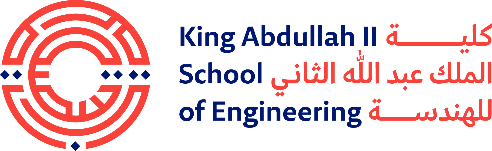
Princess Sumaya University for Technology

King Abdullah II Faculty of Engineering

Electrical Engineering Department



|  |
| --- |
| **RFID Killer** |

|  |  |  |  |
| --- | --- | --- | --- |
| *Authors:* |  |  |  |
| *Student Name: Zaid Taha*  *Mohammad Elayyan*  *Omar Hamada* | *Student No.:*  *20190708*  *20200931*  *20191016* | *Specialization:*  *Computer Engineering*  *Computer Engineering*  *Computer Engineering* | *Email:*  [*Zai20190708@std.psut.edu.jo*](mailto:Zai20190708@std.psut.edu.jo)  [*Moh20200931@std.psut.edu.jo*](mailto:Moh20200931@std.psut.edu.jo)  [*Oma20191016@std.psut.edu.jo*](mailto:Oma20191016@std.psut.edu.jo) |

*November 21, 2022*

Introduction:

Typical “smart” doors these days depend on Magnetic Stripe Cards, RFID Card, or NFC tags. Unfortunately, all of these options suffer from major design flaw, they all “willingly” transmit data (The secret key/pin to open the door in this case) in **plain-text**. Adversaries or Threat Actors can easily clone/copy by these cards (by simply reading them!) to unlock doors and gain unauthorized access. This type of attack is referred to as the “Replay Attack”. This project offers a fundamental solution to the problem by replacing these cards with a “smart key” containing an embedded micro-controller inside. The project will utilize **AES encryption** and an authentication technique inspired by the **Kerberos protocol,** a widely adopted standard for authenticating Windows Computers in Corporation/Enterprise Networks, **Kerberos** was designed to defeat Man-in-the-middle/Replay/Cloning Attacks.

As explained previously, the root problem to be tackled is eliminating the need to send the secret pin/key in plain-text (which can be sniffed or cloned) to the Door Lock Reader. The project proposes a solution by replacing the authentication method with a more-secure version. Instead of transmitting the secret pin, both door and key will use the secret pin to encrypt and decrypt authentication "challenges". The smart key has embedded micro-controller inside which would be powered by the Door Lock. This technique is used to power up microprocessors under the golden chip in SIM cards and VISA/Mastercard. This way the attacker can’t retrieve the secret pin by sniffing/reading the in/outgoing requests and responses.

Diagrams:

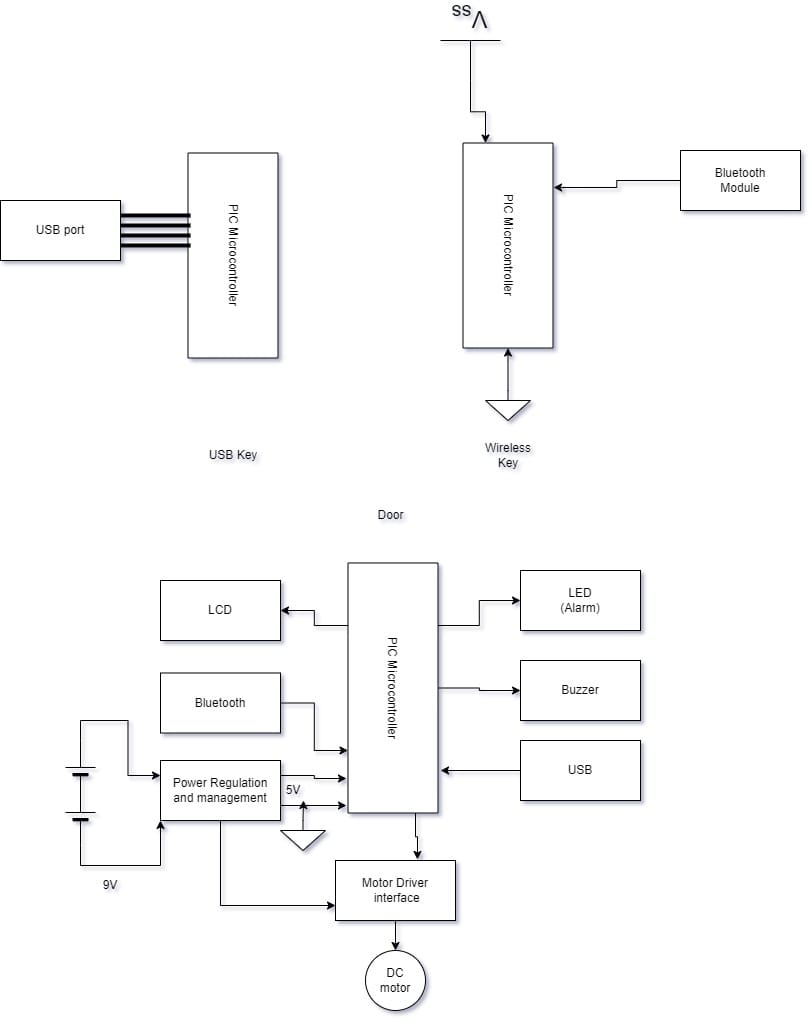
As it can be observed from figure1 this project will use PIC microcontroller as the main processing unit for the “Challenge” word between the key and the door, there is two main concepts for the key first a wired key, by connecting the PIC microcontroller with a USB port through the 4 ports that are attached to the USB port (VCC, GND, TDX, RDX).

Figure 1:Design Block Diagram

The second concept will be a wireless key using a Bluetooth module then transmitted through another that is attached to the door through serial communication.

Also, the door has its own components such as DC motor to open and close the door after solving the challenge word as described in the introduction, a power management unit in case a higher voltage was added to the circuit and since the PIC microcontroller only accepts 5V , and of course the is a Bluetooth module so it can communicate with the wireless key (in case the wireless key was the main key concept), the rest of the components is used as an indicator for the user that the door was open successfully or not; like the LCD screen that will show pass if its correct and access denied if not, an LED light will be added also if false entry was added it will turn red, if its true it will be green, a buzzer was added to the door components as an accessibility feature for people with visual problems. Last and not least there is the USB port to connect to the wired key (in case the wired key was the main concept to be used with the project), the Bluetooth module that is connected to the door is also will be a way to communicate with a mobile phone through an application that we will develop using Flutter framework and firebase.

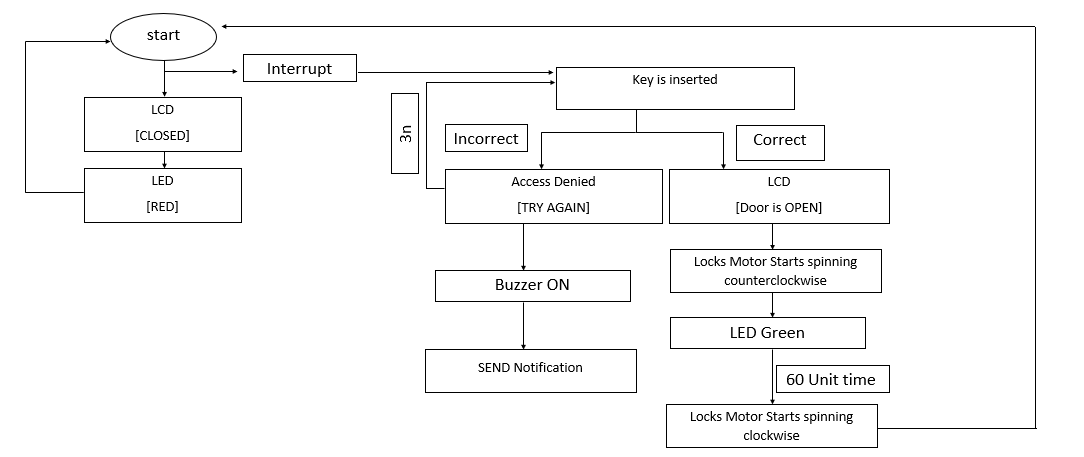


Figure 2: Program flow for the project

In the above figure we explain the main program flow that our project will follow, as it can be noticed the door will be always in a ready state waiting for an interrupt form the user by inserting the key, after that the program will leave the main function and go to the unlock function, there is two cases for that first if it is true it will pass and the door will open and the LED will turn green, then it will send a notification to the user that the door have been unlocked, if not it will give access denied on both the mobile phone and the LCD that attached to the door module . after a period of time (60 seconds) the door will close automatically by rotating the DC motors and then go back to the main function of the program.

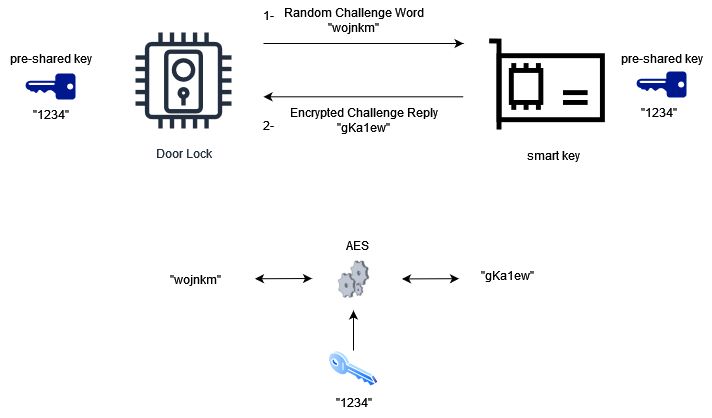


Figure 3:the mechanism of how the system works

Figure3 shows how will both the key and the door work with each to achieve the specified goal of the entire project.

Components:

* DC MOTOR: <https://mikroelectron.com/Product/DC-motor-with-encoder-disk-41-lines/> 10 JD
* 3 PIC16F877A: <https://mikroelectron.com/Product/PIC16F877A-Original/> 10.5JD/piece
* 2 Bluetooth modules: <https://mikroelectron.com/Product/HC-06-Wireless-Bluetooth-Module-TTL-normal-Quality/> 7.5JD/piece
* RGB LED: <https://mikroelectron.com/Product/RGB-LED-Common-Anode-5MM/> 0.25JD/piece
* Buzzer: <https://mikroelectron.com/Product/5V-Magnetic-Buzzer/> 0.4JD/piece
* LCD: <https://mikroelectron.com/Product/LCD-16x2-Blue-Screen/>3JD/piece or <https://mikroelectron.com/Product/128x64-OLED-0-96-inch-Display-Module-4-pin-Blue/> 7JD/piece
* 2 USB port: <https://mikroelectron.com/Product/USB-to-DIP-Adapter-Converter-4-pin-for-2-54mm-PCB-Board-Power-Supply/> 1JD/piece
* VOLTAGE REGULATOR: <https://mikroelectron.com/Product/Voltage-Regulator-7805-5V/> 0.5JD/piece

***Estimated total cost:***

***50JD – 75JD***