روش های رمزنگار مدرن

نام و نام خانوادگی نویسنده اول (مجتبی کرکه آبادی)
مدرس دانشگاه آزاد واحد پیشوا ورامین

چکیده

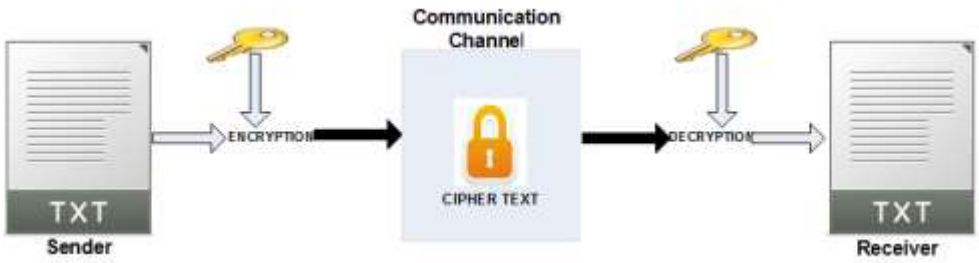
روش های رمزگذاری مدرن نقش مهمی در ایمن سازی داده های حساس در عصر دیجیتال دارند. با افزایش اتکا به فناوری و اینترنت، رمزگذاری برای محافظت از محرمانه بودن، یکپارچگی و صحت اطلاعات ضروری شده است. این چکیده مروری بر روش‌های رمزگذاری مدرن، اصول اصلی آنها و تأثیر آنها بر امنیت سایبری ارائه می‌کند. روش‌های رمزگذاری مدرن از الگوریتم‌ها و رمزنگاری‌های پیشرفته ریاضی برای تبدیل متن ساده به متن رمزی استفاده می‌کنند و اطمینان می‌دهند که فقط افراد مجاز می‌توانند به داده‌ها دسترسی داشته باشند و آن‌ها را تفسیر کنند. فرآیند رمزگذاری متکی بر کلیدهای رمزنگاری است که توالی منحصر به فردی از کاراکترها هستند که برای رمزگذاری و رمزگشایی اطلاعات استفاده می شوند. این کلیدها نقش حیاتی در تضمین امنیت داده های رمزگذاری شده ایفا می کنند، زیرا باید مخفی باقی بمانند و در برابر دستکاری های غیرمجاز مقاوم باشند. یکی از پرکاربردترین روش‌های رمزگذاری، استاندارد رمزگذاری پیشرفته است که مبتنی بر رمزنگاری کلید متقارن است. سایر روش‌های رمزگذاری مانند رمزنگاری منحنی بیضی نیز به طور گسترده در کاربردهای مختلف استفاده می‌شوند. این روش ها سطوح مختلفی از امنیت و کارایی را ارائه می دهند و به سازمان ها این امکان را می دهند که مناسب ترین روش رمزگذاری را برای نیازهای خاص خود انتخاب کنند.

رمزگذاری همچنین نقش مهمی در انتقال امن داده ها از طریق شبکه ایفا می کند و کانال های ارتباطی را از شنود و شنود محافظت می کند. با این حال، توجه به این نکته مهم است که رمزگذاری در برابر حملات مصون نیست و آسیب پذیری ها می توانند توسط افراد ماهر مورد سوء استفاده قرار گیرند. تحقیق و توسعه مداوم در زمینه رمزگذاری برای جلوتر ماندن از تهدیدات سایبری در حال تحول حیاتی است. علاوه بر این، مدیریت کارآمد کلیدهای رمزنگاری، از جمله تولید، توزیع و ذخیره سازی آنها، برای حفظ امنیت و اثربخشی سیستم های رمزگذاری حیاتی است. در نتیجه، روش‌های رمزگذاری مدرن در حوزه امنیت سایبری ضروری هستند. با به کارگیری الگوریتم‌های پیچیده و تکنیک‌های رمزگذاری، سازمان‌ها می‌توانند از داده‌های حساس خود در برابر دسترسی غیرمجاز محافظت کنند و محرمانگی، یکپارچگی و صحت اطلاعات را حفظ کنند. درک کامل و اجرای روش‌های رمزگذاری مدرن برای اطمینان از اقدامات امنیتی قوی در دنیای دیجیتالی که به طور فزاینده‌ای به هم پیوسته است، ضروری است.

واژگان کلیدی: رمزنگاری پیشرفته، ایمنی داده ها، الگوریتم رمزنگاری، کد گذاری محرمانه.

مقدمه

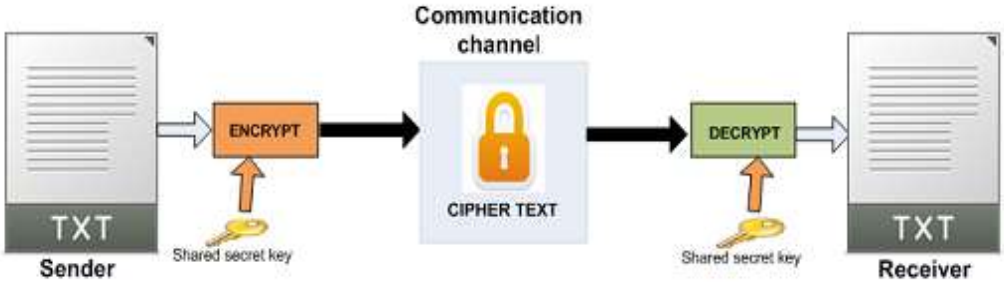
رمزنگاری هنر مخفی نویسی است که از زمان رومیان برای مخفی نگه داشتن اطلاعات محرمانه استفاده می شود. برای مخفی نگه داشتن اطلاعات، یک روش پرکاربرد رمزگذاری/رمزگشایی است. اساساً رمزگذاری/رمزگشایی کارکردهای اساسی رمزنگاری هستند. در رمزگذاری، یک پیام ساده (متن ساده) به شکل غیرقابل خواندن به نام متن رمز تبدیل می شود. در هنگام رمزگشایی، یک متن رمزی به متن اصلی (متن ساده) تبدیل می شود. هر دوی این عملکردها برای ایمن کردن پیام در برابر افرادی که مجاز به مشاهده محتوای پیام نیستند استفاده می شود [۱]. کار ساده توابع رمزگذاری و رمزگشایی در شکل ۱ نشان داده شده است [۲].



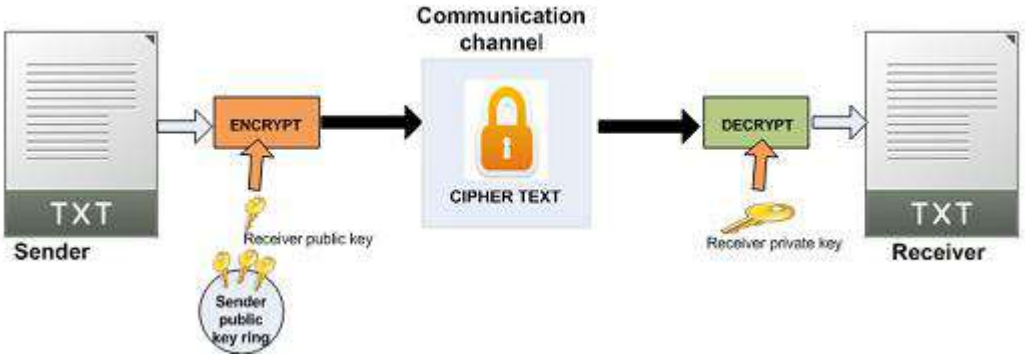
شکل ۱. کار رمزگذاری و رمزگشایی [۲].

مدل های متقارن و نامتقارن انواعی از رمزنگاری هستند که به طور گسترده پذیرفته شده‌اند. مدل متقارن (که رمزنگاری کلید متقارن[1] نیز نامیده می شود) از ارتباط ایمن بین فرستنده و گیرنده با استفاده از همان کلید مخفی متمرکز استفاده می کند در حالیکه رمزنگاری نامتقارن (که رمزنگاری کلید عمومی[2] نیز نامیده می شود) ارتباط را با استفاده از کلیدهای عمومی و خصوصی ایمن می کند [۳]. کلید خصوصی در ارتباطات به صورت جداگانه نگه داشته می شود در حالی که کلید عمومی به دلیل ماهیت عمومی برای همه شناخته شده است. شکل ۲ الف و ب به ترتیب رمزنگاری متقارن و نامتقارن را نشان می دهد. برای ایمن سازی ارتباطات، اندازه کلید مهمترین پارامتر در رمزنگاری متقارن و متقارن است. اندازه کلید رمزنگاری متقارن کمتر از رمزنگاری نامتقارن است که امنیت رمزنگاری متقارن را برای داده‌های حساس‌تر کمتر می‌کند [۴]. زمان محاسباتی رمزنگاری نامتقارن بیشتر از رمزنگاری متقارن است که رمزگذاری/رمزگشایی را برای حجم زیادی از داده ها پیچیده تر می کند [۵].

[1] symmetric key cryptography
[2] public key cryptography



الف) رمزنگاری متقارن

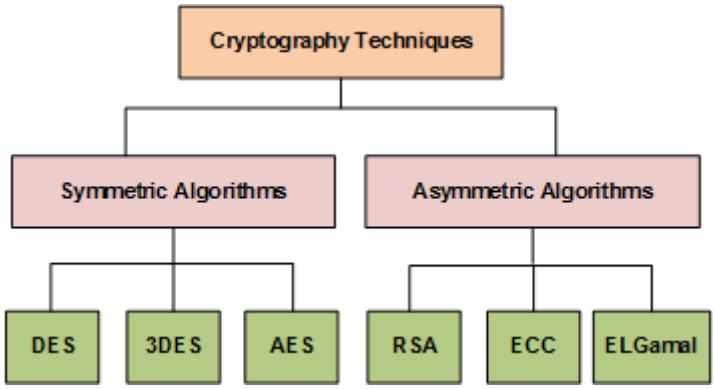


ب) رمزنگاری نامتقارن

شکل ۲. نمایی از رمزنگاری الف) متقارن، ب) نامتقارن [۶].

با توجه به اندازه کلید بزرگتر و زمان محاسباتی بیشتر رمزنگاری نامتقارن، رمزنگاری کلید عمومی یک بار فقط برای تبادل کلید استفاده می شود و رمزگذاری/رمزگشایی بیشتر توسط رمزنگاری کلید متقارن انجام می شود [۷]. زمان محاسباتی تکنیک های رمزنگاری بیشتر به عنوان زمان رمزگذاری/رمزگشایی، تولید کلید و زمان تعویض کلید طبقه بندی می شود. زمان رمزگذاری/رمزگشایی با تبدیل یک متن ساده (پیام) به متن رمزی و بالعکس محاسبه می شود [۸]. زمان تولید کلید بسته به اندازه طول کلید است که برای رمزنگاری متقارن و نامتقارن متفاوت است. زمان تبادل کلید به کانال ارتباطی بین فرستنده و گیرنده بستگی دارد [۳, ۹]. الگوریتم های رمزنگاری زیادی برای رمزگذاری و رمزگشایی طراحی شده است [۱۰]. همانطور که در بالا توضیح داده شد، طرح های رمزنگاری به عنوان الگوریتم های متقارن و نامتقارن طبقه بندی می شوند. در این مقاله، الگوریتم های متقارن شامل مدل استاندارد رمزگذاری داده ها[۳]، مدل استاندارد رمزگذاری داده های سه گانه[۴]، مدل استاندارد رمزگذاری پیشرفته[۵]. همچنین، الگوریتم های نامتقارن عبارتند از مدل آراس‌ای[۶]، مدل الگامال[۷] و مدل رمزنگاری منحنی بیضوی[۸] [۱۱]. شکل ۳ طبقه بندی تکنیک های رمزنگاری را شرح می دهد [۱۲].

[3] Data Encryption Standard (DES)
[4] Triple Data Encryption Standard
[5] Advanced Encryption Standard
[6] Rivest, Shamir and Adleman (RSA)
[7] Elgamal
[8] Elliptic Curve Cryptography



شکل ۳. طبقه بندی تکنیک های رمزنگاری [۱۲].

۱. مروری بر ادبیات

الگوریتم‌های رمزنگاری زیادی وجود دارند که برای ایمن کردن اطلاعات استفاده می‌شوند مانند استاندارد رمزگذاری داده ها و پیلیئر[9] [۲]. همه این الگوریتم ها در مدل خود منحصر به فرد هستند. با این حال، مشکل این است که چگونه می توان بهترین الگوریتم امنیتی را پیدا کرد که امنیت بالایی را فراهم می کند و همچنین زمان کمتری را برای تولید کلید، رمزگذاری و رمزگشایی اطلاعات صرف کند. الگوریتم های امنیتی به مزایا و معایب هر الگوریتم، نیاز و مناسب برای کاربردهای مختلف بستگی دارد [۱۳]. در مطالعه انجام شده توسط مرجع [۱۴] ارزیابی شده است که عملکرد دو الگوریتم استاندارد رمزگذاری داده ها و مدل بلوفیش[10] بر اساس پارامترهای خاصی مانند سرعت رمزگذاری، مصرف انرژی و تحلیل امنیتی. نتایج آزمایش نشان داد که عملکرد مدل بلوفیش از الگوریتم استاندارد رمزگذاری داده ها و استاندارد رمزگذاری پیشرفته سریع‌تر است [۱۵]. با این حال، در مرجع [۱۶] نتایج نشان داد که عملکرد مدل استاندارد رمزگذاری پیشرفته نسبت به مدل بلوفیش خوب است. در مرجع [۱۰] برخی از جزئیات الگوریتم های رمزنگاری مانند استاندارد رمزگذاری پیشرفته، استاندارد رمزگذاری داده ها، استاندارد رمزگذاری داده های سه گانه و مدل بلوفیش آورده شده است. علاوه بر این، عملکرد این الگوریتم های امنیتی نیز ارزیابی شده و آزمایش بر روی فایل متنی و تصویر انجام می شود. نتیجه مطالعات آنها نشان داد که عملکرد همه الگوریتم‌ها در مقایسه با مدل بلوفیش کاهش می‌یابد زیرا اندازه بسته افزایش می‌یابد. با این حال، انتخاب تصویر به عنوان نوع داده به جای فایل متنی و سپس مدل بلوفیش الگوریتم زمان بیشتری را نسبت به الگوریتم‌های استاندارد رمزگذاری پیشرفته، استاندارد رمزگذاری داده هاو استاندارد رمزگذاری داده های سه گانه صرف کرده است. نتیجه آنها همچنین نشان داد که استاندارد رمزگذاری داده ها هنوز در عملکرد سریعتر از استاندارد رمزگذاری داده های سه گانه است [۱۰].

در مرجع [۱۷] اندازه های مختلف یک فایل را برای ارزیابی عملکرد الگوریتم رمزنگاری در نظر گرفته شده است. این آزمایش بر روی تک پردازنده و محاسبات ابری انجام شده است. نتیجه آنها ثابت کرد که الگوریتم رمزنگاری در محاسبات ابری سریعتر از یک کامپیوتر تک پردازنده کار می کند. استاندارد رمزگذاری پیشرفته با فایل ورودی کوچک دارای بالاترین نسبت سرعت است، در حالی که مدل آراس‌ای زمان برترین است. در مطالعات انجام شده توسط مرجع [۱۸]، عملکرد الگوریتم های رمزنگاری مختلف مانند استاندارد رمزگذاری داده ها، استاندارد رمزگذاری پیشرفته و استاندارد رمزگذاری داده های سه گانه را برای یافتن زمان رمزگذاری و رمزگشایی و

[9] Paillier
[10] Blowfish

توان عملیاتی برای سخت افزارهای مختلف ارزیابی شد. از این الگوریتم ها برای محاسبه زمان رمزگذاری استفاده می شود. زمان رمزگذاری با افزایش اندازه داده ها در حال افزایش است. بنابراین، سرعت افزایش رمزگذاری به فایل (بر حسب بایت) بستگی دارد نه به نوع داده یک فایل [۱۹]. توان عملیاتی استاندارد رمزگذاری داده های سه گانه در مقایسه با استاندارد رمزگذاری پیشرفته، فایل های متنی و تصاویر مورد استفاده برای ارزیابی عملکرد کمتر است [۲۰]. چارچوب خالص نقطه ای برای اجرای استاندارد رمزگذاری داده ها و مدل سه گانه آن استفاده می شود که در مقایسه با الگوریتم استاندارد رمزگذاری پیشرفته زمان پردازش بیشتری را می طلبد [۱۸]. فقط از یک پارامتر برای اندازه گیری زمان رمزگذاری استفاده می شود. عملکرد استاندارد رمزگذاری داده ها برای استفاده از نرم افزار سریعتر نیست. با این حال، عملکرد استاندارد رمزگذاری داده ها روی سخت افزار سریعتر است [۲۱].

عملکرد استاندارد رمزگذاری پیشرفته، استاندارد رمزگذاری داده ها و مدل بلوفیش با استفاده از اندازه های مختلف فایل متنی از نظر سرعت رمزگذاری و رمزگشایی ارزیابی شده است. در مطالعه انجام شده توسط مرجع [۲۲]، مدل آراس‌ای، استاندارد رمزگذاری داده ها و استاندارد رمزگذاری پیشرفته مورد بحث قرار گرفته است. تجزیه و تحلیل ها بر اساس برخی پارامترها مانند استفاده از حافظه، زمان محاسبه و بایت خروجی انجام می شود. فایل متنی مورد استفاده برای ارزیابی و پیاده سازی نتیجه که نشان می دهد استاندارد رمزگذاری داده ها و استاندارد رمزگذاری پیشرفته تفاوت جزئی برای زمان رمزگذاری فایل دارند در حالی که زمان رمزگذاری مدل آراس‌ای طولانی ترین است و همچنین حافظه بالایی را مصرف می کند. سرویس گیرنده و سرور موبایل برای ارزیابی عملکرد الگوریتم رمزنگاری مدل آراس‌ای و رمزنگاری منحنی بیضوی استفاده می شود [۷]. پروتکل امنیتی لایه حمل و نقل بی سیم[11] برای ارزیابی عملکرد استفاده می شود. در آزمایش آنها، نتایج نشان می دهد که مدل آراس‌ای برای سمت کلاینت سریع‌تر است اما عملکرد در سمت سرور در مقایسه با عملکرد مدل رمزنگاری منحنی بیضوی کندتر است.

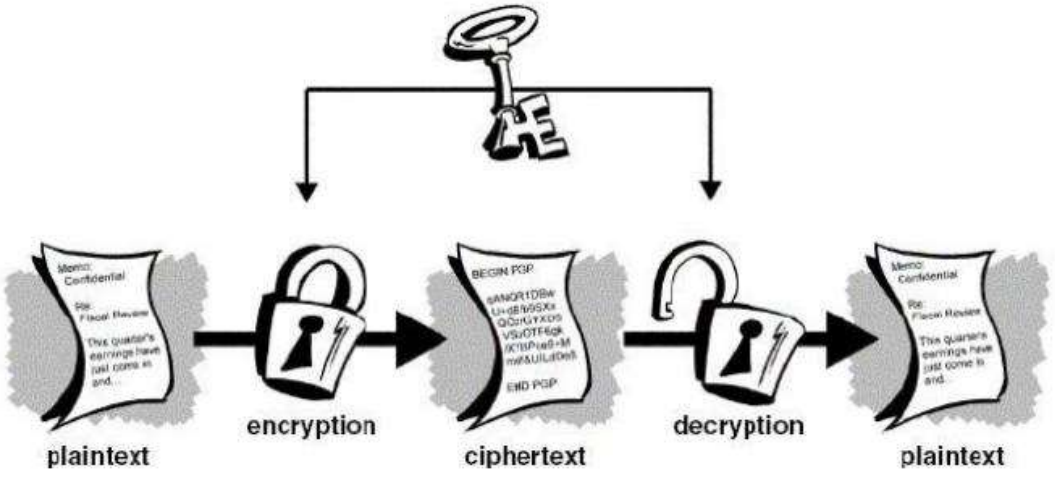
مدل آراس‌ای، الگامال و پیلیئر برای ارزیابی عملکرد بر اساس پارامترهایی مانند اندازه فایل رمزگذاری شده، اندازه فایل رمزگشایی شده، زمان رمزگذاری، زمان رمزگشایی و توان عملیاتی استفاده شده‌اند. نتایج تجربی نشان داد که زمان رمزگذاری مدل آراس‌ای بهتر از الگامال است اما زمان رمزگشایی الگامال بهتر از مدل آراس‌ای است. همچنین نتایج نشان داد که توان عملیات رمزگذاری مدل آراس‌ای بهتر و توان عملیاتی در فرآیند رمزگشایی عملکرد الگامال بهتر از مدل آراس‌ای است. عملکرد کلی با توجه به پارامتر انتخاب شده مدل آراس‌ای بهتر از همه دو الگوریتم دیگر پیلیئر و الگامال است [۲۳]. در مرجع [۲۴] تجزیه و تحلیل کاغذ انجام شده و مدل آراس‌ای با اندازه کلید و متغیر طول کلمه متفاوت از نظر فرآیند رمزگذاری و رمزگشایی نیاز به اندازه حافظه و زمان اجرا دارد. نتایج آزمایش نشان داد که زمان اجرای مدل آراس‌ای کند است و در مقایسه با رمزنگاری منحنی بیضوی به حافظه بیشتری نیاز دارد. توافق کلید و توزیع کلید مشکل اصلی در الگوریتم استاندارد رمزگذاری داده ها است، اما در رمزگذاری و رمزگشایی مدل آراس‌ای، هر دو عملیات زمان بیشتری را صرف می‌کنند. نتایج مرجع [۲۵] در یک شبیه سازی نشان داد که مدل آراس‌ای در عملکرد کندتر از استاندارد رمزگذاری داده ها است و ارزیابی کرد که توان عملیاتی الگوریتم آراس‌ای بهتر از الگوریتم استاندارد رمزگذاری داده ها نیست. همچنین، نتایج شبیه‌سازی نشان داد که توان مصرفی و توان عملیاتی الگوریتم استاندارد رمزگذاری داده ها بسیار بهتر از الگوریتم دیگری است [۲۵].

۲. سیستم کریپتو و اصطلاحات مرتبط

[11] Wireless Transport Layer Security

سیستم رمزنگاری مجموعه ای از الگوریتم ها و پروتکل هایی است که برای امنیت ارتباطات و تبادل اطلاعات استفاده می شود. از سه جزء اصلی تشکیل شده است [۲۶]: الگوریتم های رمزگذاری، الگوریتم های رمزگشایی و رویه های مدیریت کلید. الگوریتم های رمزگذاری برای تبدیل متن ساده (داده های رمزگذاری نشده) به متن رمزی (داده های رمزگذاری شده) استفاده می شود. این الگوریتم ها از یک کلید یا کلیدهای مخفی برای انجام فرآیند رمزگذاری استفاده می کنند و متن رمز را برای اشخاص غیرمجاز نامفهوم می کنند. از سوی دیگر، الگوریتم‌های رمزگشایی برای تبدیل مجدد متن رمزگذاری شده به متن ساده با استفاده از همان کلید مخفی که برای رمزگذاری استفاده می‌شد، استفاده می‌شوند. رمزگشایی فقط باید توسط افراد مجاز که دارای کلید صحیح هستند امکان پذیر باشد. رویه های مدیریت کلید شامل تولید، ذخیره و توزیع کلیدهای رمزگذاری ایمن است [۲۷]. قدرت یک سیستم رمزنگاری به محرمانه بودن و تصادفی بودن کلیدهای استفاده شده بستگی دارد. مدیریت صحیح کلید برای جلوگیری از دسترسی غیرمجاز به داده های رمزگذاری شده بسیار مهم است. سیستم‌های رمزنگاری به طور گسترده در برنامه‌های کاربردی مختلفی مانند ارتباطات امن از طریق اینترنت، رمزگذاری داده‌ها برای حفاظت از حریم خصوصی، ذخیره‌سازی امن اطلاعات حساس و سیستم‌های احراز هویت برای تأیید هویت کاربران یا نهادها استفاده می‌شوند. در زیر برخی از رایج ترین اصطلاحات مورد استفاده در زمینه رمزنگاری آمده است. شکل ۴ شماتیکی از فرایند رمزگذاری را نشان می دهد [۲۸].

- ✓ متن ساده یا واضح متن ساده ای است که به راحتی برای انسان قابل درک است.
- ✓ فرآیند استفاده از الگوریتم های ریاضی برای پنهان کردن اطلاعات حساس در متن ساده رمزگذاری نامیده می شود.
- ✓ این الگوریتم‌ها که اغلب به عنوان رمزارز شناخته می‌شوند، از مجموعه‌ای از فرآیندهای کاملاً تعریف شده تشکیل شده‌اند که پیام مخفی را برای هر مهاجمی غیرقابل شکست می‌سازند. پس از رمزگذاری، متن رمزی برای شما باقی می ماند که هیچ معنایی ندارد. این مرحله ای است که پیام شما در آن پنهان می شود.
- ✓ برای اینکه کار کند به کلیدی نیاز است که مختص الگوریتم و پیام باشد.
- ✓ کلید و نام الگوریتم برای رمزگشایی متن رمزگذاری شده باید شناخته شود. رمزگشایی فرآیند تبدیل متن رمز شده به متن ساده است.



شکل ۴. شماتیکی از فرایند رمزگذاری [۲۷].

برای بازیابی همان متن ساده از روش رمزگشایی، باید همیشه کلید یکسانی ارسال شود. اگر کلید دستکاری شده باشد، خروجی غیرمنتظره، نامطلوب یا معمولاً ناخواسته خواهد بود. در نتیجه، کلید چیزی است که باید محافظت شود. مهاجمان ممکن است از الگوریتم آگاه باشند و متن رمز را در اختیار داشته باشند. تا زمانی که کلید را ندانند، نمی توانند پیام را بشکنند. یک سیستم رمزنگاری از تمام این تکنیک ها، پروتکل ها و اصطلاحات تشکیل شده است. به اجرای ایمن روش‌های رمزنگاری کمک می‌کند و پنهان کردن محتوای پیام را آسان‌تر می‌کند. سپس داده ها را می توان در صورت نیاز در زیرساخت سیستم رمزگشایی کرد [۲۸].

۳. اصول رمزنگاری

چالش درک پیامی که برای شما در نظر گرفته نشده بود و در واقع عمداً پنهان شده بود، چالشی گسترده است که در زمینه های مختلف ظاهر شده است. در زمینه ارتباطات نظامی به اوج سختی خود دست یافته و بیشترین نوآوری را در راه حل الهام گرفته است. هدف این بخش برجسته کردن برخی اصول اساسی است. ممکن است روش‌های جایگزینی برای بیان این اصول و همچنین مفاهیم دیگر وجود داشته باشد، اما اینها به این معنا اساسی هستند که نمی‌توان از آنها اجتناب کرد. به بیان ساده، یک رهگیر B به پیام‌های ارسال شده از A به c گوش می‌دهد، که برای نگه داشتن B در ناآگاهی تلاش می‌کنند. تنها راه موفقیت A و C این است که آنها از برخی اطلاعات پس زمینه استفاده کنند که B از آنها بی اطلاع است. این معمولاً محتوای از پیش تنظیم شده است که به آن "کلید" می گویند [۲۸]. سپس پیام در این زمینه درج می شود تا یک عبارت منسجم ایجاد شود. اصل اول این است که ارتباطات A و C باید حاوی اطلاعاتی باشند که رهگیر در اختیار ندارد. اگر قرار است پیوند A به C مفید باشد، باید بتواند هر پیامی را از بانک عظیمی از امکانات بپذیرد و این کار را در مقادیر زیاد انجام دهد. غیرممکن است که A از قبل پیش بینی کند چه پیام هایی از این بانک ارسال خواهد کرد و نه به چه تعداد. پیوند ارتباطی در صورت امکان غیر ضروری خواهد بود. ارتباط دهنده هیچ کنترلی بر پیام هایی که قرار است ارسال شود ندارد. آ؛ او باید همه افراد را ببرد. کلید او باید ویژگی های مشابهی داشته باشد. باید غیر قابل پیش بینی باشد اگر کلیدهای او همگی از یک زیرمجموعه کاملاً تعریف شده باشند، تحلیلگر رمزارز B به محض اینکه متوجه این موضوع شد، احتمال بازیابی اطلاعات زیادی دارد. به عنوان مثال، تصور کنید کلید شامل صفر نیست و برای افزودن ارقام به متن ساده دیجیتال استفاده می‌شود. اصل دوم این است: اگر کلید از زیرمجموعه‌ای باشد که تقریباً همه احتمالات را حذف می‌کند، تحلیلگر رمز در نهایت می‌تواند برخی از پیام‌ها را بخواند. ضعف دیگر این است که مجموعه کلیدهای ممکن ممکن است وجود داشته باشد. رمزارز تنها زمانی می تواند با یک کلید فرعی برخورد کند که کلید بتواند به صورت ترکیبی از کلیدهای فرعی به گونه ای نمایش داده شود که این نمایش از طریق رمزگذاری انجام شود. برای مثال Hagelin C-38 دارای کلیدی است که حاصل مشارکت ۶ چرخ مختلف است. حمله به یکی از این چرخ ها در یک زمان یک راه معمول برای یافتن راه حل است. این اصل سوم است. اگر بتوان کلیدها را به گونه ای تقسیم کرد که تقسیم از طریق رمزگذاری انجام شود، تحلیلگر رمز می تواند هر بار به یک بخش حمله کند. رمزنگار A و رمزنگار B درگیر یک بازی ریاضی هستند. بازی به گونه ای است که سود یکی لزوما با ضرر دیگری برابر نیست. منبع پیام و خطراتی که ممکن است در مسیر با آنها روبرو شوند، هر دو جنبه‌های شانس کلیدی در بازی هستند (شکست). بازیکن A باید استراتژی خود را از قبل انتخاب کند و در حالت دفاعی باشد. او نمی تواند اشتباه کند.

بازیکن B در حالت تهاجمی است و زمانی که اطلاعات تازه در دسترس قرار می گیرد، می تواند استراتژی خود را تنظیم کند. این واقعیت که این یک بازی است، دشواری عظیمی را توضیح می دهد که هر تلاشی برای فهرست نویسی حملات رمزنگاری با آن مواجه خواهد شد. این سطح از پیچیدگی معمولاً در تجویز جامع یک استراتژی دیده می شود. اصل چهارم این است که گزینه‌های موجود برای A و B استراتژی‌های بازی را تشکیل می‌دهند که در آن اثربخشی هر بازیکن توسط اقدامات دیگری تعیین می‌شود.

٤. تکنیک‌های مدرن رمزنگاری

انواع روش‌های رمزگذاری مدرن به تکنیک‌های متعددی اشاره دارد که برای ایمن کردن و محافظت از داده‌های الکترونیکی و ارتباطات از دسترسی یا حملات غیرمجاز استفاده می‌شوند. این روش‌ها لایه‌ای قوی از محرمانگی و یکپارچگی را فراهم می‌کنند و تضمین می‌کنند که اطلاعات در دنیای دیجیتالی فزاینده ایمن و ایمن باقی می‌مانند [۲۸]. یکی از روش‌های رایج رمزگذاری مدرن، رمزگذاری متقارن است که شامل استفاده از یک کلید مخفی برای رمزگذاری و رمزگشایی داده‌ها می‌شود. این کلید معمولاً بین فرستنده و گیرنده به اشتراک گذاشته می شود و اطمینان حاصل می کند که فقط اشخاص مجاز می توانند به اطلاعات دسترسی داشته باشند. الگوریتم‌های رمزگذاری متقارن مانند استاندارد رمزگذاری پیشرفته و استاندارد رمزگذاری داده‌ها معمولاً در برنامه‌های مختلف مانند پیام‌رسانی امن، ذخیره‌سازی فایل‌ها و رمزهای بلاک استفاده می‌شوند [۲۶]. یکی دیگر از روش های مهم رمزگذاری، رمزگذاری نامتقارن است که به عنوان رمزنگاری کلید عمومی نیز شناخته می شود. از دو کلید مجزا اما از نظر ریاضی مرتبط استفاده می کند: یک کلید عمومی و یک کلید خصوصی. کلید عمومی با دیگران به اشتراک گذاشته می شود در حالی که کلید خصوصی توسط مالک مخفی نگه داشته می شود. رمزگذاری با استفاده از کلید عمومی گیرنده انجام می شود و فقط گیرنده می تواند با استفاده از کلید خصوصی خود آن را رمزگشایی کند. الگوریتم های رایج رمزگذاری نامتقارن شامل استاندارد رمزگذاری پیشرفته، Diffie-Hellman، و رمزنگاری منحنی بیضوی هستند [۲۸]. توابع هش یکی دیگر از اجزای ضروری روش های رمزگذاری مدرن هستند. این الگوریتم‌ها داده‌های ورودی را می‌گیرند و یک خروجی با اندازه ثابت تولید می‌کنند که به عنوان مقدار هش یا خلاصه پیام شناخته می‌شود. توابع هش معمولاً برای ذخیره رمز عبور، امضای دیجیتال و تأیید صحت داده ها استفاده می شود. توابع هش محبوب عبارتند از الگوریتم هش ایمن (SHA-2 و SHA-3) و الگوریتم خلاصه پیام[12]. علاوه بر این، روش‌های رمزنگاری مدرن، حالت‌های عملیاتی مختلفی را برای رفع نیازهای مختلف ترکیب می‌کنند. زنجیره بلوک رمز[13]، کتاب کد الکترونیکی[14] و حالت شمارنده[15] نمونه‌هایی از حالت‌هایی هستند که نحوه تقسیم، رمزگذاری و رمزگشایی بلوک‌های داده را تعریف می‌کنند. در سال های اخیر، ظهور محاسبات کوانتومی نگرانی هایی را در مورد امنیت روش های رمزگذاری سنتی ایجاد کرده است. برای مقابله با این چالش، تحقیقات رمزنگاری پس از کوانتومی با هدف توسعه الگوریتم‌های رمزگذاری مقاوم در برابر حملات رایانه‌های کوانتومی است. اینها شامل طرح های رمزگذاری مبتنی بر شبکه، مبتنی بر کد و چند متغیره است. علاوه بر این، روش‌های رمزگذاری مدرن شامل اجزای مهمی مانند مدیریت کلید، گواهی‌های دیجیتال و پروتکل‌های ایمن هستند. مدیریت کلید شامل ذخیره سازی، مبادله و توزیع ایمن کلید برای اطمینان از صحت و محرمانه بودن کلیدها است. گواهی های دیجیتال برای تأیید هویت طرفین استفاده می شود و بخشی جدایی ناپذیر از ارتباطات ایمن است. پروتکل های امن، مانند امنیت لایه حمل و

[12] Message Digest Algorithm
[13] Cipher block chaining
[14] electronic codebook
[15] counter mode

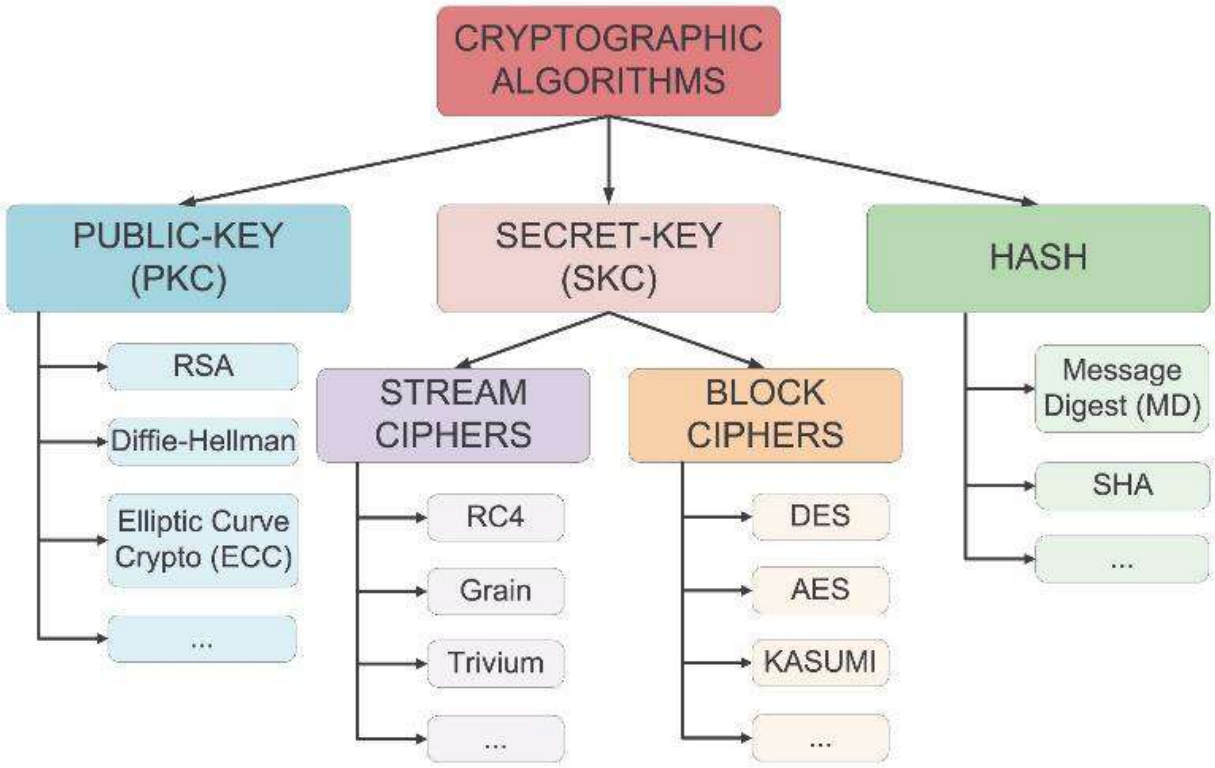
نقل[16] و پوسته ایمن[17]، کانال های ارتباطی رمزگذاری شده را در شبکه ها ارائه می دهند. در نتیجه، انواع روش‌های رمزگذاری مدرن نقش مهمی در تضمین محرمانه بودن، یکپارچگی و صحت داده‌ها و ارتباطات در چشم‌انداز دیجیتال امروزی دارند. این روش‌ها از طریق رمزگذاری متقارن و نامتقارن، توابع هش، حالت‌های عملیاتی و تحقیقات رمزنگاری پس از کوانتومی، اطلاعات حساس را از دسترسی غیرمجاز محافظت می‌کنند و اعتماد را در تعاملات دیجیتالی ایجاد می‌کنند [۲۶].

تکنیک‌های مورد استفاده برای حفاظت از اطلاعات در رمزنگاری از اصول ریاضی و مجموعه‌ای از محاسبات مبتنی بر قاعده به‌عنوان الگوریتم‌هایی که پیام‌ها را به گونه‌ای تغییر می‌دهند که رمزگشایی آن‌ها را دشوار می‌کند، مشتق شده‌اند. این الگوریتم‌ها برای تولید کلیدهای رمزنگاری، امضای دیجیتالی اسناد، تأیید حریم خصوصی داده‌ها، مرور اینترنت و محافظت از تراکنش‌های مخفی مانند تراکنش‌های کارت اعتباری و کارت نقدی استفاده می‌شوند. در عصر کامپیوتر امروزی، رمزنگاری اغلب با فرآیند تبدیل متن ساده به متن رمزی مرتبط است، متنی که به گونه‌ای رمزگذاری شده است که فقط گیرنده متن می‌تواند آن را رمزگشایی کند، فرآیندی که به نام رمزگذاری شناخته می‌شود. رمزگشایی به فرآیند تبدیل متن رمز به متن ساده اشاره دارد. ویژگی های رمزنگاری به شرح زیر است [۲۸]:

- ✓ محرمانه بودن: فقط فردی که اطلاعات برای او در نظر گرفته شده است به آن دسترسی دارد و هیچ کس دیگری به آن دسترسی ندارد.
- ✓ یکپارچگی: اطلاعات را نمی توان در ذخیره سازی یا انتقال بین فرستنده و گیرنده مورد نظر بدون توجه به آن تغییر داد.
- ✓ عدم انکار: خالق/فرستنده اطلاعات نمی تواند قصد خود را برای ارسال اطلاعات در مرحله بعدی انکار کند.
- ✓ احراز هویت: هویت فرستنده و گیرنده تأیید شده است. مقصد/منشا اطلاعات نیز تایید شده است.

رمزنگاری به طور کلی به سه دسته طبقه‌بندی می‌شود: رمزنگاری کلید متقارن (رمزنگاری کلید مخفی)، رمزنگاری کلید نامتقارن (رمزنگاری کلید عمومی) و توابع هش[18]. شکل ۵ انواع روش های اصلی رمزنگاری را نشان می دهد.

[16] Transport Layer Security
[17] Secure Shell
[18] Hash Function



شکل ۵. انواع روش های اصلی رمزنگاری [۲۹].

۵. انواع رویکردهای رمزنگاری

۵،۱ رمزنگاری متقارن

رمزگذاری متقارن روشی رایج است که در زمینه رمزنگاری برای حفظ محرمانه بودن و یکپارچگی داده ها استفاده می شود. این تکنیکی است که در آن از یک کلید رمزنگاری برای هر دو فرآیند رمزگذاری و رمزگشایی استفاده می شود. این بدان معناست که فرستنده و گیرنده باید از قبل کلید یکسانی را به اشتراک بگذارند. در رمزگذاری متقارن، پیام متنی ساده با استفاده از کلید مشترک در متن رمزگذاری شده رمزگذاری می شود. این فرآیند شامل استفاده از الگوریتم‌های پیچیده ریاضی برای تنظیم مجدد و دستکاری بیت‌های متن ساده می‌شود و آن را برای هر کسی که کلید را در اختیار ندارد نامفهوم می‌کند. هنگامی که متن رمزی تولید می شود، می توان آن را به طور ایمن از طریق کانال های ارتباطی ناامن و بدون خطر دسترسی غیرمجاز منتقل کرد. در انتهای گیرنده، گیرنده از همان کلید برای رمزگشایی متن رمز و بازگرداندن آن به شکل اصلی خود به عنوان متن ساده استفاده می کند. فرآیند رمزگشایی شامل اعمال معکوس الگوریتم رمزگذاری به متن رمز شده، با استفاده از کلید مشترک برای بازیابی پیام اصلی است. یکی از مزایای کلیدی رمزگذاری متقارن سرعت و کارایی آن است. از آنجایی که هم رمزگذاری و هم رمزگشایی از یک کلید استفاده می کنند، در مقایسه با الگوریتم های رمزگذاری نامتقارن، به توان محاسباتی کمتری نیاز دارد. این آن را برای ایمن سازی ارتباطات بلادرنگ، مانند پیام رسانی فوری یا کنفرانس ویدیویی، که در آن رمزگذاری و رمزگشایی سریع ضروری است، ایده آل می کند. با این حال، یکی از محدودیت‌های اصلی رمزگذاری متقارن، توزیع امن کلید بین طرف‌های ارتباطی است. اگر کلید به خطر بیفتد یا به دست اشتباه بیفتد، می تواند منجر به دسترسی غیرمجاز به داده های رمزگذاری شده شود. بنابراین، مکانیزم تبادل کلید ایمن مانند پروتکل های توزیع کلید امن یا کلیدهای

از پیش مشترک برای حفظ امنیت ارتباطات رمزگذاری شده بسیار مهم است. چالش دیگر با رمزگذاری متقارن، مقیاس پذیری زمانی است که چندین طرف نیاز به برقراری ارتباط امن دارند. با توجه به اینکه هر جفت کاربر به یک کلید منحصر به فرد نیاز دارد، با افزایش تصاعدی تعداد کاربران، مدیریت کلید پیچیده می شود. برای غلبه بر این محدودیت، می توان از طرح های رمزگذاری ترکیبی استفاده کرد، که در آن ترکیبی از رمزگذاری متقارن و نامتقارن استفاده می شود.

به طور خلاصه، رمزگذاری متقارن یک تکنیک رمزگذاری پرکاربرد است که حفاظت سریع و کارآمد داده ها را فراهم می کند. این امکان برقراری ارتباط امن را با استفاده از یک کلید برای هر دو فرآیند رمزگذاری و رمزگشایی فراهم می کند. در حالی که دارای محدودیت هایی مانند توزیع کلید و مقیاس پذیری است، رمزگذاری متقارن بخشی جدایی ناپذیر از رمزنگاری مدرن باقی می ماند و در برنامه های مختلف از جمله پیام رسانی امن، ذخیره سازی داده ها و شبکه های خصوصی مجازی استفاده می شود. به عبارتی دیگر، رمزنگاری متقارن در دسته طرح های رمزنگاری قرار می گیرد که در آن از یک کلید مشترک برای تبدیل متن ساده به متن رمزی استفاده می شود. یک کلید مخفی یکسان توسط فرستنده و گیرنده مشترک است. در زیر طرح های رمزنگاری متقارن آمده است.

- ✓ استاندارد رمزگذاری داده:

استاندارد رمزگذاری داده یک الگوریتم رمزنگاری متقارن است که برای رمزگذاری و رمزگشایی پیام استفاده می شود [۱۲]. در این مدل، تنها یک کلید مخفی هم برای رمزگذاری و هم برای رمزگشایی استفاده می شود. اندازه کلید استاندارد رمزگذاری داده ۵۶ بیتی است. برای انجام رمزگذاری/رمزگشایی، فرستنده و گیرنده باید کلید یکسانی داشته باشند. در این مدل، رمزگذاری را روی یک بلوک ۶۴ بیتی انجام می دهد [۸]. الگوریتم استاندارد رمزگذاری داده به طور گسترده در بسیاری از برنامه ها استفاده می شود [۱۶] و برخی از کاربردهای رایج در سیستم های نظامی، تجاری و امنیتی سیستم های ارتباطی می باشد [۱۴]. در مورد الگوریتم استاندارد رمزگذاری داده های سه گانه، ساز کلید ۱۶۸ بیتی استو سه بار روی هر بلوک داده عملیات انجام می دهد، در نتیجه این الگوریتم کندتر از استاندارد رمزگذاری داده است.

- ✓ استاندارد رمزگذاری پیشرفته:

این الگوریتم در سال ۱۹۹۷ توسط (موسسه ملی استاندارد و فناوری) معرفی شد. اساسا، استاندارد رمزگذاری پیشرفته بر اساس رمز ریجیندائل[19] ساخته شده توسط دو رمزنگار، جوآن دائمون[20] و وینست ریجمان[21]، می باشد. این الگوریتم متفاوت از دو نوع قبلی می باشد که دلیل آن اندازه کلیدهای متغیر مانند ۱۲۸، ۱۹۲ و ۲۵۶ بیت است [۱۶]. همانند دو مدل قبلی، استاندارد رمزگذاری پیشرفته نیز روی بلوک هایی که ۱۲۸ بیتی هستند رمزگذاری را انجام می دهد [۸]. الگوریتم استاندارد رمزگذاری پیشرفته در دستگاه های کوچک برای رمزگذاری پیام برای ارسال از طریق شبکه استفاده می شود. برخی از برنامه های کاربردی این الگوریتم تراکنش های پولی [۱۸] و برنامه های امنیتی [۳۰] هستند.

۵،۲. رمزنگاری نامتقارن

[19] Rijndael
[20] Joan Daemen
[21] Vincent Rijmen

رمزگذاری که به نام رمزنگاری کلید عمومی نیز شناخته می‌شود، یک الگوریتم رمزنگاری است که از یک جفت کلید – یک کلید عمومی و یک کلید خصوصی – برای برقراری ارتباط امن در شبکه‌های ناامن مانند اینترنت استفاده می‌کند. این یک روش امن برای رمزگذاری و رمزگشایی داده ها، اطمینان از محرمانه بودن، یکپارچگی و اعتبار ارائه می کند. در رمزگذاری نامتقارن، هر کاربر دارای یک جفت کلید منحصر به فرد است: یک کلید عمومی و یک کلید خصوصی. کلید عمومی را می توان آزادانه برای هر کسی توزیع کرد، در حالی که کلید خصوصی باید مخفی نگه داشته شود و به طور ایمن توسط مالک نگهداری شود. این کلیدها از نظر ریاضی مرتبط هستند اما از نظر محاسباتی برای استخراج یک کلید از کلید دیگر غیر ممکن است. کلید عمومی برای رمزگذاری استفاده می شود، در حالی که کلید خصوصی برای رمزگشایی استفاده می شود. این تفاوت اساسی با رمزگذاری متقارن، که در آن هر دو طرف ارتباط کلید مخفی یکسانی را به اشتراک می گذارند، امنیت و انعطاف پذیری بیشتری را در رمزگذاری نامتقارن فراهم می کند. هنگامی که یک فرستنده می خواهد یک پیام محرمانه برای گیرنده ارسال کند، از کلید عمومی گیرنده برای رمزگذاری داده ها استفاده می کند. متن رمزی حاصل از این فرآیند رمزگذاری فقط می تواند توسط گیرنده با استفاده از کلید خصوصی خود رمزگشایی شود.

از آنجایی که کلید خصوصی فقط برای گیرنده شناخته شده است، محرمانه بودن پیام حفظ می شود. علاوه بر محرمانه بودن، رمزگذاری نامتقارن همچنین امکان احراز هویت و یکپارچگی داده ها را فراهم می کند. به عنوان مثال، امضاهای دیجیتالی را می توان با استفاده از کلید خصوصی فرستنده تولید کرد، که سپس توسط هر کسی که به کلید عمومی مربوطه فرستنده دسترسی دارد، تأیید می شود. این فرآیند تأیید تضمین می کند که پیام در حین انتقال دستکاری نشده است و صحت فرستنده را تأیید می کند. رمزگذاری نامتقارن به طور گسترده در برنامه های کاربردی مختلف از جمله ارتباطات ایمیل ایمن، انتقال امن فایل، مرور امن وب و تراکنش های آنلاین امن استفاده می شود. این ابزاری امن برای تبادل اطلاعات حساس بین طرفین بدون نیاز به کلید مخفی از پیش مشترک فراهم می کند. علاوه بر این، مقیاس پذیری رمزگذاری نامتقارن امکان توزیع امن کلیدهای عمومی را فراهم می کند و ارتباط امن با چندین کاربر را تسهیل می کند. با این حال، رمزگذاری نامتقارن از نظر محاسباتی در مقایسه با رمزگذاری متقارن گران‌تر است، و آن را برای رمزگذاری مقادیر زیادی داده مناسب‌تر می‌کند. بنابراین، معمولاً از الگوریتم‌های رمزگذاری نامتقارن برای ایجاد یک کانال امن و تبادل امن یک کلید متقارن مشترک استفاده می‌شود که سپس برای رمزگذاری و رمزگشایی داده‌ها با استفاده از یک الگوریتم رمزگذاری متقارن سریع‌تر استفاده می‌شود. الگوریتم‌های رمزگذاری نامتقارن رایج شامل آراس‌ای و رمزنگاری منحنی بیضی هستند که هر کدام سطوح مختلفی از امنیت و عملکرد را ارائه می‌دهند. به طور کلی، رمزگذاری نامتقارن نقش حیاتی در ایمن سازی ارتباطات دیجیتال و حفاظت از اطلاعات حساس در عصر دیجیتال ایفا می کند. به عبارتی دیگر، رمزنگاری نامتقارن نیز در دسته طرح های رمزنگاری قرار می گیرد. برخلاف رمزنگاری متقارن، از دو کلید استفاده می‌شود: یکی عمومی و دیگری خصوصی. کلید عمومی توسط هر کسی در سیستم رمزنگاری به اشتراک گذاشته می شود در حالی که کلید خصوصی توسط کاربر تأیید شده مخفی نگه داشته می شود. در زیر الگوریتم های رمزنگاری نامتقارن آمده است.

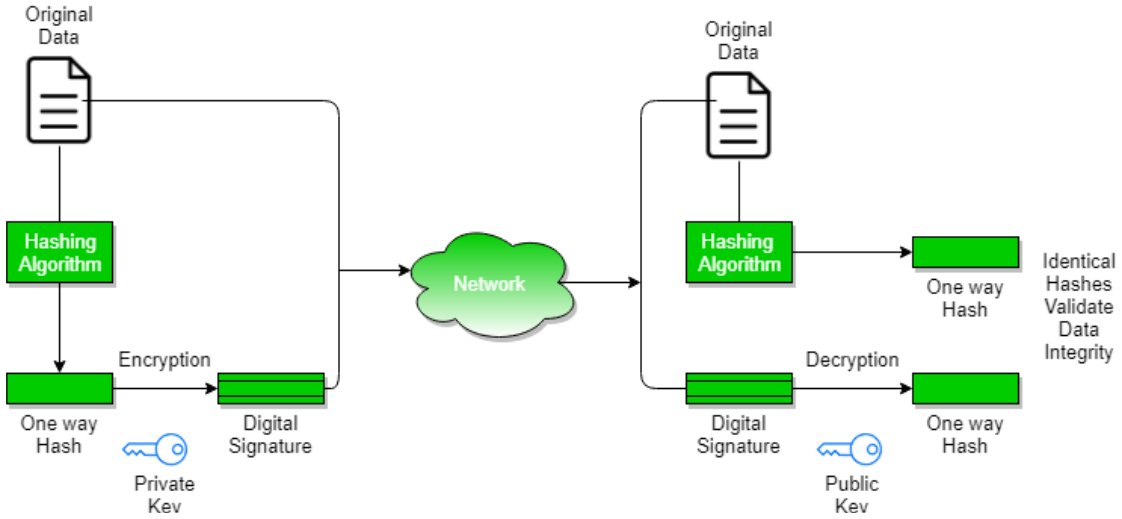
- ✓ آراس‌ای

آراس‌ای یک الگوریتم رمزنگاری نامتقارن است [۲] که برای رمزگذاری و رمزگشایی پیام نیز استفاده می شود. آراس‌ای به طور گسترده ای در انتقال کلیدها از طریق یک کانال ناامن استفاده می شود. به دلیل ماهیت نامتقارن، از دو کلید در الگوریتم استفاده شده است. یکی کلید عمومی و دومی کلید خصوصی. کلید عمومی به طور آشکار برای همه افراد در سیستم رمزنگاری قابل دسترسی است و کلید

خصوصی توسط شخص مجاز مخفی نگه داشته می شود. این الگوریتم محرمانه بودن، یکپارچگی، صحت و عدم انکار داده ها را فراهم می کند [۳۱]. همچنین، الگوریتم آراسِای بیشتر در صنعت الکترونیک برای انتقال پول آنلاین استفاده می شود [۳۲]. در آینده، آراسِای می تواند در کارت های جاوا استفاده شود [۳۳].

✓ الگامال

الگوریتم الگامال در سال ۱۹۸۵ توسط طاهر الگامال [۲۳] معرفی شد. این الگوریتم رمزگذاری کلید نامتقارن است که بر اساس تبادل کلید Diffie-Helman به عنوان جایگزینی برای آراسِای برای رمزگذاری کلید عمومی است. همچنین در الگوریتم تولید امضای دیجیتال به نام طرح امضای الگامال استفاده می شود [۳۴]. همچنین، یک الگوریتم هم شکل به نام پیلیئر برای امنیت معنایی آن استفاده می شود [۳]. به عنوان مثال، شکل ۶ نمایی از فرآیند امضا دیجیتال را نشان می دهد.



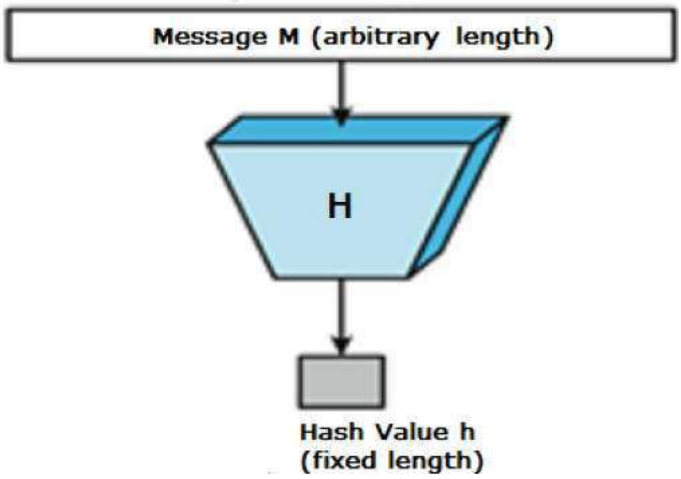
شکل ۶. نمایی از فرآیند امضا دیجیتال [۳۵].

✓ رمزنگاری منحنی بیضوی

رمزنگاری منحنی بیضوی در سال ۱۹۸۵ توسط نیل کوبلیتز و ویکتور اس میلر معرفی شد. این الگوریتم در دسته طرح نامتقارن قرار دارد که بر اساس منحنی های بیضوی است. کاربردهای رمزنگاری منحنی بیضوی عبارتند از رمزگذاری، امضای دیجیتال و تولیدکنندگان شبه تصادفی [۱۳].

۵/۳. تابع هش

توابع هش فوق العاده ارزشمند هستند و تقریباً در هر برنامه ای که با امنیت اطلاعات سروکار دارد یافت می شود. یک تابع هش یک مقدار ورودی عددی را به مقدار عددی فشرده دیگری تبدیل می کند. ورودی تابع هش دارای طول دلخواه است اما خروجی همیشه دارای طول ثابت است. خلاصه پیام، یا به سادگی مقادیر هش، نتایج یک الگوریتم هش هستند. تابع هش در نمودار زیر نشان داده شده است. شکل ۷ نمایی از تابع هش را نشان می دهد.



شکل ۷. تابع هش [۳۶].

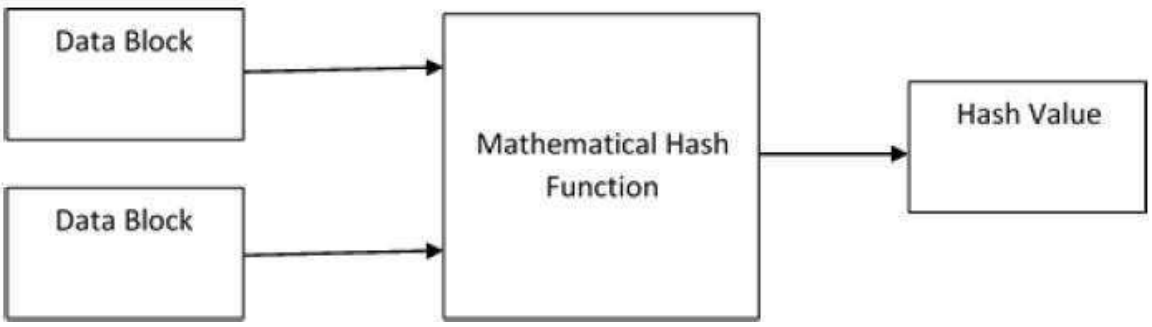
ویژه گی‌های تابع هش در زیر آورده شده است.

- ✓ خروجی طول ثابت (مقدار هش):

تابع هش داده های هر طولی را به طول ثابت تبدیل می کند. درهم کردن داده ها اصطلاحی است که برای توصیف این فرآیند استفاده می شود. تابع هش n بیتی یک تابع هش با خروجی n بیت است. توابع هش محبوب مقادیری از ۱۶۰ تا ۵۱۲ بیت را ارائه می دهند.

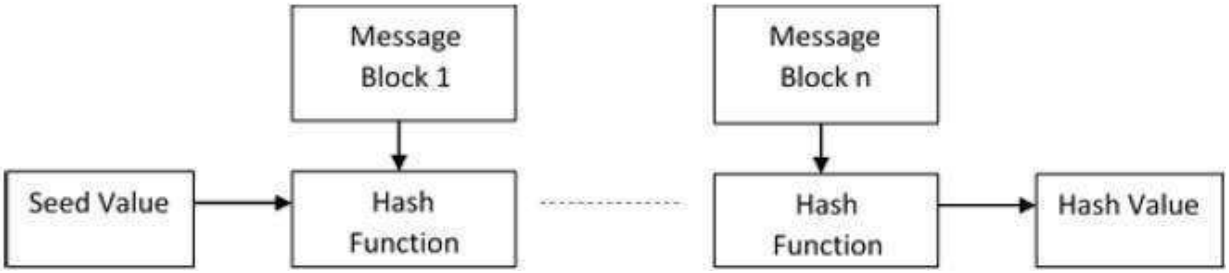
- ✓ عملکرد مناسب در اجرا:

به طور کلی، برای محاسبه h(x) برای هر تابع هش h با ورودی x یک روش سریع است. توابع هش از نظر محاسباتی بسیار سریعتر از رمزگذاری متقارن هستند. یک فرمول ریاضی که بر روی دو بلوک با اندازه ثابت از داده ها برای ایجاد یک کد هش عمل می کند، در پایه هش قرار دارد. بخشی از الگوریتم هش این تابع هش است. بسته به الگوریتم، اندازه هر بلوک داده تغییر می کند. اندازه بلوک معمولا بین ۱۲۸ تا ۵۱۲ بیت است. تابع هش در شکل ۸ نشان داده شده است.



شکل ۸. نمایی از عملیات تابع هش [۳۶].

مانند یک رمز بلوکی، الگوریتم هش از دور تابع هش بالا استفاده می کند. هر دور یک ورودی با اندازه ثابت را می پذیرد که معمولاً ترکیبی از بلوک پیام اخیر و خروجی دور قبلی است. این روش به تعداد دفعات لازم برای هش کردن کل پیام انجام می شود. شکل ۹ شماتیک الگوریتم هش را نشان می دهد.



شکل ۹. شماتیکی از الگوریتم هش [۳۶].

در نتیجه، مقدار هش بلوک پیام اول به ورودی عملیات هش دوم تبدیل می شود که خروجی آن نتیجه عملیات سوم و غیره را تغییر می دهد. این به عنوان اثر بهمن هش شناخته می شود. هنگامی که دو پیام حتی با یک بیت داده متفاوت هستند، اثر بهمنی منجر به تفاوت قابل توجهی در مقادیر هش می شود.

نتیجه گیری

تحلیل تطبیقی تکنیک‌های رمزنگاری مدرن، جنبه‌های مختلف الگوریتم‌های رمزنگاری را که معمولاً برای ایمن کردن اطلاعات حساس استفاده می‌شوند را روشن کرده است. از طریق این تجزیه و تحلیل، مشخص شده است که هیچ راه حل یکسانی برای رمزنگاری وجود ندارد، زیرا هر تکنیک دارای نقاط قوت و ضعف خاص خود است. یافته‌های این مطالعه اهمیت در نظر گرفتن عواملی مانند پیچیدگی محاسباتی، کارایی، طول کلید و مقاومت در برابر حملات را هنگام انتخاب یک الگوریتم رمزنگاری مناسب نشان می‌دهد. تکنیک هایی مانند رمزنگاری کلید متقارن، رمزنگاری کلید نامتقارن، و توابع هش به طور گسترده مورد بررسی و مقایسه قرار گرفته اند و درک جامعی از ویژگی ها و کاربرد آنها در سناریوهای مختلف ارائه می دهند. علاوه بر این، پیشرفت‌ها در محاسبات کوانتومی و تهدیدات نوظهور بر نیاز به تکنیک‌های رمزنگاری قوی‌تر تاکید کرده‌اند. تجزیه و تحلیل نشان داده است که تکنیک‌هایی مانند رمزنگاری پس کوانتومی و رمزگذاری هوموروفیک راه‌حل‌های امیدوارکننده‌ای را برای چالش‌های احتمالی ناشی از رایانه‌های کوانتومی ارائه می‌دهند. به طور کلی، این تجزیه و تحلیل مقایسه ای به عنوان یک منبع ارزشمند برای متخصصان امنیتی، محققان و توسعه دهندگان عمل می کند و آنها را در تصمیم گیری آگاهانه در مورد اجرای تکنیک های رمزنگاری راهنمایی می کند. همانطور که تکنولوژی به تکامل خود ادامه می دهد، حوزه رمزنگاری نیز باید برای اطمینان از محرمانه بودن و یکپارچگی اطلاعات حساس، سازگار و تکامل یابد. با به‌روز ماندن با آخرین پیشرفت‌ها در تکنیک‌های رمزنگاری مدرن، جامعه امنیتی می‌تواند به حفاظت از داده‌ها و محافظت در برابر تهدیدات نوظهور در دنیایی که به طور فزاینده‌ای به هم پیوسته است، ادامه دهد.

مراجع

.١ Chauhan, J.S. and S. Sharma, *A comparative study of cryptographic algorithms.* Int. J. Innov. Res, 2015: p. 24-28.

.٢ Al Hasib, A. and A.A.M.M. Haque. *A comparative study of the performance and security issues of AES and RSA cryptography*. in *2008 third international conference on convergence and hybrid information technology*. 2008. IEEE.

.٣ Farah, S., et al. *An experimental study on performance evaluation of asymmetric encryption algorithms*. in *Recent Advances in Information Science, Proceeding of the 3rd European Conf. of Computer Science,(EECS-12)*. 2012.

.٤ Upadhyaya, S., *Secure communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks.* Procedia Computer Science, 2015. **70**: p. 808-813.

.٥ Patil, A. and R .Goudar, *A comparative survey of symmetric encryption techniques for wireless devices.* International journal of scientific & technology research, 2013. **2**.(٨)

.٦ Bresson, E., O. Chevassut, and D. Pointcheval. *Security proofs for an efficient password-based key exchange*. in *Proceedings of the 10th ACM conference on Computer and communications security*. 2003.

.٧ Levi, A. and E. Savas. *Performance evaluation of public-key cryptosystem operations in WTLS protocol*. in *Proceedings of the eighth IEEE symposium on computers and communications. ISCC 2003*. 2003. IEEE.

.٨ Shetty, A., K. Shravya, and K. Krithika, *A review on asymmetric cryptography RSA and ElGamal algorithm.* International Journal of Innovative Research in Computer and Communication Engineering, 2014. **2** :(٥)p. 98-105.

.٩ Elminaam, D.S.A., H.M.A. Kader, and M.M. Hadhoud, *Performance evaluation of symmetric encryption algorithms.* IJCSNS International Journal of Computer Science and Network Security, 2008. **8**(12): p. 280-286.

.١٠ Dongjiang, L., W. Yandan, and C. Hong. *The research on key generation in RSA public-key cryptosystem*. in *2012 Fourth international conference on computational and information sciences*. 2012. IEEE.

.١١ Mathur, H. and Z. Alam, *Analysis in symmetric and asymmetric cryptology algorithm* . International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2015. **4**.(١)

.١٢ Sukhija, D., *Performance Evaluation of Cryptographic Algorithms: AES and DES.* vol, 2014. **3**: p. 582-585.

.١٣ Rathod, R.H. and C. Dhote, *Comparison of symmetric key encryption algorithms.* International Journal of Research in Information Technology (IJRIT), 2014.

.١٤ Tripathi, R. and S. Agrawal, *Comparative study of symmetric and asymmetric cryptography techniques.* International Journal of Advance Foundation and Research in Computer (IJAFRC), 2014. **1**(6): p. 68-76.

.١٥ Verma, O.P., et al. *Notice of Violation of IEEE Publication Principles: Peformance analysis of data encryption algorithms*. in *2011 3rd International Conference on Electronics Computer Technology*. 2011. IEEE.

.١٦ Jeeva, A., D.V. Palanisamy, and K. Kanagaram, *Comparative analysis of performance efficiency and security measures of some encryption algorithms.* International Journal of Engineering Research and Applications (IJERA), 2012. **2**(3): p. 30.٣٠٣٧-٣٣

.١٧ Arora, P., A. Singh, and H. Tyagi, *Evaluation and comparison of security issues on cloud computing environment.* World of Computer Science and Information Technology Journal (WCSIT), 2012. **2**(5): p. 179-183.

.١٨ Mittal, M., *Performance evaluation of cryptographic algorithms.* International Journal of Computer Applications, 2012. **41**.(٧)

.١٩ Masram, R., et al., *Analysis and comparison of symmetric key cryptographic algorithms based on various file features.* International Journal of Network Security & Its Applications, 2014. **6**(4): p. 43.

.٢٠ Kansal, S. and M. Mittal. *Performance evaluation of various symmetric encryption algorithms*. in *2014 international conference on parallel, distributed and grid computing*. 2014. IEEE.

.٢١ Soni, S., H. Agrawal, and M. Sharma, *Analysis and comparison between AES and DES Cryptographic Algorithm.* International Journal of Engineering and Innovative Technology (IJEIT), 2012. **2**(6): p. 362-365.

.٢٢ Maqsood, F., et al., *Cryptography: A comparative analysis for modern techniques.* International Journal of Advanced Computer Science and Applications, 2017. **8**.(٦)

.٢٣ Nalwaya, P., V.P. Saxena, and P. Nalwaya. *A cryptographic approach based on integrating running key in feedback mode of elgamal system*. in *2014 International Conference on Computational Intelligence and Communication Networks*. 2014. IEEE.

.٢٤ Vijayalakshmi, P. and K.B. Raja. *Performance analysis of RSA and ECC in identity-based authenticated new multiparty key agreement protocol*. in *2012 International Conference on Computing, Communication and Applications*. 2012. IEEE.

.٢٥ Aman, K., J. Sudesh, and M. Sunil, *Comparative Analysis between DES and RSA Algorithm.* International Journal of Advanced Research in Computer Science and Software Engineering, 2012. **2**(7): p. 38.٣٩١-٦

.٢٦ Banoth, R. and R. Regar, *Mathematical Foundation for Classical and Modern Cryptography*, in *Classical and Modern Cryptography for Beginners*. 2023, Springer. p. 85-108.

.٢٧ Ullah, S., et al., *Elliptic Curve Cryptography; Applications, challenges ,recent advances, and future trends: A comprehensive survey.* Computer Science Review, 2023. **47**: p. 100530.

.٢٨ Al-Amri, R.M., D.N. Hamood, and A.K. Farhan, *Theoretical Background of Cryptography.* Mesopotamian Journal of CyberSecurity, 2023. **2023**: p. 7-15.

.٢٩ Pal, S., B. Datta, and A. Karmakar, *An Artificial Neural Network Technique of Modern Cryptography.* Journal of Scientific Research, 2022. **14**.(٢)

.٣٠ Sterbenz, A. and P. Lipp. *Performance of the AES Candidate Algorithms in Java*. in *AES Candidate Conference*. 2000. Citeseer.

.٣١ Alanazi, H., et al., *New comparative study between DES, 3DES and AES within nine factors.* arXiv preprint arXiv:1003.4085, 2010.

.٣٢ Alqadi, Z., *Improving Standard Methods of Message Cryptography.* 2022.

.٣٣ Bernabé, G. and N. Clarke, *Study of RSA Performance in Java Cards.* Advances in Communications, Computing, Networks and Security Volume 10, 2013: p. 45.

.٣٤ Li, X., X. Shen, and H. Chen, *Elgamal digital signature algorithm of adding a random number.* Journal of Networks, 2011. **6** :(٥)p. 774.

.٣٥ Wellem, T., Y. Nataliani, and A. Iriani, *Academic Document Authentication using Elliptic Curve Digital Signature Algorithm and QR Code.* JOIV: International Journal on Informatics Visualization, 2022. **6**(3): p. 667-675.

.٣٦ Qian, Y., F. Ye ,and H.-H. Chen, *Cryptographic Techniques.* 2022.