
# بررسی الگوریتم سایفر در کریپتوگرافی

## الگوریتم سایفر چیست؟

از آنجا که اینترنت شبکه‌ای از شبکه‌ها است و در واقع میلیاردها کاربر و سرور هر روزه به صورت تارهای به هم پیوسته در حال ارسال و دریافت اطلاعات و دیتا در بستر آن هستند؛ پس حفظ امنیت هر آنچه که ما بر روی اینترنت آپلود یا از آن دانلود می‌کنیم، اهمیت بسزایی دارد.

اهمیت بالا بردن پیچیدگی رمزنگاری داده‌ها آنجایی پررنگ‌تر می‌شود که یک سری حملات سایبری به منظور دسترسی به اطلاعات و تخریب و یا سو استفاده از آنها در بستر اینترنت انجام می‌گیرد و کاربران احتیاج دارند که در برابر اینگونه نفوذها مقام مانده و از حریم شخصی خود دفاع کنند. به این منظور الگوریتم‌های رمزنگاری بسیاری برای حفظ امنیت دیتا طراحی شدند.

ضرورت وجود چنین الگوریتم‌هایی در بعضی زمینه‌ها نظیر داد و ستد و معامله بر پایه اینترنت و در بازارهای مالی آنلاین نظیر کرپیتوکارنسی یا همان ارزهای دیجیتال بیشتر مشخص می‌شود؛ چرا که اگر امنیت داده در این زمینه به خوبی حفظ نشود، سرمایه میلیاردها انسان ممکن است در خطر قرار گیرد و اساسا این بازارها نابود می‌شوند.

الگوریتم سایفر یا رمز یکی از همین الگوریتم‌هاست که در واقع یک فرمول با ماهیت ریاضی است که به طور خاص برای رمزگذاری ارزش و محتوای یک داده طراحی شده تا بتواند اطلاعات آن را در محیطی شبکه‌ای مانند اینترنت حفظ کند. الگوریتم سایفر نیز مانند بسیاری از الگوریتم‌های رمزنگاری دیگر از یک عبارت خاص تحت عنوان کلید به عنوان بخشی از فرمول خود استفاده می‌کنند.

در واقع این فرمول طبق دستورالعمل‌های خود، داده مفید و قابل خوانش شما را که برای هکرها بسیار جذاب است، به یک داده ناخوانا و رمزنگاری تبدیل می‌کند که هر کسی جز خود الگوریتم نمی‌تواند آن را به حالت اولیه دربیاورد. کلیدی که این الگوریتم از آن استفاده می‌کند، دو منظوره می‌باشد یعنی این کلید همانطور که در ابتدا برای الگوریتم رمزنگاری ارز دیجیتال، اطلاعات و دیتا

استفاده می‌شود، می‌تواند در موقع نیاز نیز می‌تواند برای رمزگشایی مورد استفاده قرار بگیرد؛ به این ترتیب، سایفر الگورتیمی برای رمزنگاری و رمزگشایی داده هاست.

اگر بخواهیم این ویژگی را به صورت تخصصی‌تر بررسی کنیم، در اصل الگوریتم سایفر در کریپتوگرافی از روش رمزگذاری کلید متقارن استفاده می‌کند. رمزنگاری کلید متقارن که نام دیگرش رمزگذاری کلید مخفی است در واقع به این معنی است که در این روش رمزها به صورت متقارن عمل می‌کنند و با در نظر گرفتن یک کلید یکسان می‌توان هم داده‌ها و متن‌های ساده را به متن رمزی و هم متن رمزی را به داده‌ها و متون ساده تبدیل کرد. به متنی که توسط الگوریتم سایفر رمزنگاری می‌شود، در کریپتوگرافی سایفرتکست ciphertext نام دارد.

میزان **امنیت الگوریتم** با استفاده از کلیدهایی با طول بیشتر، بالا می‌رود؛ اما نکته‌ای که درخور توجه است این است که هرچه کلیدی که برای رمزنگاری داده استفاده می‌شود بزرگتر باشد، زمان محاسباتی که الگوریتم نیاز دارد تا دوباره داده را رمزگشایی کرده و به حالت دیتای مفید و قابل استفاده در آورد بیشتر می‌شود؛ از این رو اگر قرار است که از این الگوریتم در زمینه‌ها و برنامه‌هایی که زمان پاسخ برای ما اهمیت بسیاری دارد استفاده شود، بهتر است اندازه این کلید متناسب با نیاز حافظتی و همچنین هزینه محاسباتی که بر ما تحمیل می‌کند، انتخاب شود تا در میان این دو مورد اصلی تعادل ایجاد گردد.

برای مثال در زمینه بازار ارز دیجیتال که قیمت‌ها به صورت لحظه‌ای جابه‌جا شده و دچار نزول یا صعود می‌شوند، اگر از الگوریتم سایفر و کلیدی با طول بسیار زیاد استفاده شود، باعث می‌شود برای هر تراکنش مدتی منتظر بمانیم و این یعنی از دست دادن فرصت‌های لحظه‌ای بازار و حتی ضررهای احتمالی.

# الگوریتم سایفر در کریپتوگرافی چگونه عمل می‌کند؟


**الگوریتم سایفر** در کریپتوگرافی در اصل یک سیستم مبتنی بر **قوانینی ثابت** است که یک متن ساده و خوانا را به یک متن رمزی که رشته‌ای ظاهرا تصادفی از کاراکترهاست تبدیل می‌کند. الگوریتم سایفر می‌تواند به شیوه‌های متفاوتی عمل کند. اگر سایفر بتواند بیت‌های یک دیتا را به صورت پشت هم و به حالت **استریم رمزنگاری** و **رمزگشایی** کند، به آن **سایفر جریان** یا **استریم سایفر** می‌گویند.

همچنین الگوریتم سایفر می‌تواند متن رمزنگاری شده یا همان سایفر تکست را به صورت بسته‌ها و بلوک‌هایی با تعداد بیت مشخص تقسیم بندی کند که به آنها سایفرهای بلوک بندی شده می‌گویند. همانطور که گفتیم این الگوریتم وابسته به یک کلید مخفی است که از آن در روند رمزگذاری استفاده می‌کند و هرچه این کلیدها اندازه طولانی‌تری داشته باشند، بر حسب اندازه‌شان در برابر حملاتی نظیر brute-force (حمله جست‌وجوی فراگیر در اصل یک روش آزمون و خطا برای رمزگشایی داده‌های مهم و حساس نظیر رمزهای پسوورد است) بیشتر مقاوم‌اند.

البته کارشناسان حوزه کریپتوگرافی بر این نظرند که طول کلید همیشه ضامن امنیت بالاتر ما نخواهد بود؛ از این رو توصیه می‌کنند که در رمزنگاری‌ها، وابسته به الگوریتم از کلیدهای حداقل 128 بیتی یا بیشتر استفاده کنند. در واقع الگوریتم سایفر قوی به نوعی طراحی شده است که حتی اگر کسی الگوریتم بشناسد و آن را برنامه نویسی کند هم بدون دانستن کلید مناسب درگاه، نمی‌تواند داده را رمزگشایی کرده و به آن دسترسی پیدا کند و این نقطه قوت این الگوریتم است. به همین ترتیب، برای اینکه الگوریتم سایفر بتواند درست کار کند، فرستند و گیرنده هر دو باید یک مجموعه از کلیدها را داشته باشند.

الگوریتم سایفر همچنین می‌تواند به دو صورت کار کند؛ **الگوریتم سایفر متقارن** و **الگوریتم سایفر نامتقارن**. الگوریتم سایفر متقارن همانطور که گفته شد از کلیدی استفاده می‌کند که برای دو منظور رمزگذاری و رمزگشایی طراحی شده است؛ در حالیکه الگوریتم سایفر نامتقارن از **کلیدهای عمومی** و **کلیدهای خصوصی** بهره می‌برد.

مطلب پیشنهادی : آموزش پیدا کردن کلید خصوصی ولت ارز دیجیتال

رمزنگاری نامتقارن به رمزنگاری کلید عمومی هم شناخته می‌شوند و در این الگوریتم، در واقع کلیدها اعداد بسیار بزرگی هستند که با هم جفت شده‌اند اما با هم تفاوت دارند. در این الگوریتم کلید عمومی را می‌توان با هرکسی به اشتراک گذاشت؛ اما کلید خصوصی اطلاعاتی است که باید توسط خود فرد به صورت پنهانی نگهداری شود.

در واقع الگوریتم سایفر اینگونه عمل می‌کند که اگر شما با کلید عمومی رمزگذاری را انجام دهید با کلید خصوصی می‌توانید آن را رمزگشایی کنید؛ به همین ترتیب کلید خصوصی فقط در دست گیرنده پیام و کلید عمومی در دست هرکسی است که می‌خواهد پیام رمزنگاری شده را به مقصدی بفرستد.

## الگوریتم سایفر در کجا کاربرد دارد؟


الگوریتم سایفر با توجه به ماهیت خود بیشتر در ارتباطات آنلاین کاربرد دارد و به منظور ایمن سازی اطلاعات ما در بسیاری از پروتکل‌های متفاوت گنجانده شده است. این الگوریتم کمک می‌کند تبادل دیتا به صورت ایمن انجام شود. یکی از اصلی‌ترین کاربردهای الگوریتم سایفر رمزنگاری ارتباطات خصوصی است؛ برای مثال این الگوریتم در پروتکل لایه حمل (TLS) برنامه‌ها و همچنین **Secure Sockets Layer** برای رمزنگاری داده‌های ارسالی از سمت فرستنده و رمزگشایی داده‌های دریافتی در سمت گیرنده استفاده می‌شوند.

همچنین سایفر در فناوری‌های ارتباطی از جمله تلفن، تلویزیون‌های دیجیتال و دستگاه‌های خودپرداز نیز کاربرد دارد و همه این‌ها به این دلیل است که این دستگاه‌ها نیز امروزه به طریقی به اینترنت متکی هستند، پس نیاز دارند توسط الگوریتمی رمزنگاری شوند.

**کاربرد الگوریتم سایفر** همچنین می‌تواند شامل دنیای ارزهای دیجیتال نیز شود؛ چرا که دیتای این بازار نیز دارای حساسیت بالایی در نگهداری است و این الگوریتم می‌تواند با رمزگذاری و رمزگشایی به واسطه کلیدهای متفاوت هکران را از دسترسی به اطلاعات حساب‌های مشتریان ناکام بگذارد.

## با الگوریتم سایفر در کریپتوگرافی دیتای ارزشمند شما به خوبی حفظ می‌شود!

الگوریتم سایفر در کریپتوگرافی به عنوان یک الگوریتم قوی در رمزنگاری داده‌های مهم در بستر اینترنت به حساب می‌آید. با توجه به خطراتی که ممکن است امروزه همه ما را به عنوان یک کاربر در اینترنت مورد هدف قرار دهد، دزدیده شدن اطلاعات و خراب شدن بانک‌های اطلاعاتی شخصی ماست؛ از این رو الگوریتم‌های مانند الگوریتم سایفر در کریپتوگرافی می‌توانند نقش بسیار مهمی در این مسئله داشته باشند.

این الگوریتم به واسطه استفاده از یک کلید می‌تواند داده ما را رمزنگاری کند. الگوریتم سایفر به دو روش متقارن و نامتقارن کار کند. در الگوریتم سایفر متقارن، سایفر از یک کلید برای دو منظور استفاده می‌کند و با استفاده از آن هم داده خوانا و ساده ما را به **سایفر تکست** تبدیل کرده (رمزگذاری) و هم سایفرتکست را دوباره به حالت داده خوانا و قابل استفاده برمی‌گرداند (رمزگشایی).

مطلب پیشنهادی : کریپتوجکینگ چیست؟

اما در الگوریتم نامتقارن ما از دو کلید تحت عنوان کلید عمومی و کلید خصوصی استفاده می‌کنیم که کلید عمومی می‌تواند در اختیار همه باشد تا بقیه بتوانند به یک گیرنده پیام‌های رمزنگاری شده بفرستند؛ اما کلید خصوصی تنها در اختیار گیرنده است و می‌تواند از آن برای رمزگشایی استفاده نماید.

الگوریتم سایفر امروزه در انواع پروتکل‌های مربوط به ارتباطات خصوصی استفاده می‌شوند؛ برای مثال پروتکل لایه حمل (TLS) و Secure Sockets Layer. فناوری‌های ارتباطی نظیر تلفن، تلویزیون هوشمند و دستگاه‌های خودپرداز و به صورت کلی، هر سیستمی که به نوعی به اینترنت پایبند است و نیاز به گردش اطلاعات امن دارد، می‌تواند از الگوریتم سایفر استفاده کند.