



OTP XOR Encryption

รายวิชา CP422031 Introduction to Cybersecurity
Section 2 Group 10

อาจารย์ประจำวิชา : ศ.ดร.จักรชัย โสอินทร์
อาจารย์ประจำวิชา : ผศ.ดร.สาริต กระเวนกิจ

100



หลักการและเหตุผล

เทคโนโลยีไร้สายมีบทบาทสำคัญในหลายอุตสาหกรรม เช่น IoT และ เครือข่ายเซ็นเซอร์ ช่วยเพิ่มประสิทธิภาพการทำงานแต่ยังมีความเสี่ยง ด้านความปลอดภัยจากการดักฟังและโจมตี โปรเจกต์นี้มุ่งศึกษาการ ส่งข้อมูลไร้สายอย่างปลอดภัย โดยใช้โมดูล **RF 433 MHz** และเข้ารหัส แบบ **One-Time Pad (OTP)** ซึ่งใช้การ **XOR** ข้อมูลกับกุญแจสุ่มที่ใช้เพียงครั้งเดียว ทำให้ถอดรหัสไม่ได้หากไม่มีกุญแจที่ตรงกัน

วัตถุประสงค์

- 1) ศึกษาการ **Encryption** และการ **Decryption** ข้อมูล
- 2) เพื่อพัฒนาการส่งข้อมูลบน **RF 433 MHz** ให้ความปลอดภัยมากยิ่งขึ้น
- 3) เพื่อศึกษาแนวทางการเข้ารหัสแบบ **One-Time Pad (OTP)** และการดำเนินการ **XOR** ในการป้องกันข้อมูล

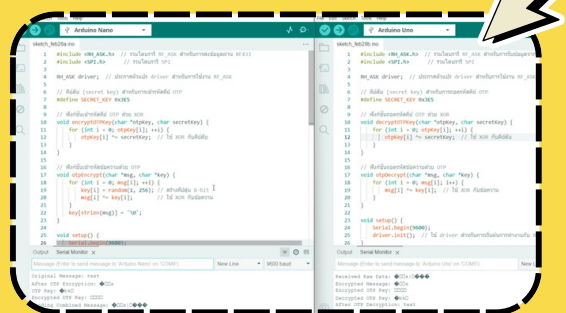
ขอบเขตการศึกษา

ศึกษาการส่งข้อมูลจากคอมพิวเตอร์ 2 เครื่อง ผ่านบอร์ด **Arduino Nano (ตัวส่ง)** ที่ทำการเข้ารหัส แบบ **OTP XOR** บน **RF 433 MHz** เพื่อเพิ่ม ความปลอดภัยในการส่งข้อมูลไปยัง **Arduino Uno R3 (ตัวรับ)** และทำการถอดรหัสข้อมูลที่ได้รับ

โปรเจกต์คืออะไร?

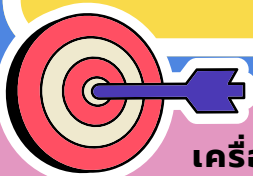
การส่งข้อความผ่านคลื่น **RF 433 MHz** โดยใช้ **Arduino** ในการเข้ารหัสและถอดรหัสแบบ **OTP XOR** ซึ่งทำให้มีความปลอดภัยมากยิ่งขึ้น

ตัวอย่างงาน

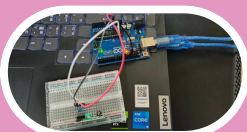


วิธีการใช้งาน

- 1) เชื่อมต่อสาย USB ระหว่างบอร์ด และคอมพิวเตอร์ทั้ง 2 เครื่อง
- 2) Import Code ลงในตัวบอร์ดทั้งตัวส่งและตัวรับจากนั้น Run Code
- 3) ส่งข้อความ



เครื่องมือที่ใช้



Hardware :

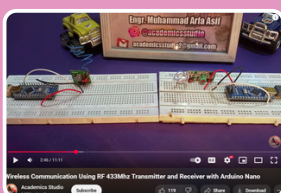
- Arduino Nano
- Arduino Uno R3
- USB RF 433 MHz
- ตัวต้านทาน
- Breadboard

Software :

- Arduino IDE



งานที่ใช้อ้างอิง



- <https://youtu.be/u86YCVu2MwYsi=MjM3uBUhh8vRZzuC>
- <https://projecthub.arduino.cc/abosalahpasha/wireless-communication-using-arduino-and-rf-module-fb186a>

GOOD

ฟังก์ชันการทำงาน

หลักการทำงานของ **OTP XOR** คือการสร้าง คีย์สุ่มที่มีขนาดเท่ากับข้อความ จากนั้นใช้การ **XOR** ระหว่างข้อความต้นฉบับและคีย์เพื่อเข้ารหัสข้อมูล เมื่อตัวรับได้รับข้อมูล จะใช้คีย์เดียวกันทำการ **XOR** อีกครั้งเพื่อถอดรหัส และกู้คืนข้อความเดิมได้อย่างสมบูรณ์ เพื่อเพิ่มความปลอดภัยมากขึ้น คีย์ที่ใช้จะถูกเข้ารหัสอีกครั้งหนึ่งก่อนส่งไปยังตัวรับ ทำให้แม้ว่ามีการดักฟังข้อมูล ก็ไม่สามารถนำคีย์ไปใช้ถอดรหัสได้โดยตรง วิธีนี้ช่วยเสริมความปลอดภัย กับการส่งข้อมูลไร้สายผ่าน **RF 433 MHz**

สรุปผล

การส่งข้อมูลที่ถูกเข้ารหัสด้วยวิธีการ **OTP XOR** ผ่านคลื่น **RF 433 MHz** โดยใช้ **Arduino Nano** เป็นตัวส่งและ **Arduino Uno R3** เป็นตัวรับ มีความปลอดภัยมากยิ่งขึ้นหากมีการจัดการคีย์อย่างเหมาะสม



สมาชิก

- | | |
|-------------|---------------------|
| 663380095-6 | กุลยา ศิริสม |
| 663380093-0 | กนกสร ศรีบัวบุญ |
| 663380099-8 | ชมพูนุช สุวรรณภักดี |
| 663380114-8 | นิติมา ผาภู |
| 663380130-0 | รุ่งฤดี พึ่งสว่าง |
| 663380460-9 | ธีรภัทร เภาฤทธิ์ |