| หมายเลขโครงงาน | |
|---|---|

# แบบฟอร์มขอบเขตโครงงาน TEAM-PROJECT 3

ชื่อภาษาไทย ระบบควบคุมการเข้าออกอัจฉริยะด้วย RFID Cryptographic Hashing

ชื่อภาษาอังกฤษ SMART ACCESS CONTROL SYSTEM WITH RFID CRYPTOGRAPHIC HASHING

โดย

นายกฤตนัย มุงคุณ รหัสนักศึกษา 66010021

นางสาวธัญญลักษณ์ เผยโคกกรวด รหัสนักศึกษา 66010366

อาจารย์ที่ปรึกษาหลัก

_____

( ผศ.มนต์ชัย แช่มช้อย ) ลงนามวันที่ _____/_____/_____

อาจารย์ที่ปรึกษาร่วม

_____

( ผศ.ดร.พิชญ สุพรรณกูล ) ลงนามวันที่ _____/_____/_____

**วัตถุประสงค์โดยคร่าวของการนำเสนอโครงงาน TEAM-PROJECT 3**

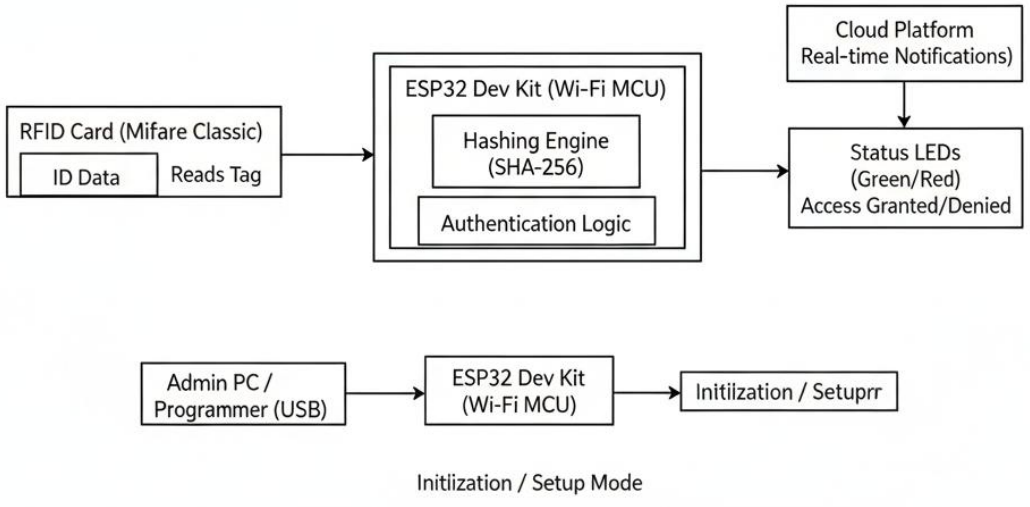
1. เพื่อออกแบบและพัฒนาระบบควบคุมการเข้า-ออกอัจฉริยะที่ใช้เทคโนโลยี RFID และการเข้ารหัสแบบแฮช (Cryptographic Hashing) เพื่อยกระดับความปลอดภัย
2. เพื่อประยุกต์ใช้ไมโครคอนโทรลเลอร์ ESP32 ในการประมวลผลอัลกอริทึมการแฮช (Hashing Algorithm) สำหรับการตรวจสอบสิทธิ์ข้อมูล ID จากบัตร RFID
3. เพื่อเพิ่มความปลอดภัยให้กับระบบ Access Control โดยการสร้างกลไกการตรวจสอบ "กุญแจจริง/กุญแจปลอม" ผ่านกระบวนการแฮชข้อมูลบนบัตร RFID
4. เพื่อแสดงผลสถานะการเข้าถึงระบบแบบไร้สายผ่านแพลตฟอร์ม Telegram หรือ Blynk โดยใช้ความสามารถด้าน Wi-Fi ของ ESP32
5. เพื่อวัดและวิเคราะห์ประสิทธิภาพของ ESP32 ในการประมวลผลอัลกอริทึมการแฮช SHA-256 เมื่อเทียบกับการประมวลผล ID แบบปกติ

| หมายเลขโครงงาน | |
|---|---|

## ขอบเขตของโครงงาน TEAM-PROJECT 3

1. สร้างต้นแบบระบบควบคุมการเข้า-ออกอัจฉริยะ (Smart Access Control Prototype) ที่ประมวลผลด้วยไมโครคอนโทรลเลอร์ ESP32 ซึ่งรองรับการเชื่อมต่อเครือข่ายไร้สาย (Wi-Fi)
2. พัฒนาอัลกอริทึมการตรวจสอบสิทธิ์ความปลอดภัยสูงด้วยวิธี Cryptographic Hashing (เช่น SHA-256) เพื่อใช้ในการตรวจสอบความถูกต้องของบัตร RFID และแยกแยะระหว่าง "กุญแจจริง" กับ "กุญแจปลอม"
3. ใช้โมดูลอ่านบัตร RFID (RC522) ย่านความถี่ 13.56 MHz เป็นอุปกรณ์รับข้อมูล และใช้ กลอนแม่เหล็กไฟฟ้า (Solenoid Lock) ขนาด 12V ร่วมกับวงจรรีเลย์ (Relay Module) เป็นอุปกรณ์ควบคุมการเปิด-ปิดประตูจริง
4. ออกแบบระบบการสื่อสารข้อมูลผ่านเครือข่ายอินเทอร์เน็ต เพื่อส่งแจ้งเตือนและรายงานสถานะการเข้า-ออก (Access Log) ไปยังแอปพลิเคชัน Telegram หรือ Blynk แบบ Real-time
5. วิเคราะห์และวัดผลประสิทธิภาพการทำงานของหน่วยประมวลผล (ESP32) ในด้านความเร็วและความถูกต้องของการประมวลผลอัลกอริทึมการเข้ารหัสเปรียบเทียบกับการอ่านข้อมูลแบบปกติ

## บล็อกไดอะแกรมของโครงงานที่นำเสนอ



| หมายเลขโครงงาน | |
|---|---|

## แผนการปฏิบัติงานตลอดภาคการศึกษา

| ช่วงการดำเนินงาน | แผนงานที่จะดำเนินการ | |
|---|---|---|
| **เดือนที่ 1 (ธ.ค. 2568)** | สัปดาห์ที่ 1 | ศึกษา ESP32 และเชื่อมต่อกับ RFID Reader (RC522) |
| | สัปดาห์ที่ 2 | ศึกษาและนำไลบรารี SHA-256 มาใช้งานบน ESP32 |
| | สัปดาห์ที่ 3 | พัฒนาระบบ Hash ข้อมูล ID จากบัตร และทดสอบการเปรียบเทียบ Hash |
| | สัปดาห์ที่ 4 | จัดทำและส่งรายงานความก้าวหน้าครั้งที่ 1 |
| **เดือนที่ 2 (ม.ค. 2569)** | สัปดาห์ที่ 1 | เชื่อมต่อ ESP32 กับ Wi-Fi และแพลตฟอร์ม Telegram/Blynk |
| | สัปดาห์ที่ 2 | พัฒนาระบบแสดงสถานะผ่าน LED และรวมเข้ากับกลไก Hash |
| | สัปดาห์ที่ 3 | พัฒนากลไก "กุญแจจริง/กุญแจปลอม" ด้วยเงื่อนไขการ Hash |
| | สัปดาห์ที่ 4 | จัดทำและส่งรายงานความก้าวหน้าครั้งที่ 2 |
| **เดือนที่ 3 (ก.พ. 2569)** | สัปดาห์ที่ 1 | การทดลองหลัก: วัดประสิทธิภาพการประมวลผล SHA-256 บน ESP32 |
| | สัปดาห์ที่ 2 | ทดสอบความเสถียรของระบบ (Stability Test) และการเชื่อมต่อ Wi-Fi |
| | สัปดาห์ที่ 3 | ปรับปรุงCode ให้มีประสิทธิภาพ และทำความสะอาดวงจร/ติดตั้งอุปกรณ์ |
| | สัปดาห์ที่ 4 | จัดทำและส่งรายงานความก้าวหน้าครั้งที่ 3 |
| **เดือนที่ 4 (มี.ค. 2569)** | สัปดาห์ที่ 1 | สรุปผลการทดลอง วิเคราะห์วิจารณ์ผล และเปรียบเทียบกับวัตถุประสงค์ |
| | สัปดาห์ที่ 2 | ตรวจสอบความถูกต้องของเล่มรายงานและจัดเตรียมสื่อนำเสนอ |
| | สัปดาห์ที่ 3 | จัดทำและส่งรายงานฉบับสมบูรณ์ |

## หมายเหตุ

รายงานความก้าวหน้าที่จะมีกำหนดส่งของทุกๆเดือน ตามประกาศของภาควิชาฯ โดยในรายงานจะต้องมีหลักฐานผลการดำเนินงานเชิงประจักษ์ เช่น ผลการทดลอง ผลการทดสอบ และสอดคล้องตามแผนการปฏิบัติงานที่ได้แสดงไว้

| หมายเลขโครงงาน | |
|---|---|

# บทคัดย่อโครงงาน TEAM-PROJECT 3

ชื่อภาษาไทย ระบบควบคุมการเข้าออกอัจฉริยะด้วย RFID Cryptographic Hashing

ชื่อภาษาอังกฤษ SMART ACCESS CONTROL SYSTEM WITH RFID CRYPTOGRAPHIC HASHING

## บทคัดย่อ

โครงงานฉบับนี้นำเสนอการออกแบบและพัฒนาระบบควบคุมการเข้า-ออกอัจฉริยะที่ประยุกต์ใช้เทคโนโลยีการเข้ารหัสแบบแฮช (Cryptographic Hashing) เพื่อยกระดับความปลอดภัยในการระบุตัวตนผ่านคลื่นวิทยุ (RFID) และรองรับการเชื่อมต่อผ่านเครือข่ายไร้สาย วัตถุประสงค์หลักของโครงงานคือการแก้ไขปัญหาความเสี่ยงจากการปลอมแปลงบัตร (Card Cloning) ในระบบควบคุมประตูทั่วไป โดยนำไมโครคอนโทรลเลอร์ ESP32 มาเป็นหน่วยประมวลผลหลักในการตรวจสอบความถูกต้องของข้อมูลด้วยอัลกอริทึม SHA-256 องค์ประกอบของระบบประกอบด้วยโมดูลอ่านบัตร RFID ย่านความถี่ 13.56 MHz และชุดควบคุมประตูด้วยกลอนแม่เหล็กไฟฟ้า (Solenoid Lock) ที่ควบคุมผ่านวงจรรีเลย์ โดยมีหลักการทำงานเริ่มจากการอ่านข้อมูลระบุตัวตนจากบัตรและนำไปผ่านกระบวนการคำนวณค่าแฮชเพื่อเปรียบเทียบกับฐานข้อมูลสิทธิ์ที่กำหนดไว้ หากค่าแฮชถูกต้องระบบจะสั่งการให้กลอนประตูปลดล็อก พร้อมทั้งส่งข้อมูลแจ้งเตือนและรายงานสถานะการเข้า-ออก (Access Log) แบบเรียลไทม์ไปยังแอปพลิเคชัน Telegram หรือ Blynk ผ่านการเชื่อมต่อ Wi-Fi ผลการดำเนินงานแสดงให้เห็นว่าระบบสามารถแยกแยะระหว่างบัตรจริงและบัตรที่ถูกทำสำเนาได้อย่างแม่นยำ และสามารถควบคุมการเปิด-ปิดประตูพร้อมรายงานผลผ่านเครือข่ายไร้สายได้อย่างมีประสิทธิภาพ ช่วยเพิ่มความสะดวกและความปลอดภัยในการบริหารจัดการระบบควบคุมการเข้า-ออก

| หมายเลขโครงงาน | |
|---|---|


## Abstract

This project presents the design and development of a Smart Access Control System utilizing Cryptographic Hashing technology to enhance security in Radio Frequency Identification (RFID) authentication and support wireless connectivity. The primary objective is to address the vulnerabilities of RFID card cloning in conventional access control systems by implementing a verification mechanism using the SHA-256 hashing algorithm on the ESP32 microcontroller. The system components include a 13.56 MHz RFID reader module and an electric solenoid lock controlled by a relay driver circuit. The operation involves retrieving the identification data from the RFID card, computing its hash value, and verifying it against an authorized database. Upon successful authentication, the system activates the solenoid lock to grant access and transmits real-time notifications and access logs to the Telegram or Blynk application via Wi-Fi connection. The results demonstrate that the system accurately distinguishes between authentic and cloned cards while effectively controlling physical access and reporting status via the wireless network, thereby significantly improving both security and convenience in access control management.