به نام خدا

کاربردهای سیستم رمز AES

گردآورندگان: فاطمه حسینی، مرضیه روشنی

استاد: دکتر حسن خدایی مهر

نیمسال دوم ۱۴۰۱-۱۴۰۰

فهرست مطالب

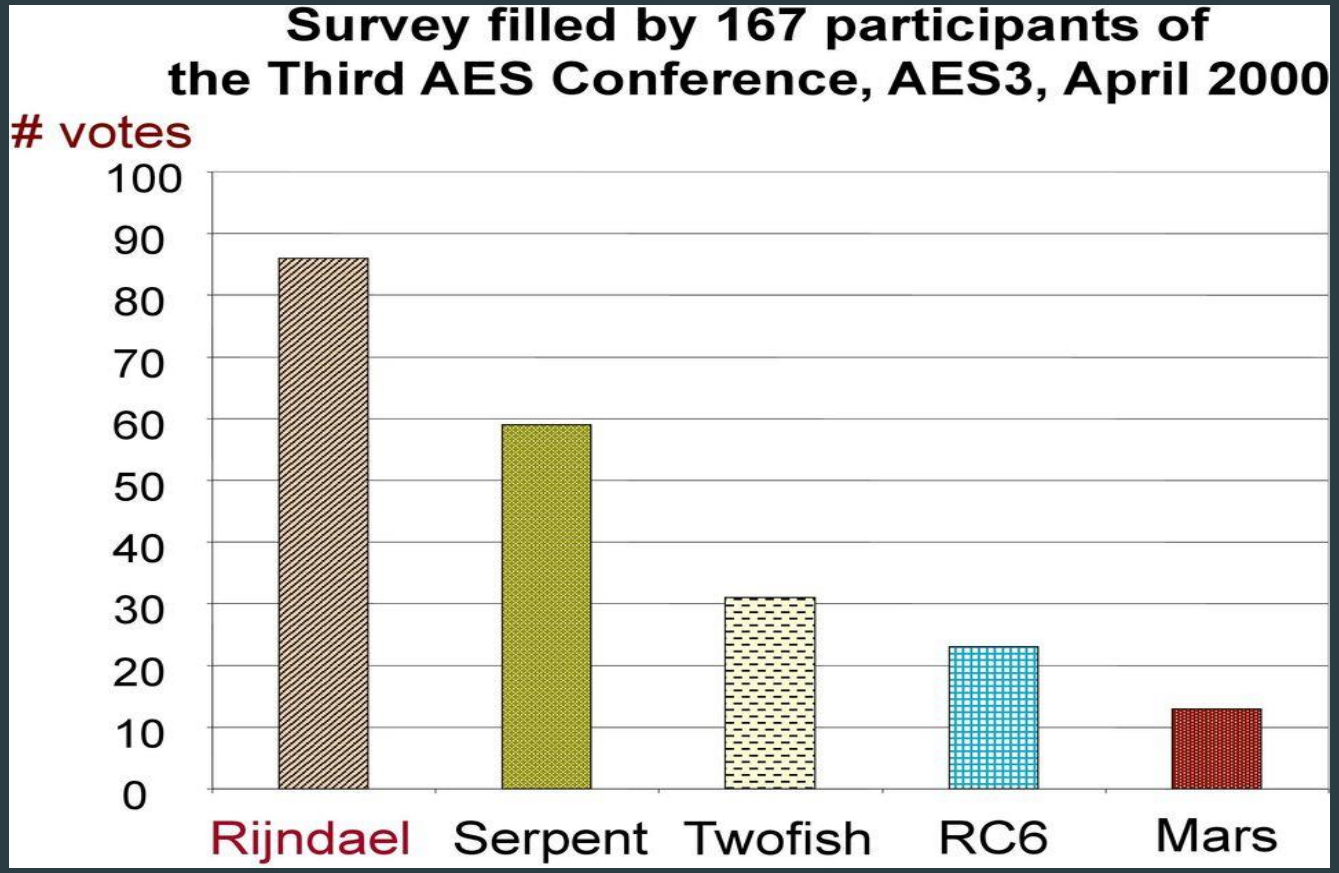
مقدمه

موسسه ملی استانداردها و تکنولوژی امریکا موسوم به NIST در دهه ۷۰ میلادی استاندارد DES را به عنوان راهکار رسمی سازمان‌های دولتی این کشور برای رمزنگاری داده‌ها معرفی نمود. این استاندارد از یک الگوریتم رمزنگاری متقارن با کلیدی به طول ۵۶ بیت بهره می‌گرفت. پیشرفت تدریجی توان پردازشی کامپیوترها و طول نسبتا کوتاه کلید رمزنگاری DES آسیب‌پذیری این استاندارد را در مقابل حملات مختلف به دنبال داشت. بنابراین انتخاب جایگزینی مناسب برای استاندارد DES در دستور کار موسسه NIST قرار گرفت. برای این منظور این موسسه با انتشار بیانیه‌ای عمومی اعلام نمود که فرآیند انتخاب الگوریتم رمزنگاری آینده دولت فدرال امریکا با کمک متخصصین رمزنگاری از سرتاسر جهان انجام خواهد شد.

در بیانیه تاکید شده بود که این الگوریتم بایستی دارای مشخصه های زیر باشد:

- امنیت: قدرت امنیتی الگوریتم‌ها به عنوان مهم‌ترین فاکتور در این رقابت مورد بررسی قرار گرفت. برای این منظور توانایی مقاومت هر الگوریتم در برابر حملات مختلف، با دیگر الگوریتم‌های شرکت‌کننده مقایسه گردید.
- کارایی: الگوریتم‌های کاندید شده از نظر بهینگی در مصرف توان محاسباتی و فضای حافظه مورد ارزیابی قرار گرفتند.
- هزینه: الگوریتم برگزیده در این رقابت با کسب عنوان AES به صورت غیر انحصاری، بدون حق امتیاز و کاملا رایگان در سطح جهانی عرضه می گردد.
- پیاده‌سازی راحت در سطح نرم‌افزار و سخت‌افزار
- انجام عملیات رمزنگاری با کلید متقارن و به صورت بلوکه‌ای: شرایط مورد نظر NIST برای الگوریتم AES آن بود که قادر باشد داده‌ها را در قالب بلوک هایی ۱۲۸ بیتی و با استفاده از کلیدهای ۱۲۸، ۱۹۲ و ۲۵۶ بیتی رمزنگاری نماید.

در نهایت از بین پنج فینالیست، سیستم رمزی که توسط Rijmen و Daemen طراحی شده بود، به عنوان رمز استاندارد پیشرفته انتخاب و نام AES (**Advanced Encryption Standard**) بر آن نهاده شد.



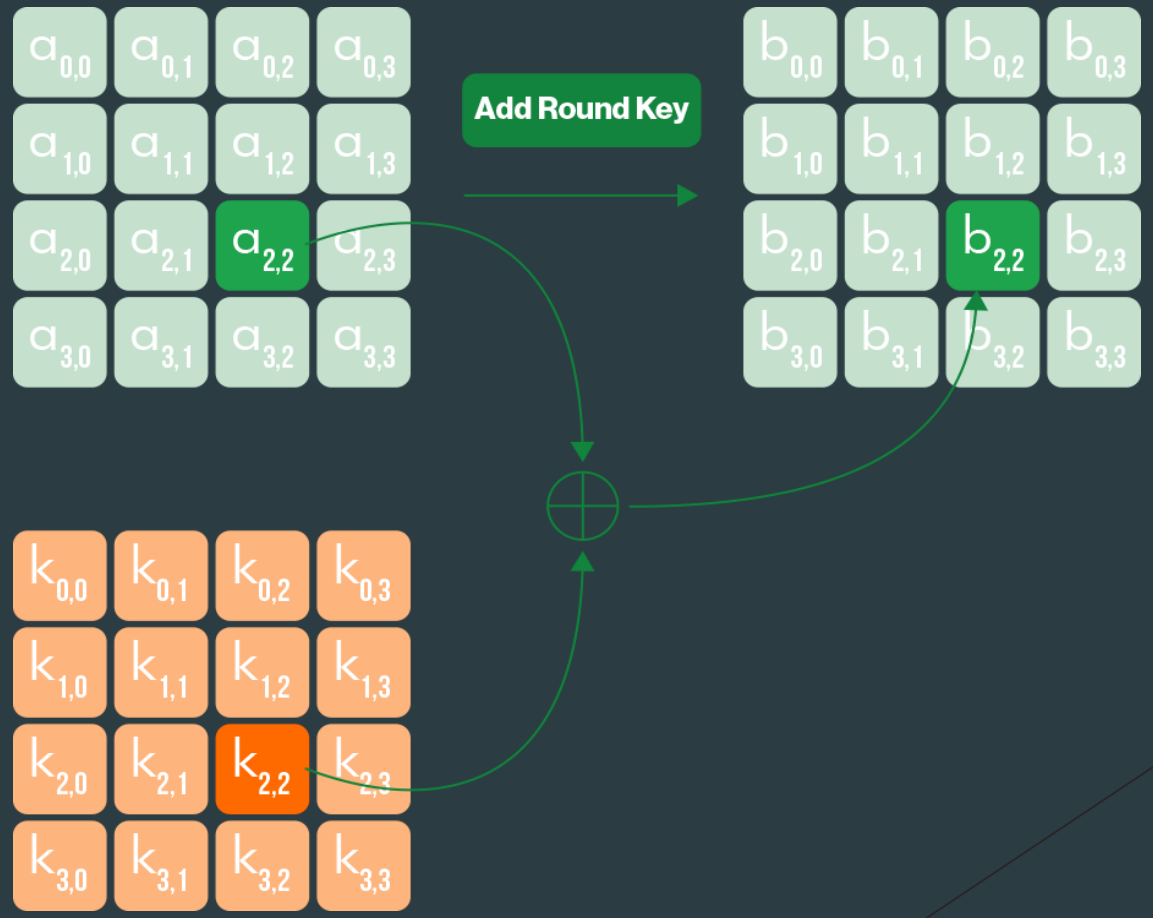
how does AES encryption work?

AES is a block cipher that encrypts and decrypts data in blocks of 128 bits using 128-bit, 192-bit, or 256-bit keys. The same key is used for encrypting and decrypting data. AES using a 128-bit key is often referred to as AES-128, etc. Data is encrypted using multiple **rounds**, each of which consists of a series of mathematical operations. The process starts with using Rijndael's key schedule algorithm to derive a series of new **round keys** from the original **secret key**. This is known as **key expansion**.

Each round then consists of one or more (or a combination) of the following operations:

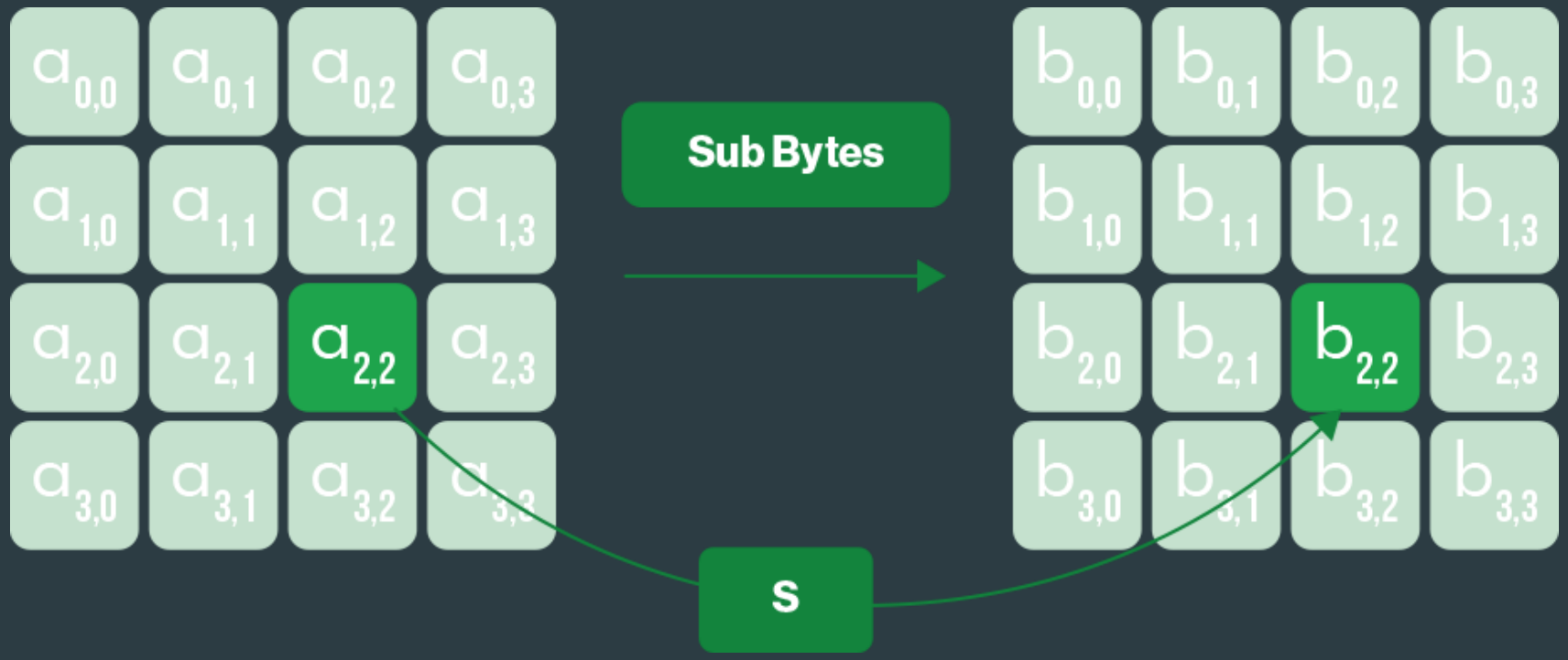
1. AddRoundKey

An XOR operation is performed to combine the data to be encrypted (the **cipher text**) with each round key.



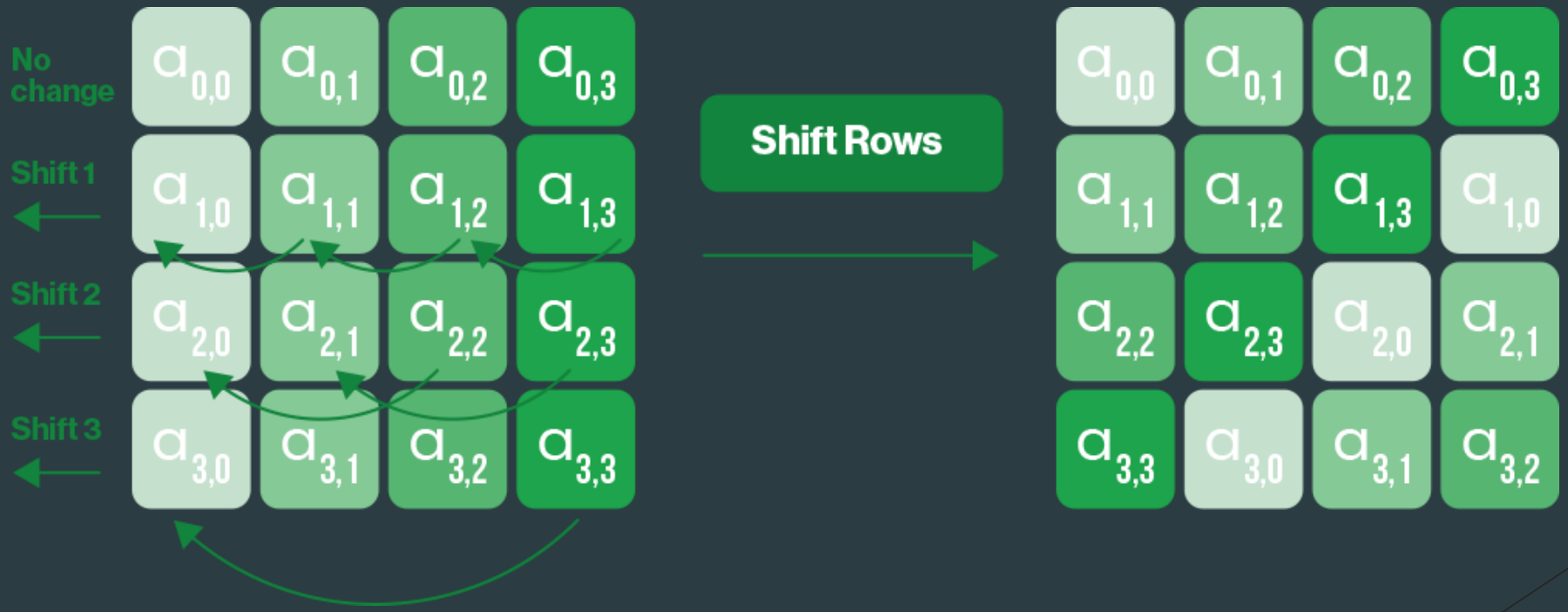
2. SubBytes

A substitution table is used to further mix up the data.



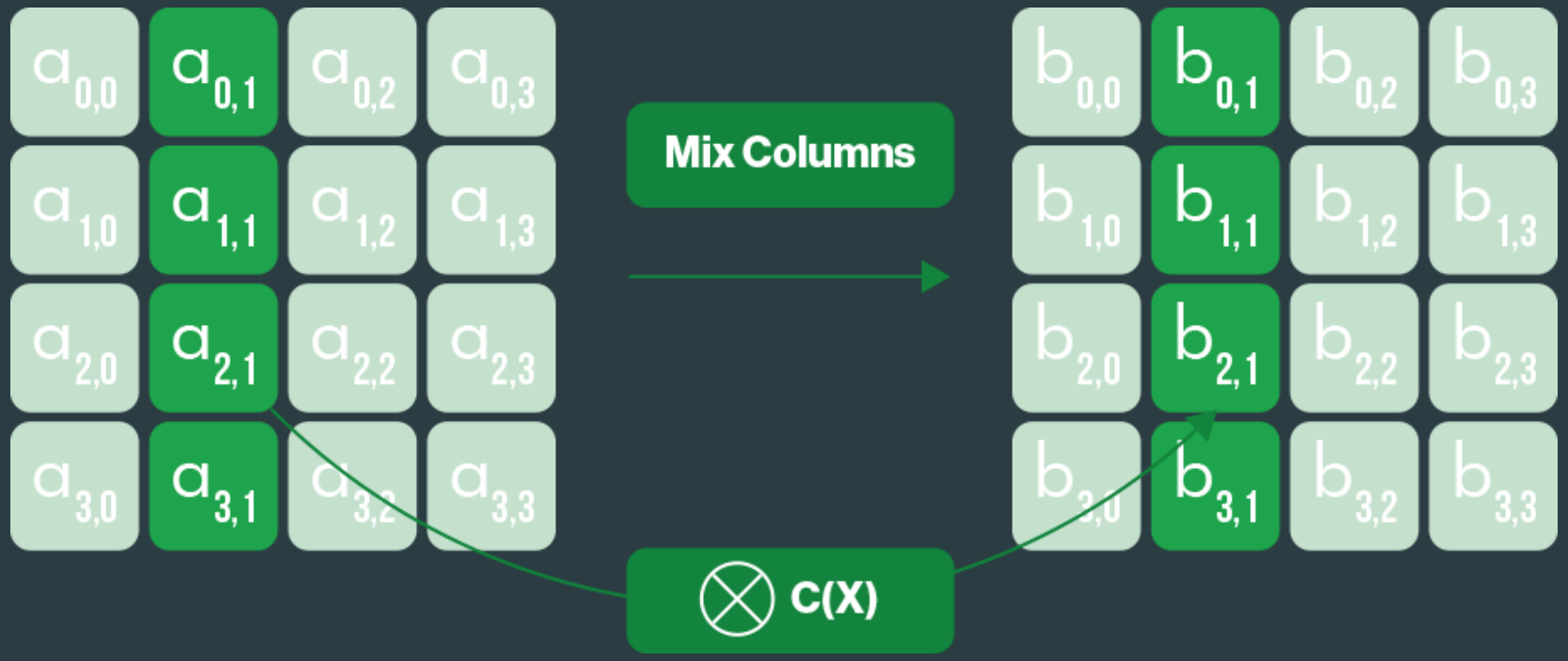
3. ShiftRows

Each 128-block of data consists of a 16-bit 4×4 block. This operation shifts each byte in a block row by a certain offset to the left.



4. MixColumns

An additional invertible linear transformation is performed on each column in the block.



This series of transformations constitutes one round, which is then repeated on the data a set number of times. The number of rounds used depends on the key size:

- AES-128 — 10 rounds
- AES-192 — 12 rounds
- AES-256 — 14 rounds

ساده ترین حمله ممکن به هر سیستم رمزی، حمله جستجوی جامع(brute force) است. در این حمله تمام ترکیب های ممکن کلید آزمایش می شود تا کلید واقعی و درست پیدا شود.

Fugaku که امروزه قدرتمندترین ابرکامپیوتر در جهان است، برای اعمال حمله جستجوی جامع روی AES-128 به ۱۲ تریلیون سال نیاز دارد.

انجام حمله جستجوی جامع روی AES-256، ۳۴۰×۱۰^{۳۶} بار سخت تر از شکستن رمز AES-128 است!

بنابراین می توان گفت که این سیستم رمزنگاری در برابر حمله آزمون جامع بسیار مقاوم است.

امنیت AES است که آن را تبدیل به یک سیستم رمزگذاری پرکاربرد کرده است.

اگرچه AES توسط موسسه استاندارد و فناوری آمریکا برای به‌کارگیری به عنوان الگوریتم رسمی رمزنگاری اسناد محرمانه دولتی آن کشور استانداردسازی گردید، اما از همان ابتدا به عنوان یک الگوریتم غیرانحصاری در اختیار عموم قرار دارد.

امنیت و کارایی مناسب در کنار مقبولیت گسترده آن در میان متخصصین رمزنگاری موجب شده است تا بسیاری از سازمان‌های دولتی، نهادهای امنیتی و نظامی، شرکت‌های خصوصی و کاربران عادی در سرتاسر دنیا از استاندارد AES برای رمزنگاری داده‌های حساس و محرمانه خود بهره گیرند.

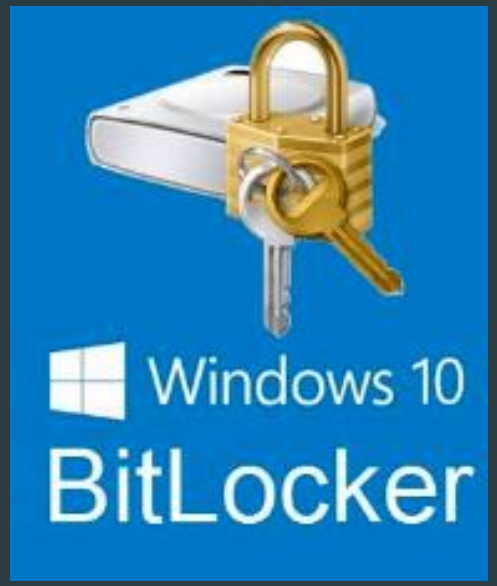
امروزه کاربران عادی می‌توانند به راحتی از طریق وب به ابزارهای رمزنگاری AES دسترسی پیدا کنند، به عنوان مثال در وب سایت AES Encryption می‌توانند با وارد کردن متن پیام و کلید رمزنگاری دلخواه خود در جعبه‌های متنی مربوطه، طول کلید رمزنگاری را مشخص نموده و با کلیک روی یک دکمه اقدام به رمزگذاری یا رمزگشایی پیام مورد نظر نمایند. بدون شک این نوع رمزنگاری از طریق یک رابط تحت وب، راهکار امن و مطلوبی برای سازمان‌های دولتی و شرکت‌های تجاری نبوده و آن‌ها به طور معمول ابزار رمزنگاری مورد نیاز خود را به صورت داخلی بر مبنای استاندارد AES پیاده‌سازی می‌نمایند.

کاربرد های سیستم رمز AES

AES در گستره وسیعی از نرم افزارها، سخت افزارها و سیستم های عامل مورد استفاده قرار می گیرد.

- معمول ترین کاربرد AES در Wi-Fi به ویژه WPA2-PSK (AES) است.
- در بسیاری از زبان های برنامه نویسی مانند Crypto++ ، Java، Python، C++، C و حتی Facebook به کار گرفته می شود.
- اپلیکیشن های تلفن همراه مثل WhatsApp
- پیاده سازی VPN
- پشتیبانی از پردازنده های بومی
- انتقال امن فایل ها و پیام های کاربران در بستر اینترنت

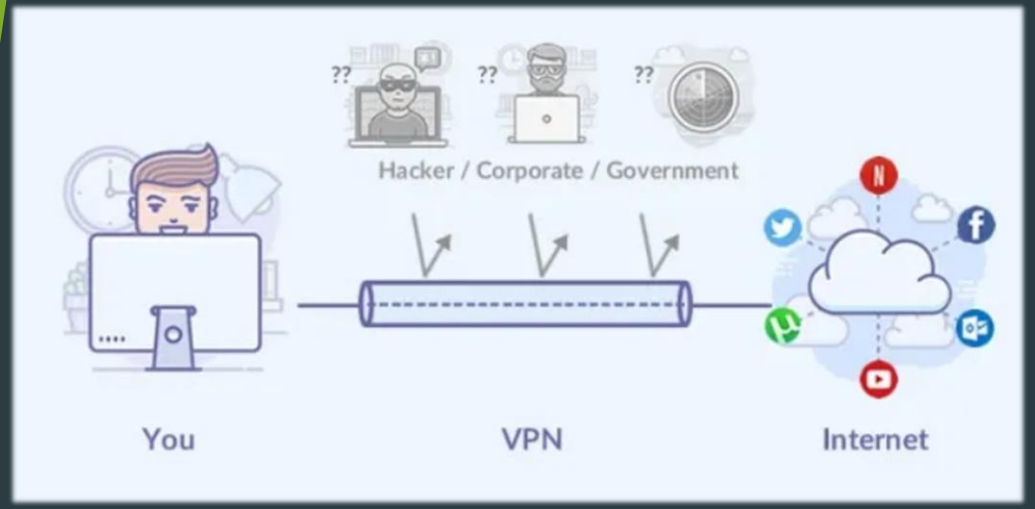
- فشرده سازی فایل ها (7 Zip, WinZip, RAR)
- بازی های ویدئویی مانند *Grand Theft Auto IV*
- سیستم رمز گذاری دیسک مانند BitLocker
- اپلیکیشن های بانکی



پیاده سازی VPN

به محض اینکه کاربر به اینترنت متصل می شود، ترافیک داده اش از ISP (Internet service provider) عبور می کند. برای دسترسی به یک وبسایت، باید یک درخواست به ISP داده شود که افراد را به مقصدشان هدایت کند. در نتیجه تمام فعالیت های آنلاین کاربران برای ISP آشکار میشود. هیچ سدّی نمی تواند مانع جمع آوری فعالیت های آنلاین کاربران توسط ISP شود. ISP میتواند اطلاعات کاربران را به تبلیغ کنندگان بفروشد یا آن را به مسئولین منتقل کند، حتی اگر ISP قابل اعتماد باشد، ممکن است که حکومت آن را مجبور کند که تاریخچه جستجوهای کاربر را به حکومت بدهد.

استفاده از VPN میتواند از تمام این اتفاقات جلوگیری میکند.



پیاده سازی VPN

VPN حضور آنلاین افراد را رمزگذاری میکند و تنها راه رمزگشایی داشتن کلید آن است. فقط کامپیوتر و VPN این کلید را می دانند و بنابراین دنبال کردن جستجوهای افراد برای ISP غیرممکن می شود.

درواقع رمزگذاری ای که VPN استفاده می کند برای این است که داده ها و افرادی که این داده ها برایشان ارسال می شوند مخفی بمانند.

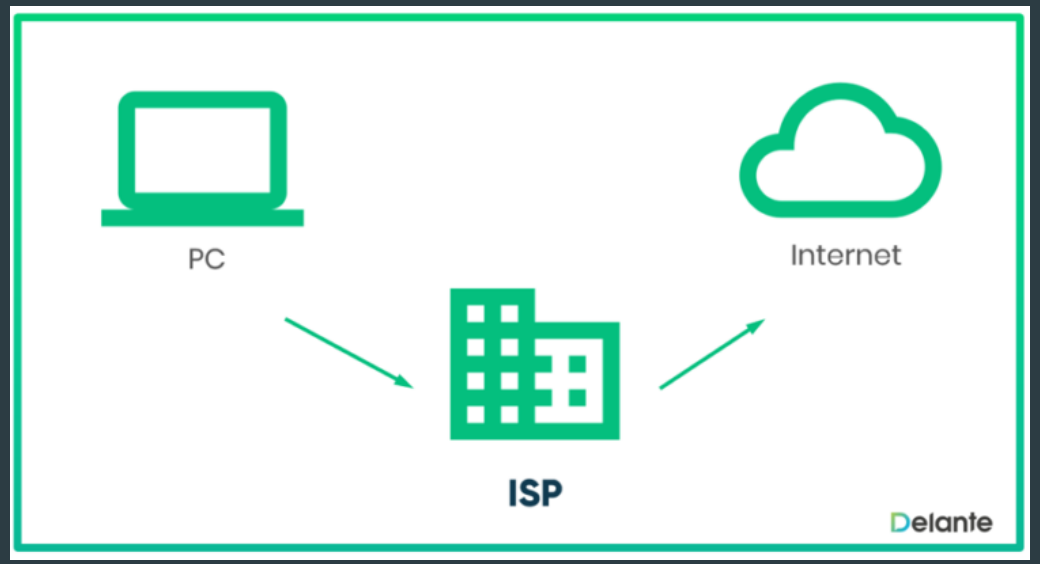
برخی از این VPN ها مانند ExpressVPN از AES-256 برای این رمزگذاری بهره می گیرند.

VPN (Virtual Private Network)

VPN یک اتصال رمزشده به سرور ایجاد می کند. وقتی به یک سرور VPN وصل می شوید و یک آدرس وب را تایپ می کنید، این درخواست به صورت یک سیگنال رمزشده به سمت سرور VPN فرستاده می شود و در همانجا رمزگشایی و به مقصد ارسال می شود و هنگامی که پاسخی از سمت مقصد دریافت کرد، آن را رمز کرده و به کاربر برمی گرداند.

تفاوت بین اتصال معمولی با اتصال VPN

درخواست از سوی مراجعه کننده (client) به طور مستقیم به وبسایت مربوطه ارسال می شود و دوباره به سمت مراجعه کننده برمی‌گردد و در این میان ISP تمام پاکت های اینترنتی رد و بدل شده را می‌بیند. بعضی اوقات ترافیک رمزگذاری شده است (HTTPS, TLS) که در این حالت ISP نمی‌تواند ترافیک کاربر را ببیند، در غیر این صورت ISP می فهمد که کاربر به کجاها وصل شده است و تمام ترافیک رمز نشده او را رصد میکند.

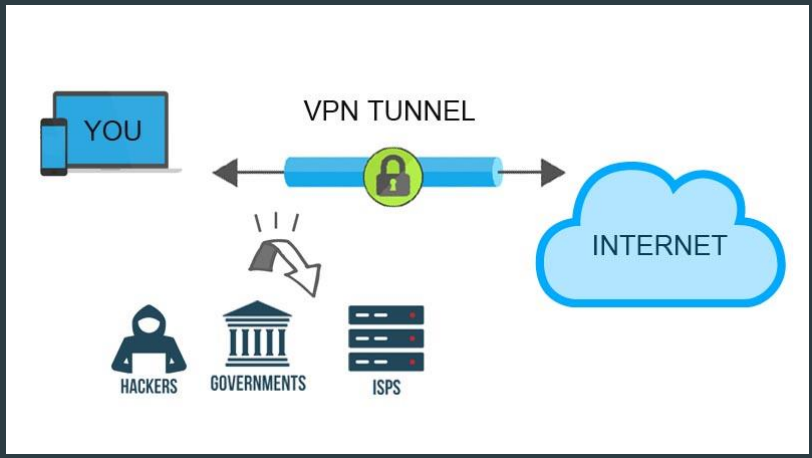


تفاوت بین اتصال معمولی با اتصال VPN

وقتی اتصال به اینترنت با VPN صورت بگیرد، VPN یک تونل میان کاربر و خودش ایجاد می‌کند، در این حالت کامپیوتر تمام ترافیک اینترنتی خود را از میان این تونل عبور می دهد. این تونل از میان ISP عبور می‌کند و چون تونل رمزگذاری شده است، ISP فقط می فهمد که کاربر از VPN استفاده کرده است.

حال به جای ISP، VPN کنترل کننده است که میتواند تمام ترافیک اینترنتی کاربر را ببیند. (البته در صورتی که اطلاعات کاربر را ثبت کرده باشد.)

بنابراین VPN میداند که کاربر به کجاها وصل شده و تمام ترافیک غیر رمزگذاری شده اش را رصد می کند.



اتصال OPEN VPN یکی از امن ترین نوع VPN است، زیرا فقط با یک پسورد رمز نمی‌شود بلکه با ترکیبی از جدیدترین روش‌های رمزگذاری متقارن و نامتقارن اطلاعات ارسالی به سرور را رمزگذاری می کند.

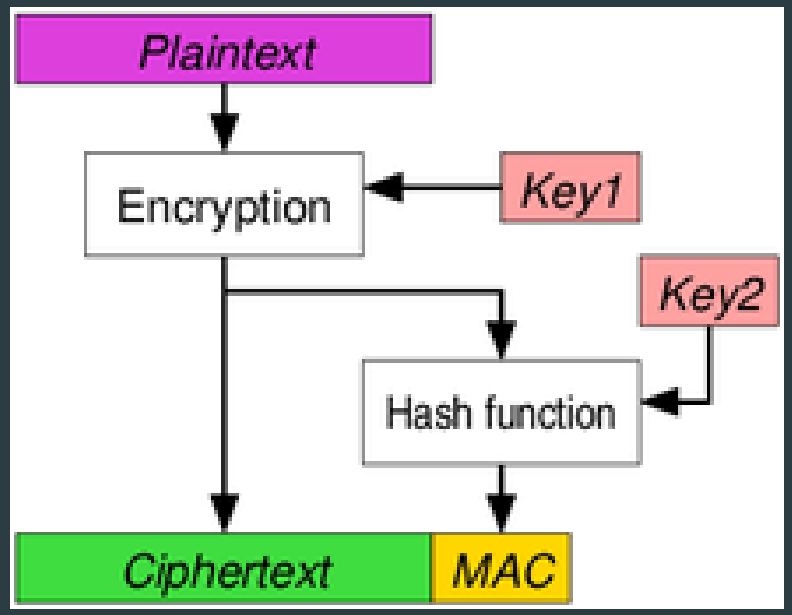
این پروتکل قابلیت پیکربندی دارد و اگر از الگوریتم AES استفاده شود، یکی از قویترین پروتکل های VPN خواهد بود.

از آنجا که این پروتکل به صورت تعبیه شده در سیستم عامل های رایج پشتیبانی نمی شود، برای استفاده از آن باید یک برنامه جانبی بر روی سیستم خود نصب کنید.

WhatsApp's end-to-end encryption

واتس اپ از سیستم رمزگذاری AES-256 برای مخدوش کردن پیام ها استفاده میکند که به همراه احراز هویت امن HMAC-SHA256 غیرقابل نفوذ میشود.

دستگاه فرستنده پیام، یک کلید موقت ۳۲ بایتی AES-256 و یک کلید موقت ۳۲ بایتی HMAC-SHA256 را تولید می کند و سپس فایل ارسال شده را با کلید AES-256 در مد CBC با یک IV تصادفی رمز کرده و با استفاده از HMAC-SHA256 یک MAC از متن رمز شده را می افزاید.



رمز کردن فایل RAR

به منظور رمز کردن فایل های RAR، فایل هایی را که می‌خواهید به آرشیو RAR اضافه کنید را انتخاب کرده و سپس روی دکمه Set Password کلیک کرده، روی دکمه Encrypt File Names کلیک و رمز مورد نظرتان را وارد کنید.

در نهایت آرشیو شما با سیستم رمزگذاری AES 256-bit رمز می شود.

انتقال امن فایل ها

این استاندارد به شکلی گسترده برای انتقال امن فایل‌ها و پیام‌های کاربران در بستر اینترنت مورد استفاده قرار می‌گیرد. به عنوان مثال هنگامی که از طریق پروتکل HTTPS (نسخه امن پروتکل وب HTTP) اقدام به باز کردن صفحات وب می‌کنید، برای انتقال فایل‌ها و اطلاعات مربوطه از رمزنگاری AES استفاده می‌شود تا بدین ترتیب ارتباط برقرار شده در مقابل آسیب‌های امنیتی مختلف به ویژه حملات Man-In-The-Middle مقاوم باشد.

Do banks use AES or RSA?

موسساتی مانند بانک ها، به دلیل **سرعت بیشتر** سیستم رمزگذاری AES در مقایسه با سیستم رمز RSA از آن استفاده می کنند. (الگوریتم RSA تقریبا چندین هزاربارکندتر از رمزهای متقارن با امنیت یکسان است.)

منابع

- https://nordvpn.com/features/next-generation-encryption/
- https://www.wikihow.com/Add-a-Password-to-a-RAR-File
- https://www.mobile.ir/news/view-2496-advanced-encryption-standard-aka-aes-overview.aspx
- https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf
- https://blog.avast.com/what-whatsapps-new-end-to-end-encryption-means-for-you#:~:text=WhatsApp%20is%20using%20AES%2D256,messages%20and%20for%20key%20verification.
- https://www.wizcase.com/blog/everything-you-need-to-know-about-vpn-encryption/#6
- https://crypto.stackexchange.com/questions/13235/how-do-institutions-like-banks-do-rsa-with-big-primes
- https://techjury.net/blog/what-is-aes/

با سپاس از توجه شما ☺