การเข้ารหัสและถอดรหัสข้อมูลด้วย AES-128-CTR

โดย สถานส่งเสริมและพัฒนาระบบสารสนเทศเพื่อการจัดการ (MIS)

1-2-2568

AES-128-CTR คืออะไร?

1. AES (Advanced Encryption Standard) คืออะไร?

AES (Advanced Encryption Standard) เป็น **อัลกอริทึมเข้ารหัสแบบสมมาตร** (Symmetric Encryption) ซึ่งถูกพัฒนาให้เป็นมาตรฐานสากลในการเข้ารหัสข้อมูล โดยใช้หลักการของ **บล็อกเข้ารหัส (Block Cipher)** และมีขนาดคีย์ที่นิยมใช้คือ

AES-128 : ใช้คีย์ขนาด **128 บิต** (16 ไ บ ต์)

AES-192 : ใช้คีย์ขนาด **192 บิต** (24 ไ บ ต์)

AES-256 : ใช้คีย์ขนาด **256 บิต** (32 ไ บ ต์)

2. CTR Mode (Counter Mode) คืออะไร?

เป็นโหมดการเข้ารหัสของ AES (Advanced Encryption Standard) ที่ใช้ ค่าเพิ่มขึ้น (Counter, Nonce) ร่วมกับคีย์ลับเพื่อเข้ารหัสข้อมูลทีละบล็อกแบบ stream cipher

Stream Cipher คืออะไร?

Stream Cipher เป็นรูปแบบการเข้ารหัสที่ทำงานกับ **ข้อมูลทีละบิตหรือทีละไบต์** (แทนที่จะเป็นบล็อกใหญ่ ๆ เหมือน **Block Cipher**) โดยใช้ **keystream (กระแสกุญแจ)** ที่สร้างจาก **คีย์ลับ + ค่าเริ่มต้น (IV/Nonce)**

```php
$encryption_key = "mysecretkey12345"; // คีย์ความลับ (ควรเก็บไว้อย่างปลอดภัย)
$cipher = "AES-128-CTR"; /* รูปแบบการเข้ารหัส */
$iv_length = openssl_cipher_iv_length($cipher); // ความยาวของ IV (16 bytes) ขนาดตัวการเข้ารหัส
```

$encryption_key : กำหนดค่าคีย์สำหรับใช้ในการเข้ารหัสและถอดรหัส (ควรเก็บไว้อย่างปลอดภัย)

$cipher : กำหนดอัลกอริทึมการเข้ารหัสเป็น AES-128-CTR

$iv_length : ค่า IV เป็นค่าที่ใช้เพื่อเพิ่มความสุ่มให้กับกระบวนการเข้ารหัส ความยาวของ IV ขึ้นอยู่กับอัลกอริทึมที่ใช้ ในกรณีนี้คือ 16 ไบต์

```php
$encodeSecretData = function($data) use ($encryption_key, $cipher, $iv_length) {
    $iv = openssl_random_pseudo_bytes($iv_length); // สร้างค่า IV ค่าที่ใช้สำหรับเพิ่มความสุ่มให้กับกระบวนการเข้ารหัส
    $encrypted = openssl_encrypt($data, $cipher, $encryption_key, 0, $iv); // เอาข้อมูลมาเข้ารหัส
    $encrypted_data = base64_encode($iv . $encrypted); // เก็บ IV รวมกับข้อมูลที่เข้ารหัส

    return $encrypted_data;
};
```

สร้างค่า IV : ใช้ openssl_random_pseudo_bytes($iv_length) เพื่อให้การเข้ารหัสมีความปลอดภัยมากขึ้น

เข้ารหัสข้อมูล : ใช้ openssl_encrypt($data, $cipher, $encryption_key, 0, $iv);

รวม IV และข้อมูลเข้ารหัส : เพื่อนำไปใช้ตอนถอด

แปลงเป็น Base64 : เพื่อให้สามารถส่งต่อเป็นข้อความธรรมดาได้

```php
$decodeSecretData = function($data) use ($encryption_key, $cipher, $iv_length){

    $encrypted_data = base64_decode($data);

    if (strlen($encrypted_data) < $iv_length) {
        return $data;
    }

    $iv = substr($encrypted_data, 0, $iv_length); // แยก IV ออก
    $encrypted = substr($encrypted_data, $iv_length); // แยกข้อมูลเข้ารหัส

    // ถอดรหัสข้อมูล
    $decrypted = openssl_decrypt($encrypted, $cipher, $encryption_key, 0, $iv);


    return $decrypted;
};
```

ถอดรหัส Base64 : แปลงข้อมูลที่เข้ารหัสกลับมาเป็น Binary ัส
ตรวจสอบความถูกต้องของข้อมูล : ถ้าไม่ตรงตามขนาด IV ให้คืนค่าเดิม
แยกค่า IV และข้อมูลเข้ารหัส : เพื่ อนำ มาใช้ ถอดรห
ถอดรหัสข้อมูล : ใช้ openssl_decrypt() เพื่อดึงค่าต้นฉบับกลับคืนมา

```php
$idcad = "123456789";

echo $encodeSecretData($idcad);

echo "<hr>";

echo $decodeSecretData("WJxdLmfFxS7SoDAVnReKdFQ3R1VJWU1XMXZTeQ==");
```

Innovate the Future

SUT

SURANAREE
UNIVERSITY OF
TECHNOLOGY

www.sut.ac.th