禪

رمزگذاری بهدنبال محدودسازی دسترسیهای غیرمجاز

فناوری رمزگذاری چگونه از اطلاعات ما محافظت میکند و آیا نفوذپذیر است؟

برای اغلب مردم واژه رمزنگاری اطلاعات بهمعنای آسودگی خیال است . به طوری که اطمینان حاصل میکنند افراد غیرمجاز به دادههای شخصی آنها روی دستگاههای الکترونیکی یا فضای ابری دسترسی نخواهند داشت. البته در این بین گروه دیگری نیز وجود دارند که با شنیدن این واژه به یاد باجافزارهایی میافتند که دادهها را رمزگذاری کرده و به آنها اجازه نمیدهند تا زمانی که مبلغ باج را پرداخت کنند، به دادههای خود دست پیدا کنند . اما فارغ از این بحثها یک حقیقت مسلم در ارتباط با این فناوری وجود دارد . گزارشی که چندی پیش منتشر شد نشان داد پروتکل رمزنگار WPA2 که در ارتباط با رمزنگاری ارتباطات بیسیم به کار میرود، روزانه از سوی میلیاردها دستگاه مورد استفاده قرار میگیرد . اما پرسشی که در این میان مطرح میشود این است که اساساً فناوری رمزگذاری چیست و آیا این فناوری بهاندازه کافی ایمن است که بتوانیم به آن اعتماد کنیم؟ در این مقاله سعی خواهیم کرد به زبانی ساده و کوتاه به این پرسش پاسخ دهیم .

همه ما کاربران فضای مجازی در طول روز بارها و بارها از این فناوری استفاده میکنیم، بدون آنکه واقعاً بدانیم در حال بهکارگیری فناوری رمزگذاری هستیم . گوشیهای هوشمند، سرویسهای پست الکترونیکی که دسترسی به ایمیلها را امکانپذیر میسازند، ارتباطات ایمنی که بر مبنای پروتکلهای رمزنگار کار میکنند، سایتهایی که برچسب پروتکل انتقال ابرمتن را نشان میدهند، همه و همه به ما این موضوع را یادآور میشوند که دادههای ما نباید بهشکل متن خام ارسال شوند .

فناوری رمزگذاری چیست؟

اولین نکتهای که باید به آن توجه داشته باشید این است که دو واژه رمزنگاری (Cryptography) و رمزگذاری (Encryption) اطلاعات دو معنای متفاوت از هم دارند . رمزگذاری نگارش پیشرفتهتر و بهروزتر رمزنگاری اطلاعات است . این فناوری به هر کاربری اجازه میدهد تا اطلاعات خود را از دسترسیهای غیرمجاز دور نگه دارد و در واقع آنها را پنهان سازد . یونانیان جزء اولین مللی بودند که فناوری رمزنگاری را برای پنهانسازی دادههای حساسی که در نامههای مکتوب ارسال میکردند مورد استفاده قرار دادند . آنها از یک شیوه ابتدایی رمزنگاری که بر مبنای وسیلهای شبیه به یک سیلندر کار میکرد و به Scytale گفته میشد، برای رمزنگاری و رمزگشایی کدها استفاده میکردند . رمزگذاری از الگوریتمها و محاسبات ریاضی پیچیدهای بهنام سایفر برای کد کردن دادهها استفاده میکند . مکانیسمی که در عمل کاراکترهای درون فایلها را به مجموعهای از کاراکترهای مبهم که خواندن آنها نهتنها برای انسانها بلکه برای برنامههای کاربردی نیز امکانپذیر نیست تبدیل میکند. در این حالت کاربر تنها زمانی میتواند چنین اطلاعاتی را رمزگشایی و مشاهده کند که کلید مخصوص را در اختیار داشته باشد . این کلید درست نقشی همانند کلیدهای فیزیکی دارد و برای باز کردن قفل و بازگرداندن متون به حالت اولیه مورد استفاده قرار میگیرد . دارندگان کلید رمزگشایی میتوانند کاراکترهای تصادفی را دو مرتبه به یک نوشته خام متنی تبدیل کنند . در حال حاضر در حوزه رمزگذاری اطلاعات از دو شیوه رمزگذاری کلید عمومی (نامتقارن) و رمزگذاری کلید خصوصی (متقارن) استفاده میشود . درست است که هر دو رویکرد به کاربران اجازه میدهند تا دادههای خود را رمزگذاری کنند و به این شکل مانع از آن شوند تا افراد غیرمجاز به دادههای آنها دسترسی داشته باشند، اما در عمل فرآیند رمزگذاری و رمزگشایی دو رویکرد متفاوت از هم هستند .

مطلب پیشنهادی

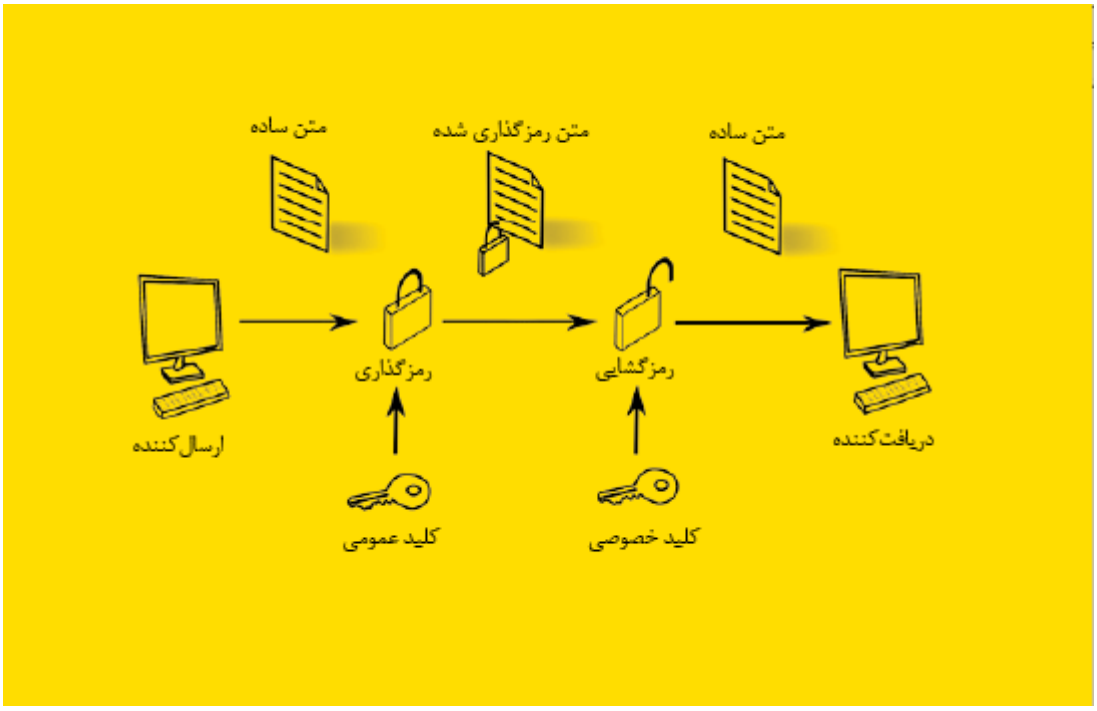
بهترین نرم‌افزارهای
رمزنگار
مخصوص سیستم عامل
ویندوز
Encryption App

دادهها را ایمن کنید

۱۸_برنامه برتر رمزنگار ویژه سیستم‌عامل ویندوز

رمزگذاری دادهها از طریق کلید عمومی

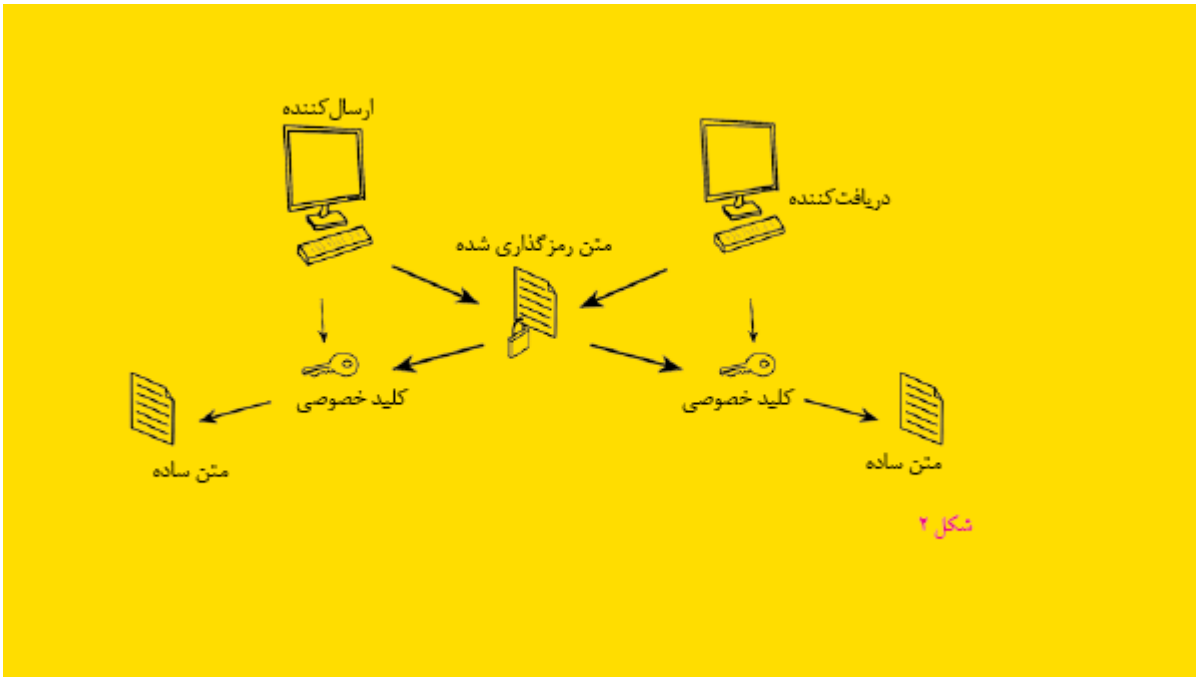
در الگوی کلید عمومی که بهنام رمزگذاری نامتقارن نیز از آن نام برده میشود، از ترکیب دو کلید عمومی و خصوصی (بر مبنای محاسبات ریاضی) برای کدگذاری اطلاعات استفاده میشود . (شکل 1) به طور مثال، دو کاربر به نامهای جو و کارن را تصور کنید که هر دو کلید مربوط به جعبهای را در اختیار دارند . جو کلید عمومی و کارن کلید خصوصی که بهمنظور تطابق مورد استفاده قرار میگیرد را دارد . جو میتواند از کلید خود برای باز کردن قفل جعبه استفاده و محتوایی را به آن اضافه کند، اما این توانایی را ندارد تا محتوایی که درون جعبه قرار گرفته است را مشاهده کند . در نتیجه نمیتواند هیچگونه محتوایی را بازیابی کند . در طرف دیگر این داستان کارن قرار دارد که قادر است جعبه را باز کند و محتوایی که درون جعبه قرار دارد را مشاهده و محتوایی را حذف کند . بهواسطه آنکه کلید خصوصی که برای تطابق مورد نیاز است را در اختیار دارد . با وجود این، کارن نمیتواند محتوایی را به جعبه اضافه کند، بهواسطه آنکه کلید عمومی را در اختیار ندارد . درست مشابه مثالی که به آن اشاره داشتیم، در دنیای دیجیتال نیز همین قاعده وجود دارد . فردی که کلید عمومی در اختیار او است این توانایی را دارد تا یک متن ساده را رمزگذاری و برای کاربران دیگر ارسال کند . اما کاربران دیگر تنها از طریق داشتن کلید خصوصی که برای تطابق مورد استفاده قرار میگیرد قادر هستند پیامهای ارسال شده را رمزگشایی کنند . در مثال یاد شده، اگر کارن در نظر داشته باشد یک متن ساده را رمزنگاری و ارسال کند، به کلید عمومی نیاز دارد . به عبارت دقیقتر، کارایی این دو کلید متفاوت از یکدیگر هستند و هیچکدام کار دیگری انجام نمیدهند .



1 شکل

[illegible]

[illegible] (شکل 2).



2 شکل

سه رویکرد سنتی رمزنگاری در دنیای قدیم

در حالی که یونانیان در زمینه رمزنگاری جزء پیشگامان این حوزه به شمار میروند، اما رومیها نیز در پیشبرد و تکامل فناوری رمزنگاری بیتأثیر نبودند . آنها از یک الگوی رمزنگاری خاص بهنام رمز سزار استفاده میکردند . در این الگو حروف درون نامه بهسمت حروف دیگری که پایینتر از حرف اصلی قرار داشت حرکت میکردند و جایگزین میشدند . به طور مثال، حرف A جای خود را به D میداد، حرف B جای خود را به E میداد و این رویکرد ادامه پیدا میکرد . نکته جالب توجهی که وجود دارد این است که این الگوی رمزنگاری تا پنج سال پیش نیز از سوی یکسری سایتهای تورنت به کار گرفته میشد تا درنهایت برنامهنویسی از طریق یک برنامه ساده چند خطی که به زبان سی شارپ نوشته شده بود نشان داد این الگوریتم رمزنگاری بهسادگی قابل شکسته شدن است .

مربع Polybius

یکی دیگر از پیشرفتهای رمزنگاری در عهد یونان باستان رخ داد که روی یک شبکه 5x5 کار میکرد که کاراکتر A در سمت چپ بالا و Z در پایین سمت راست ("J", "I") مربع قرار میگرفت . اعداد 1 تا 5 بهصورت افقی و عمودی در بالای ردیفهای بالای ستونها قرار میگرفتند . برای رمزگشایی شما به شمارهها و سپس قرار دادن درست شمارهها در این شبکه متکی بودید . به طور مثال، واژه Ball متناظر به 12,11,31,31 بود .(شکل3)

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

شکل **3**

مقدمة حول التشفير

التشفير هو عملية تحويل البيانات من شكلها الأصلي إلى شكل غير مفهوم، بحيث لا يمكن قراءتها إلا من قبل الأشخاص الذين يمتلكون المفتاح المناسب. يستخدم التشفير في العديد من التطبيقات، مثل حماية البيانات المخزنة على الأجهزة، وتأمين الاتصالات عبر الإنترنت، وحماية المعاملات المالية. يعتمد التشفير على خوارزميات رياضية معقدة تستخدم مفاتيح لتشفير وفك تشفير البيانات.

أنواع التشفير

هناك نوعان رئيسيان من التشفير: التشفير المتماثل والتشفير غير المتماثل.

التشفير المتماثل (Symmetric Encryption)

في التشفير المتماثل، يستخدم نفس المفتاح لتشفير وفك تشفير البيانات. هذا يعني أن المرسل والمستقبل يجب أن يكونا على علم بالمفتاح السري. من أمثلة خوارزميات التشفير المتماثل معيار تشفير البيانات (DES) الذي تم تطويره في السبعينيات. على الرغم من أنه كان آمنًا في ذلك الوقت، إلا أنه أصبح عرضة للهجمات في العقود اللاحقة. في عام 1977، قدرت وكالة الأمن القومي الأمريكية أن كسر تشفير DES يتطلب جهدًا حاسوبيًا هائلًا.

التشفير غير المتماثل

في التشفير غير المتماثل، يستخدم مفتاحان مختلفان: مفتاح عام ومفتاح خاص. المفتاح العام يستخدم لتشفير البيانات، والمفتاح الخاص يستخدم لفك تشفيرها. يمكن توزيع المفتاح العام بحرية، بينما يجب الحفاظ على سرية المفتاح الخاص. من أمثلة خوارزميات التشفير غير المتماثل RSA و ECC. يستخدم التشفير غير المتماثل على نطاق واسع في التجارة الإلكترونية والتوقيعات الرقمية.

معيار تشفير البيانات المتقدم (AES)

معيار تشفير البيانات المتقدم (AES) هو خوارزمية تشفير متماثل تستخدم على نطاق واسع اليوم. تم اعتماده من قبل المعهد الوطني للمعايير والتقنية (NIST) في عام 2001 كبديل لـ DES. يدعم AES أطوال مفاتيح مختلفة، بما في ذلك 128 بت و 192 بت و 256 بت. يعتبر AES آمنًا جدًا ضد الهجمات المعروفة حتى الآن. يستخدم AES في العديد من التطبيقات، بما في ذلك حماية البيانات في شبكات Wi-Fi وتشفير الملفات على الأقراص الصلبة.

يعتمد AES على عملية تسمى شبكة استبدال-تبديل (Substitution-permutation network). تتكون هذه الشبكة من سلسلة من الخطوات التي تتضمن استبدال البايتات وتبديل الصفوف والأعمدة ومزج البيانات باستخدام مفتاح التشفير. عدد هذه الخطوات يعتمد على طول المفتاح. على سبيل المثال، يستخدم AES-128 10 جولات، بينما يستخدم AES-256 14 جولة. كل جولة تزيد من تعقيد التشفير وتجعل من الصعب على المهاجمين كسره.

3DES

3DES هو تطبيق لـ DES يستخدم ثلاث مرات. تم تطويره في عام 1977 كطريقة لتعزيز أمان DES. يستخدم 3DES ثلاثة مفاتيح DES مختلفة لتشفير البيانات. يعتبر 3DES أكثر أمانًا من DES، ولكنه أبطأ بكثير.

Triple DES או 3DES, שיטה שנוצרה כדי להתגבר על החולשות של DES. 3DES מבצעת שלושה סבבים של DES, כל אחד עם מפתח אחר, ולכן אורך המפתח האפקטיבי הוא 168 ביט. 3DES נחשבת עדיין בטוחה יחסית, אך היא איטית יחסית ולכן פחות נפוצה כיום. רוב המערכות החדשות עוברות לשימוש ב-AES או בצפנים מודרניים אחרים.

AES – התקן הנוכחי

Advanced Encryption Standard (AES) הוא התקן הנוכחי לצפנה סימטרית, שאומץ על ידי ממשלת ארצות הברית ב-2001 לאחר תחרות פתוחה בין מספר אלגוריתמים. הזוכה היה אלגוריתם בשם Rijndael, שפותח על ידי שני חוקרים בלגיים. AES תומך באורכי מפתח של 128, 192 או 256 ביט, ומבצע את הצפנת המידע בבלוקים של 128 ביט. מספר הסבבים תלוי באורך המפתח: 10 סבבים עבור מפתח של 128 ביט, 12 עבור 192 ביט ו-14 עבור 256 ביט. AES נחשב כיום לבטוח מאוד, ואין ידוע על פרצה משמעותית בו. בניגוד ל-DES, שתוכנן במקור לחומרה, AES תוכנן מלכתחילה להיות יעיל גם בתוכנה, ולכן הוא מהיר ונוח לשימוש במגוון רחב של מכשירים, החל ממחשבים חזקים ועד למכשירים ניידים. בשל כך, AES הפך לבחירה הנפוצה ביותר בעולם. הוא משמש בפרוטוקולים כמו TLS, בקבצי ZIP מוצפנים, ברשתות Wi-Fi מאובטחות ובתוכנות כמו FileVault של אפל. כמעט כל מערכת חדשה שדורשת הצפנה סימטרית בוחרת כיום ב-AES כברירת מחדל.

RSA – הצפנה אסימטרית

RSA הוא אחד האלגוריתמים הידועים ביותר בתחום ההצפנה האסימטרית. הוא פותח בשנת 1977 על ידי שלושה חוקרים במכון הטכנולוגי של מסצ'וסטס (MIT): רון ריבסט, עדי שמיר ולאונרד אדלמן, שמקור שמם נגזר מהאותיות הראשונות של שמותיהם. בניגוד לצפנים סימטריים, שבהם אותו מפתח משמש להצפנה ולפענוח, RSA עושה שימוש בזוג מפתחות: מפתח ציבורי, שניתן לשתף עם כל אחד, ומפתח פרטי, שחייב להישמר בסוד. ניתן להצפין הודעה באמצעות המפתח הציבורי, אך ניתן לפענח אותה רק באמצעות המפתח הפרטי המתאים. RSA מבוסס על הקושי המתמטי בפירוק מספרים גדולים למכפלת גורמים ראשוניים. כאשר המפתחות ארוכים מספיק, כלומר 2048 ביט או יותר, אין כיום דרך יעילה לבצע זאת, ולכן RSA נחשב בטוח מאוד. בשל מהירותו הנמוכה יחסית, RSA משמש בעיקר להחלפת מפתחות סימטריים ולחתימה דיגיטלית, ולא להצפנת כמויות גדולות של מידע. הוא נמצא בשימוש נרחב בתוכנות כמו PGP ובפרוטוקולים כמו SSH. עם זאת, RSA הולך ומאבד מקרקע לטובת אלגוריתמים חדשים יותר, כמו ECC, שמספקים אבטחה דומה עם מפתחות קצרים בהרבה.

ECC – הצפנה מבוססת עקומות אליפטיות

הצפנה מבוססת עקומות אליפטיות, או ECC, היא שיטה מודרנית יחסית שהולכת וצוברת פופולריות בשנים האחרונות. היתרון המרכזי שלה הוא שהיא מספקת רמת אבטחה גבוהה עם מפתחות קצרים בהרבה מאלו של RSA. לדוגמה, מפתח של 256 ביט ב-ECC נחשב לבטוח בערך כמו מפתח של 3072 ביט ב-RSA. בזכות זה, ECC מתאים במיוחד למכשירים עם משאבים מוגבלים, כמו טלפונים חכמים, כרטיסי חכם ומערכות IoT. הוא נמצא בשימוש נרחב בפרוטוקולים מודרניים כמו TLS 1.3, ב-Bitcoin וב-Ethereum, וכן בתוכנות כמו Signal ו-WhatsApp. למרות יתרונותיו, ECC מורכב יותר להבנה ולמימוש נכון, ולכן יש לבחור בספריות מוכרות ולהימנע מכתיבת קוד קריפטוגרפי בעצמך.

תמונה לדוגמה

[קישור לדוגמה](#)

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]:
[illegible]
[illegible]:
wired
makeuseof
[illegible]:
[illegible]
[illegible]:
12:00 - 20/06/1397
[illegible]:
[illegible] - [illegible] - [illegible] - [illegible] - [illegible] - Cryptography [illegible] - RSA [illegible] - AES [illegible] - 3DES [illegible] - Polybius [illegible] - [illegible] - Backdoor [illegible] - [illegible]

[illegible]

https://www.shabakeh-mag.com/security/12513/%D9%81%D9%86%D8%A7%D9%88%D8%B1%:□□□□
DB%8C-%D8%B1%D9%85%D8%B2%DA%AF%D8%B0%D8%A7%D8%B1%DB%8C-
%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D8%B2-
%D8%A7%D8%B7%D9%84%D8%A7%D8%B9%D8%A7%D8%AA-%D9%85%D8%A7-
%D9%85%D8%AD%D8%A7%D9%81%D8%B8%D8%AA-
%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D8%AF-%D9%88-%D8%A2%DB%8C%D8%A7-
%D9%86%D9%81%D9%88%D8%B0%D9%BE%D8%B0%DB%8C%D8%B1-
%D8%A7%D8%B3%D8%AA%D8%9F