

Assignment การแข่ง CTF – CPECipherCrack 2025 (กลุ่มละ 3-5 คน)

ให้นักศึกษาออกแบบการแข่งขัน CTF เกี่ยวกับการเข้ารหัส ด้วยข้อกำหนดดังนี้

ข้อกำหนดบังคับ

1. โจทย์สำหรับเข้าทำสามารถอยู่ในรูป Web application, Command-line Interfaces (CLIs), Web API หรือสามารถเสนอได้
2. โจทย์มีเอกลักษณ์ที่น่าสนใจ (มีคะแนนในส่วนนี้)
3. โจทย์ CTF ต้องประกอบไปด้วยทั้ง 3 วิธีการข้างล่าง (ผสมก่อนหลังได้อิสระ)
 - a. Symmetric cryptography
 - b. Asymmetric cryptography
 - c. Hash function
4. วิธีการเข้ารหัสทั้ง 3 วิธีข้างบนจะมีที่มาที่ไปที่เหมาะสมในการใช้ (มีคะแนนในส่วนนี้)
5. สามารถเอาสิ่งอื่นแต่สามารถเข้าถึงจาก Computer มาเป็นส่วนหนึ่งในขั้นตอนการแก้โจทย์ได้แต่ต้องเป็นสิ่งที่อยู่ใน มทส. เท่านั้น ยกตัวอย่างเช่น มีรูปภาพตึกเครื่องมือในโจทย์นี้ ซึ่งอาจตีความเป็นตัวเลขจำนวนตึกเครื่องมือทั้งหมดใน มทส. มาเป็นตัวเลขในการไขปริศนาได้
6. ทุกคนในทีมต้องมีการแบ่งหน้าที่ (มีคะแนนในส่วนนี้)
7. นักศึกษาในทีมต้องสามารถเล่าการทำงานของวิธีการเข้ารหัสทุกขั้นตอนได้ (รวมถึงการทำงานหลักๆ ของอัลกอริทึมการเข้ารหัส แต่ไม่ต้องถึงขนาดเข้าใจสมการ) (มีคะแนนในส่วนนี้)
8. โจทย์ต้องมีความเหมาะสมในการใช้เวลาแก้โจทย์ไม่เกิน 2 ชั่วโมง (มีคะแนนในส่วนนี้)
9. ความยากที่เหมาะสม ไม่ยากเกินไปและไม่ง่ายเกินไป (มีคะแนนในส่วนนี้)

สิ่งที่ต้องส่ง

0. Zip ไฟล์ทั้งหมดข้างล่าง
 1. Source code
 2. รายงานอธิบายการแก้โจทย์ พร้อมผลลัพธ์ (ไม่เกิน 20 หน้า)