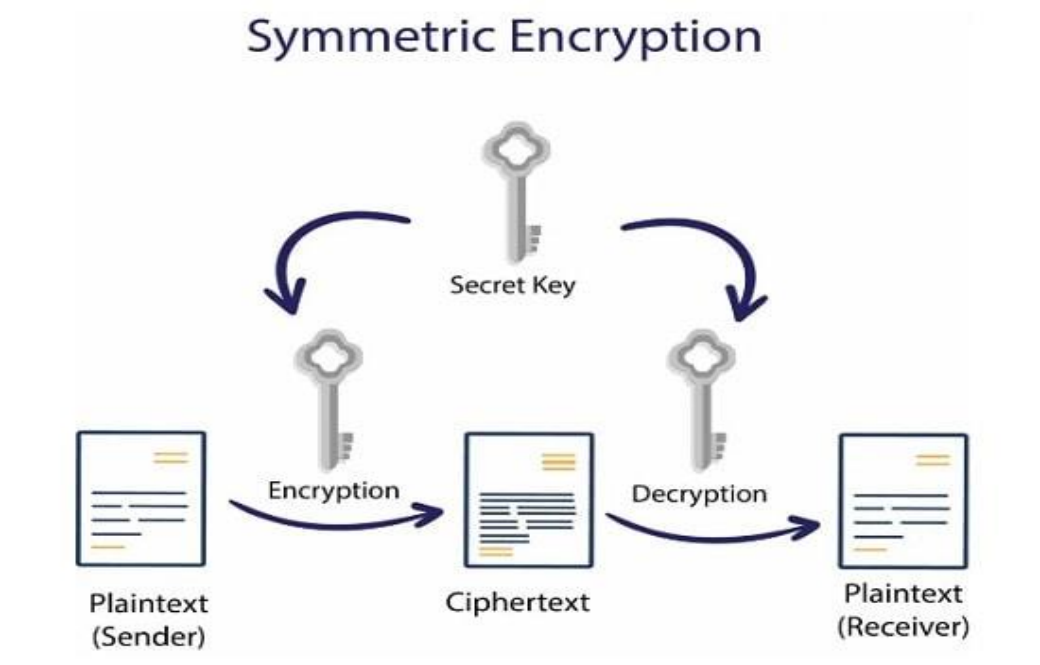
تفاوت در سطح اهمیت حفاظت از انتقال اطلاعات در اینترنت، باعث شده تا الگوریتم های رمزنگاری به روش های مختلفی ابداع شوند.

در همین راستا انواع الگوریتم های رمزنگاری را می توان به صورت زیر دسته بندی کرد:

الگوریتم رمزنگاری متقارن (Symmetric Cryptography Algorithm)

اولین الگوریتم رمزنگاری که برای حفاظت از اطلاعات در اینترنت مورد استفاده قرار گرفت، الگوریتم متقارن است.

داستان از این قرار است که در این الگوریتم برای رمزگذاری و رمزگشایی اطلاعات از کلید یکسانی استفاده می شود. در اصطلاح رایج به آن کلید مخفی (Secret Key) می گویند.



این کلید با استفاده از قوانین خاصی که مبتنی بر فرمول های ریاضی است، کار تغییر در داده ها را انجام می دهد.

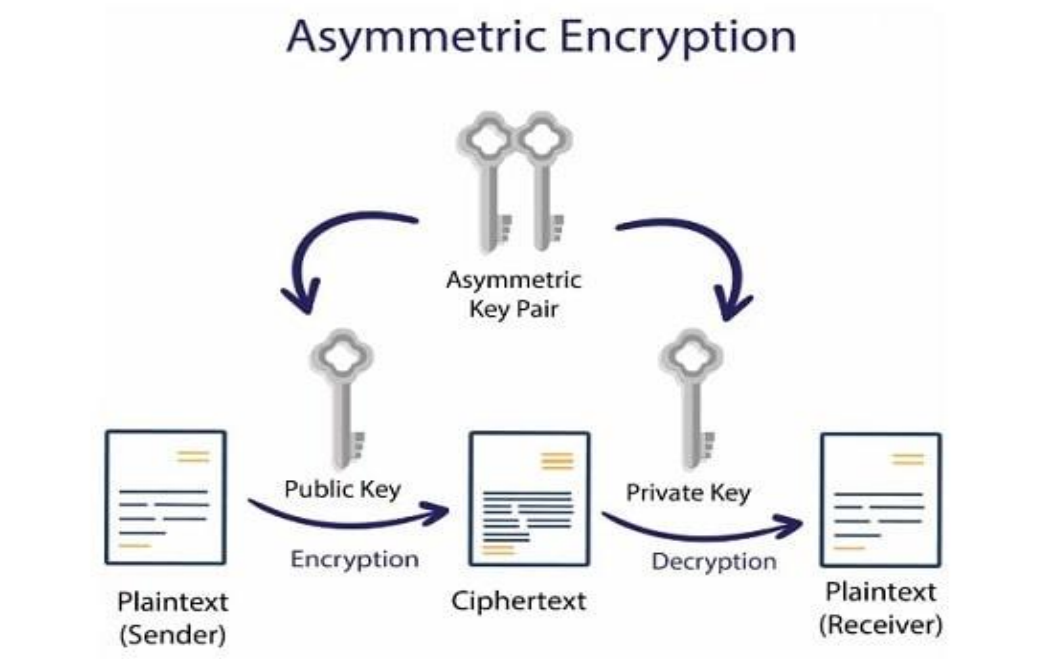
الگوریتم متقارن فرآیند انتقال داده ها را سریع تر از روش نامتقارن انجام می دهد؛ ولی در عین حال از امنیت کمتری برخوردار است.

الگوریتم رمزنگاری نامتقارن (Asymmetric Cryptography Algorithm)

سطح پیشرفته تری از الگوریتم های رمزنگاری که برای حفاظت از اطلاعات ابداع شد، با نام الگوریتم نامتقارن شناخته می شود. در این الگوریتم از دو کلید جداگانه برای رمزگذاری و رمزگشایی داده ها استفاده می شود.

کلید رمزگذاری و رمزگشایی در این الگوریتم به ترتیب با نام های کلید عمومی (Public Key) و کلید خصوصی (Secret Key) شناخته می شوند.

کلیدهای عمومی قابل انتشار هستند و می توان آن ها را در اختیار دیگران قرار داد؛ اما کلیدهای خصوصی باید نزد صاحبان آن ها به طور کاملا محفوظ باقی بمانند.



اگر تجربه فعالیت در بازار ارزهای دیجیتال را داشته باشید، به خوبی با این مفاهیم آشنا هستید. برای انتقال ارز دیجیتال بین کیف پول های مختلف باید از کلید عمومی استفاده کنید.

الگوریتم تابع هش (Hash Function Cryptography Algorithm)

نسل سوم الگوریتم رمزنگاری با نام تابع هش شناخته می شود.

در این الگوریتم دیگر خبری از کلید برای رمزگذاری و رمزگشایی اطلاعات نیست؛ بلکه داده با تعداد کاراکتر مشخصی در اختیار کاربر قرار می گیرد.

سپس با استفاده از فرمول های ریاضی، خروجی با طول ثابت و مشخص تولید می شود. خروجی این الگوریتم در اصطلاح به عنوان هش یا خلاصه پیام (Hashed Text) شناخته می شود.

هر تابع هش روی دو بلوک از داده ها کار می کند که از کنار هم قرار گرفتن آن ها زنجیره ای از بلوک ها به وجود می آید. دقت داشته باشید که الگوریتم هش کاملا یک طرفه کار می کند و پس از رمزگذاری، دیگر داده ها رمزگشایی نمی شوند.

از این روش معمولا برای ذخیره اطلاعات در بستر اینترنت استفاده می شود. بالاترین سطح امنیت برای تبادل دیتا در بستر اینترنت را الگوریتم تابع هش فراهم می کند. چرا که عملا کلیدی در کار نیست که با دسترسی دیگران به آن، امنیت داده ها به خطر بیفتد.