คู่มือขั้นสูงสำหรับ Advanced Encryption Standard (AES)

การเข้ารหัสมีผลกระทบสำคัญต่อความเป็นส่วนตัวของคุณ มักจะถูกพูดถึงว่าเป็นวิธีที่มีประสิทธิภาพสูงสุดในการรักษาความปลอดภัย การเข้ารหัสให้**ความปลอดภัยในการส่งข้อมูลที่สำคัญ**เช่นบันทึกข้อมูลของรัฐบาลและข้อมูลสุขภาพส่วนตัว

เนื่องจากฟีเจอร์ด้านความปลอดภัยกำลังได้รับความสนใจไปสู่ตลาดอย่างกว้างขวางด้วยการเปิดตัวการสื่อสารที่เข้ารหัสเช่น Whatsapp **ผู้ใช้จะต้องเข้ารหัสแบบ end-to-end** กับเกือบทุกวิธีการสื่อสารที่นำเสนอ

การเข้ารหัสคืออะไรกันแน่และทำไมมันจึงสำคัญกับชีวิตประจำวัน นี่คือทุกสิ่งที่คุณจำเป็นต้องรู้เกี่ยวกับการเข้ารหัสและเหตุผลที่สำคัญสำหรับคุณ

Encryption – **การเข้ารหัสข้อมูลส่วนตัว**

คุณอาจมีข้อมูลที่ละเอียดอ่อน เช่นข้อมูลทางการเงินในโทรศัพท์ แล็ปท็อป แท็บเล็ตหรืออุปกรณ์อื่น ๆ **หากไม่มีการเข้ารหัสข้อมูลส่วนตัวใด ๆ ก็สามารถเข้าถึงได้โดยบุคคลที่สามและบุคคลที่ไม่ประสงค์ดี**
เมื่อมีการเข้ารหัสข้อมูล มันจะจัดเรียงข้อความใหม่ทำให้ไม่สามารถอ่านได้ซึ่งเรียกว่า ciphertext เพื่อเข้าถึงข้อมูล**บุคคลที่ต้องการอ่านจะต้องมีคีย์การเข้ารหัส**เพื่อให้สามารถถอดรหัสลับข้อความและส่งกลับไปยังรูปแบบที่อ่านได้

ขณะนี้**ระดับการเข้ารหัสสูงสุดคือ 256-bit และ 128-bit** เพียงแค่ใส่บิตหมายเลขขนาดของคีย์การเข้ารหัสและมันจะที่ทำหน้าที่เป็นรหัสผ่าน ยิ่งมีขนาดใหญ่เท่าไหร่ก็ยิ่งยากขึ้นเท่านั้น เพื่อให้เข้าใจได้ง่ายขึ้นการเข้ารหัส 128-bit จะใช้โดยธนาคารและทหารและมีความแข็งแกร่งกว่าการเข้ารหัส 40-bit ล้านล้านเท่า

สองรูปแบบของการเข้ารหัส: แบบสมมาตรและไม่สมมาตร

การเข้ารหัสแบบสมมาตรและการเข้ารหัสแบบไม่สมมาตรมีความปลอดภัยในการส่งข้อมูล อย่างไรก็ตามการเข้ารหัสแบบไม่สมมาตรไม่จำเป็นต้องมีการกระจายคีย์ส่วนตัวของคุณ เพิ่มชั้นความปลอดภัยพิเศษในขณะที่อัลกอริทึมสมมาตรอาจเร็วกว่าเนื่องจากไม่จำเป็นต้องใช้การคำนวณมากนัก

- **การเข้ารหัสแบบสมมาตร**

การเข้ารหัสแบบสมมาตรหรือที่เรียกว่าคีย์ลับ**ใช้รหัสเดียวกันสำหรับการเข้ารหัสและถอดรหัสข้อมูล** รหัสลับนี้จะแชร์ให้กับผู้ส่งและผู้รับเท่านั้น อย่างไรก็ตามหากบุคคลภายนอกเข้าถึงรหัสนี้การเข้ารหัสจะถูกบุกรุกและข้อมูลของคุณจะไม่ได้รับการปกป้องอีกต่อไป

- **การเข้ารหัสลับแบบไม่สมมาตร**

หรือที่รู้จักกันในชื่อรหัสอัลกอริทึมแบบไม่สมมาตรการเข้ารหัสประเภทนี้**ใช้รหัสที่แตกต่างกันสำหรับการเข้ารหัสและถอดรหัสข้อมูล** การใช้ทั้งisylส่วนตัว (รู้เพียงเจ้าของ) และคีย์สาธารณะ (รู้แค่ในเครือข่ายเดียวกัน) ข้อมูลที่เข้ารหัสสาธารณะสามารถถูกถอดรหัสโดยรหัสส่วนตัวที่เทียบเท่าได้เท่านั้น

มาตรฐานการเข้ารหัสขั้นสูง – AES

เดิมเรียกว่า Rijndael **AES ย่อมาจาก Advanced Encryption Standard** เป็นหนึ่งใน**วิธีที่ใช้กันทั่วไปในการเข้ารหัสข้อมูลที่สำคัญ**ซึ่งใช้โดยองค์กรตั้งแต่ Apple และ Microsoft ไปจนถึง NSA

ฟีเจอร์ด้านความปลอดภัย AES

AES เป็นขั้นตอนวิธีการเข้ารหัสมาตรฐานชั้นสูงที่ทันสมัยเนื่องจากมีฟีเจอร์ดังต่อไปนี้:

การรักษาความปลอดภัย อัลกอริทึม AES มีความสามารถในการต่อต้านการโจมตีได้มากกว่าวิธีการเข้ารหัสอื่น ๆ

ค่าใช้จ่าย: มีเป้าหมายที่จะปล่อยให้ใช้งานได้ทั่วโลก ไม่ผูกขาดและไม่เสียค่าใช้จ่าย อัลกอริทึม AES มีประสิทธิภาพในการคำนวณและหน่วยความจำ

การดำเนินงาน: อัลกอริธึม AES มีความยืดหยุ่นและเหมาะสมอย่างยิ่งเมื่อใช้งานกับฮาร์ดแวร์และซอฟต์แวร์รวมทั้งใช้งานง่าย

อัลกอริทึมแบบ Block Ciphe

วิธีการเข้ารหัสนี้จัดเก็บข้อมูลโดยใช้อัลกอริทึมแบบ Block Ciphe Blocks จะสร้างข้อมูลข้อความและเป็นผลลัพธ์ของ ciphertext ซึ่งวัดค่าเป็นหน่วย bit ตัวอย่างเช่นถ้าใช้ AES 128-bit จะมี **128 bit ของข้อความที่ไม่สามารถอ่านได้ที่เขียนต่อข้อความจำนวน 128 bit**

โดยรวมทั้งหมด**มี block ciphers สามประเภทที่ AES ประกอบด้วย AES-128, AES-192 และ AES-256** แต่ละ AES เข้ารหัสจะเข้ารหัสและถอดรหัสข้อมูลในบล็อค 128 bits โดยใช้คีย์เข้ารหัสลับ 128, 192 และ 256-bit **โดย 256-bit เป็นระบบที่ปลอดภัยที่สุด** สำหรับคีย์ 128-bit มีกระบวนการเข้ารหัส 10 รอบ 12 รอบสำหรับคีย์ 192 บิตและ 14 รอบสำหรับคีย์ 256 บิต **อัลกอริทึม AES แบบสมมาตร**ซึ่งหมายความว่ามีการใช้คีย์เดียวกันสำหรับกระบวนการเข้ารหัสและถอดรหัสดังนั้นผู้ส่งและผู้รับจะรู้ว่าต้องใช้คีย์เดียวกัน

AES vs. DES: **ยุคใหม่ของการเข้ารหัส**

Data Encryption Standard หรือ DES เป็นพื้นฐานของ AES ในช่วงต้นปี 1970 ไอบีเอ็มได้พัฒนา DES แบบต้นฉบับ ซึ่งได้ส่งต่อให้ National Bureau of Standards และใช้โดย NSA **DES เป็นอัลกอริธึมการรักษาความปลอดภัยมาตรฐานที่ใช้โดยรัฐบาลสหรัฐอเมริกาเป็นเวลา 20 ปี**จนกระทั่ง distributed.net ร่วมมือกับมูลนิธิพรมแดนอิเล็กทรอนิกส์**เปิดเผย DES ต่อสาธารณชนในเวลาไม่ถึง 24 ชั่วโมง**

AES เริ่มพัฒนาใน National Institute of Standards and Technology (NIST) เมื่อเห็นได้ชัดว่าจำเป็นต้องมีตัวตายตัวแทนของ DES หลังจากกลายเป็นกลุ่มเสี่ยงต่อการโจมตี อัลกอริธึมใหม่นี้ได้รับการออกแบบมาให้ใช้งานง่ายในฮาร์ดแวร์ซอฟต์แวร์และสภาพแวดล้อมแบบ จำกัด AES จะไม่มีการแบ่งประเภท

และสามารถป้องกันข้อมูลที่มีความสำคัญของรัฐบาลต่อเทคนิคการโจมตีต่าง ๆ **AES จะเร็วกว่า DES 6 เท่าและเร็วกว่า 3 เท่าของ DES**

การเปรียบเทียบ DES กับ AES

	DES	AES
ถูกพัฒนา	1977	1999
ความยาวของรหัส	56 bits	128, 192 หรือ 256 bits
ประเภทการเข้ารหัส	การเข้ารหัสลับแบบสมมาตร	การเข้ารหัสลับแบบสมมาตร
ขนาดบล็อค	64 bits	128 bits
ความปลอดภัย	ได้รับการพิสูจน์แล้วว่าไม่เพียงพอ	ถือว่าปลอดภัย

การใช้งานทั่วไปของ AES

AES นำเสนอในทั้งเชิงพาณิชย์และไม่ใช่เพื่อการค้า เอกชนและสาธารณชนเพื่อใช้งานฟรี นี่คือการใช้ทั่วไปอื่น ๆ สำหรับอัลกอริทึม AES:

- **VPN**

Virtual Private Networks (VPN) มักใช้ AESS VPN คือเครื่องมือที่ช่วยให้คุณสามารถรักษาความปลอดภัยการเชื่อมต่อเครือข่ายโดยส่งที่อยู่ IP ของคุณไปยังเซิร์ฟเวอร์ที่ปลอดภัยซึ่งดำเนินการโดยผู้ให้บริการในตำแหน่งอื่น ๆ ในโลก **VPN ทำงานได้ดี**เมื่อเชื่อมต่อกับเครือข่ายแบบเปิด เครือข่ายที่ไม่มีการป้องกันเช่นร้านกาแฟ

- **คลังข้อมูลและการบีบอัด**

ไฟล์ใด ๆ ก็ตามสามารถถูกบีบอัดได้เพื่อลดขนาดและลดผลกระทบในฮาร์ดดิสก์ของคุณ **จะอาศัยซอฟต์แวร์ที่มีการเข้ารหัส AES** ไฟล์เหล่านี้มักเป็นไฟล์ที่สามารถดาวน์โหลดได้จากอินเทอร์เน็ตเช่น WinZip, Zip 7 และ RAR

- **การเขารหัสทั้งดิสก์/เฉพาะส่วน**

หากคุณคุ้นเคยกับการเข้ารหัสและทำงานเพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลของคุณปลอดภัย**คุณจะใช้ซอฟต์แวร์การเข้ารหัสดิสก์/เฉพาะส่วนที่บูรณาการเข้ากับอัลกอริทึม AES** ซอฟต์แวร์เช่น BitLocker, FileVault และ CipherShed ทำงานบน AES เพื่อรักษาความเป็นส่วนตัวของข้อมูลของคุณ

- **โปรแกรมอื่น ๆ**

a. **เครื่องมือรหัสผ่าน**: เครื่องมือรหัสผ่านนิยมใช้การเข้ารหัส AES 256-bit เพื่อรักษาความปลอดภัยข้อมูลผู้ใช้
b. **วิดีโอเกมส์**: นักพัฒนาซอฟต์แวร์เช่น Rockstar ที่สร้างเกม Grand Theft Auto ใช้การเข้ารหัส AES เพื่อป้องกันไม่ให้แฮกเกอร์ละเมิดการใช้งานในเซิร์ฟเวอร์หลายผู้เล่น
c. **แอพพลิเคชั่นข้อความ**: WhatsApp เข้ารหัสข้อความที่ส่งผ่านแอ็พพลิเคชันโดยใช้ AES

ข้อสรุป

ด้วยความก้าวหน้าทางเทคโนโลยีอย่างต่อเนื่องความถี่ของการโจมตีทางไซเบอร์จะเพิ่มขึ้นเรื่อย ๆ ปัจจุบันยังไม่มีวิธีสามารถละเมิดการเข้ารหัส AES ทำให้เป็นแรงผลักดันที่สำคัญในด้านความปลอดภัยและจำเป็นสำหรับการปกป้องข้อมูลของคุณและลดความเสี่ยงในการถูกโจมตี การเข้ารหัส AES ถูกบูรณาการเข้าไว้ในระบบซอฟต์แวร์และฮาร์ดแวร์จำนวนมากและหากได้รับการยอมรับอย่างเต็มที่ ศักยภาพของมันดูเหมือนจะไร้ขีดจำกัด

ที่มา

https://th.wizcase.com/blog/คู่มือขั้นสูงสำหรับ-advanced-encryption-standard/