Assignment (Cyber Secuirty)

ให้นักศึกษาเขียนโปรแกรมเข้ารหัสและถอดรหัสข้อความหรือไฟล์ ด้วยภาษา C/Python/Java/JavaScript เป็นต้น

ข้อกำหนด

- โปรแกรมจะใช้ AES ที่มี Key ขนาด 256 bits เข้ารหัสข้อความ (เอาเฉพาะ text มาเข้ารหัส) และไฟล์อื่น (เช่น PDF, JPG, Doc เป็นต้น)
- IV (Initialization vector) สำหรับ AES ใช้เป็น Random
- สามารถถอดรหัสกลับมาเป็นไฟล์เดิมได้ (มี function หรือ method ทั้งเข้ารหัสและถอดรหัส)
- ดังนั้นจะมีไฟล์ text 1 ไฟล์ และไฟล์ประเภทอื่น 1 ไฟล์ โดย
    1. ไฟล์ text จะมีข้อความเป็น รหัสนักศึกษา และชื่อสกุล ให้เอาแค่ข้อความในไฟล์ text มาเข้ารหัส พร้อม**ทำ Digital signature** ด้วย RSA ที่มี Key ขนาด 2048 bits (สร้าง Digital signature ให้ใช้ SHA512 และเซ็นด้วย Private key)
    2. ไฟล์อื่นๆ (เช่น PDF, JPG, Doc เป็นต้น) ให้เข้ารหัสไฟล์นั้นทั้งก้อน และ**ไม่ต้อง**ทำ Digital signature

สิ่งที่ต้องส่ง

1. Source code
2. Video แสดงการเข้ารหัสและถอดรหัสพร้อมอธิบายหลักการของโปรแกรม (ไม่เกิน 5 นาที)
3. Signature ของข้อความ
4. ไฟล์ต้นฉบับทั้ง 2 ไฟล์
5. ไฟล์หลังเข้ารหัส (ถ้าไฟล์ text ให้ระบุข้อความที่ถูกเข้ารหัส)