BLM4021 Gömülü Sistemler
Laboratuvar Projesi Final Raporu

Grup No: 27

Proje Kategorisi:11

Kişilerin Çalışma Yüzdesi:

Grup Sorumlusu :	**Mevlana Halit Kaya**	**25**	**Yazılım Rapor Yazımı**
	Ahmet Zahit Can	25	**Ekip Lideri, Yazılım, Donanım**
	Ömer Fazıl Yürük	25	**Yazılım, Rapor Yazımı**
	Bedrettin Şamil Öztürk	25	**Donanım, Rapor Yazımı**

İçerik

I. Giriş ve Proje Tanıtımı

Projemizde bir gömülü sistem uygulaması gerçekleştirilmiştir. Gömülü sistemler, belirli bir görev için tasarlanmış, özel bir işlemciye sahip ve genellikle birincil bir sistem tarafından kontrol edilen sistemlerdir. Gömülü sistemler, birçok farklı alanda kullanılabilir ve genellikle birincil sistemlerin bir parçası olarak tasarlandıklarından küçük boyutludur. Örnekleri arasında, bir akıllı telefonun işlemcisi, bir otomobilin motor kontrol birimi ve bir beyaz eşyada bulunan programlanabilir denetleyiciler sayılabilir. Gömülü sistemler, günlük hayatımızda sıklıkla kullandığımız birçok cihazda bulunur ve bu cihazların işlevselliğini sağlarlar. Projemizde bir network uygulaması olarak Wifi şifre bulucu gerçekleştirme seçildi.

Bu projede, Raspberry Pi 1 kullanıldı. Raspberry Pi, küçük boyutu ve yüksek işlem gücü sayesinde gömülü sistemler alanında sıklıkla kullanılan bir cihazdır. Bu cihazın konfigürasyonu yapılarak, proje isterlerine uygun bir şekilde kullanıldı, Raspberry pi kurulumları gerçekleştirildi. Bir Wifi adaptör kullanarak çevredeki ağlar dinlendi. Ağlar bulunduktan sonra bunlar yazmış olduğumuz tasarım arayüzü ile ekranımızda gösterildi. Bu ekranda ağları seçmemize yarayan butonlar ile saldırı gerçekleştireceğimiz ağı seçerek şifre bulma işlemine geçildi.
Burada Python dili yazdığımız kod ile şifre bulma işlemi uygulandı.

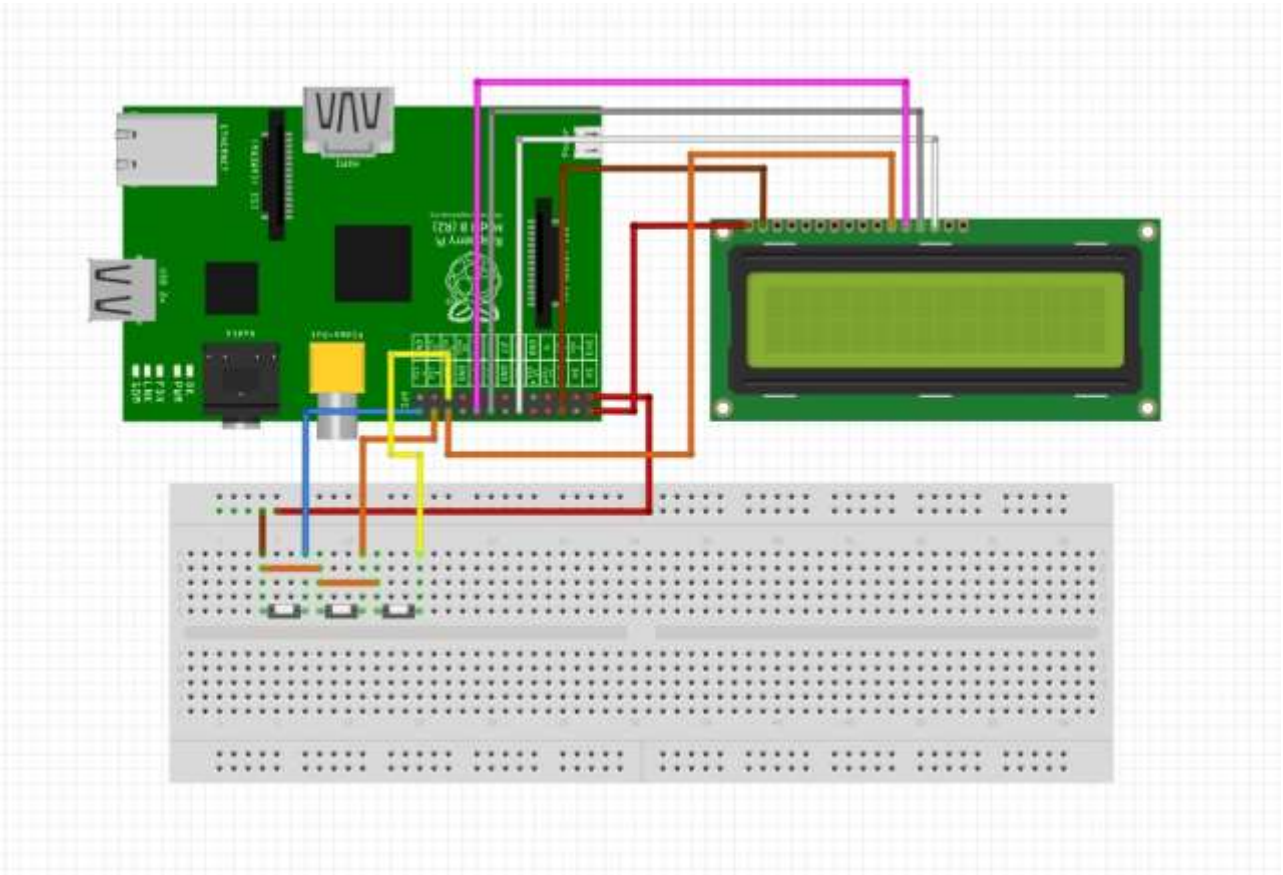
Bu algoritmada sözlük saldırısı ile Brute-Force yöntemi kullanılarak olabilecek olasılıklar tek tek denendi. Sözlük saldırısı, bir ağa giriş yapmaya çalışan bir kişinin ya da bir programın, bir sözlük dosyasında bulunan kelimeleri kullanarak ağın parolasını tahmin etmeye çalışmasıdır. Bu saldırı yöntemi, parolanın kelime değerlerini kullanarak parolayı bulmaya çalışır. Eğer parola kelime değerlerinden birine uygunsa, sözlük saldırısı başarılı olur ve ağa giriş yapılabilir. Ancak, parola kelime değerlerinden birine uymuyorsa, sözlük saldırısı başarısız olur ve ağa giriş yapılamaz.

Sözlük saldırısı yöntemi, parolanın kelime değerlerinden birine uygun olma olasılığına göre düşük başarı oranına sahiptir. Projemizde de adaptör tarafından bulunan ağlar arasında butonlar ile saldırı yapılacak olan ağın seçimi yapılarak bahsedilen sözlük saldırısı ile şifre bulunmaya çalışıldı. Eğer şifre bulunmuşsa sonuç ekranda gösterildi.

II. *Fritsing* ile Ön Tasarım

Projemize ait Fritsing tasarımı aşağıdaki gibidir. Raspberry Pi-1, breadboard ve kullandığımız ekran, tasarımda yer almaktadır. Raspberry Pi'nin GPIO (General Purpose Input/Output) pinleri Raspberry Pi'nin dış ortam ile etkileşim kurmasını sağlıyor ve çeşitli sensörler, aktüatörler ve diğer elektronik cihazların bağlanmasına olanak verir. [1]

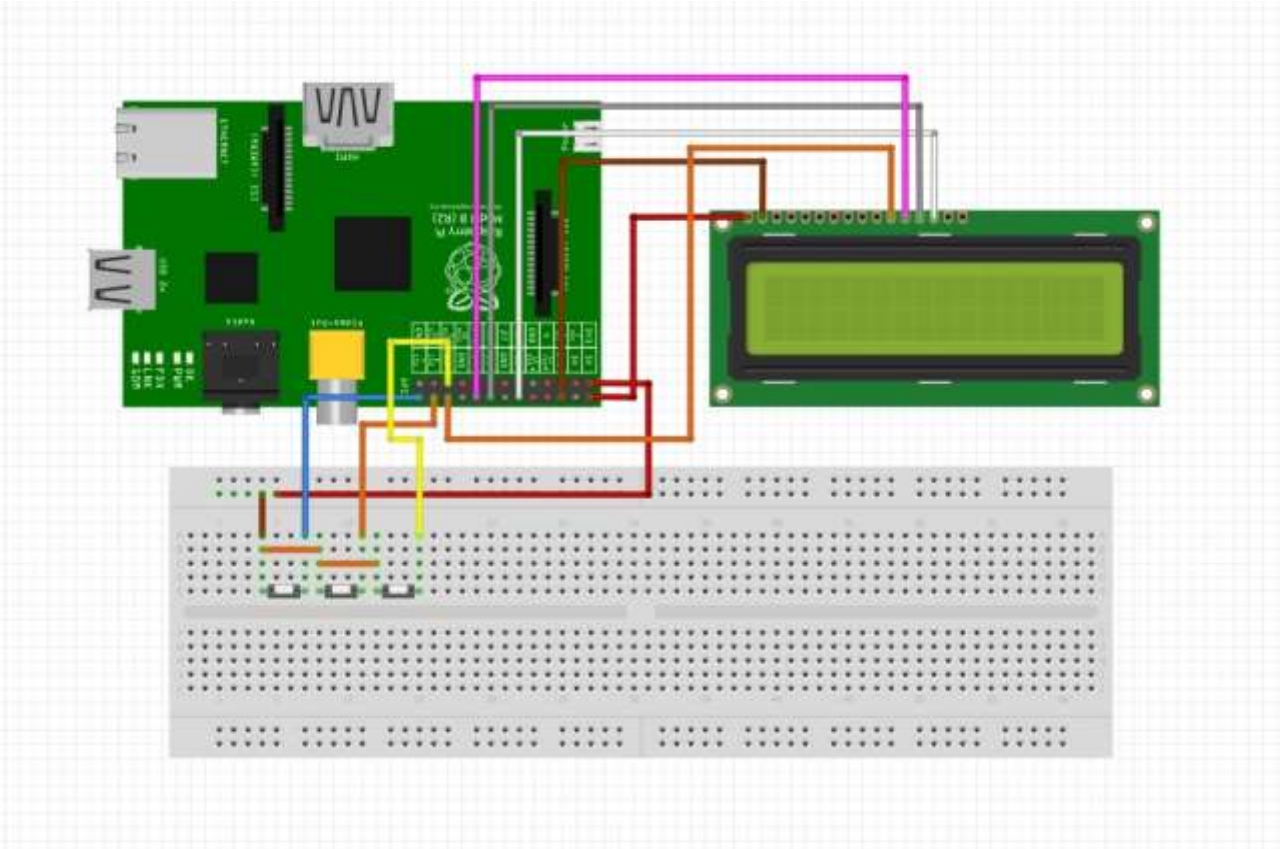
GPIO pinleri breadboard üzerinde bağlanarak, Raspberry Pi'nin diğer elektronik cihazlar ile haberleşmesini sağlandı. Breadboard ile elektronik parçaları denenmesi gerçekleştirildi. Bu sayede, Raspberry Pi'nin GPIO pinlerini breadboard üzerinde bağlayarak, projenin gerçekleşmesi sağlandı.



Şekil 1: *Fritsing tasarımı*.

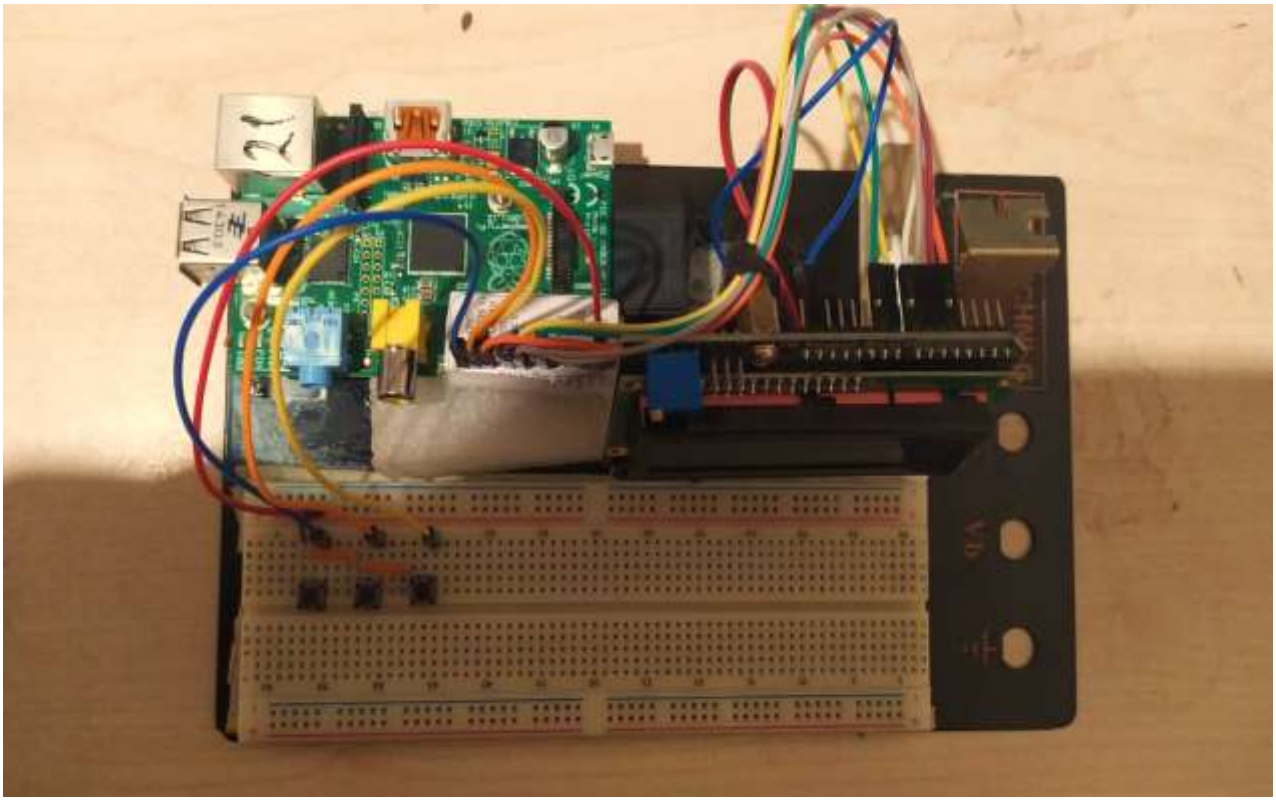
Kullanmış olduğumuz raspberry modeli: Rasperry Pi-1 Model B Revizyon 2
Kullanmış olduğumuz pinler: GPIO 7-8-9-14-15-17-18-22-23-24-25.
Kullanmış olduğumuz ekran: 2x16 LCD ekrandır.

III. Kurulan Devre Detayları



Fritsing kısmında da yer vermiş olduğumuz tasarım bu şekildedir. Bu tasarım üzerinden gerçekleştirdiğimiz projemizin görüntüsü ise **Şekil 2**'de aşağıda yer verilmiştir.

Devre kurulumu sırasında karşılaşılan bir sorun ekranda bulunan butonlarda gerçeklenmiştir. Ekranda bulunan butonlar tek bir pine bağlı durumdadır. Bu butonların basılmasıyla volt derecelerinin ölçülmesi gerektiğinden bunun için ayrı bir analog to digital converter gerekmekteydi. Bunun yerine 3 ayrı buton ekleyerek sorunu çözdük. Ayrıca bu şekilde yaptığımız çözüm kullanım açısından daha uygun ve kolay olmuş oldu.



Şekil 2: *Projenin canlı devre görüntüsü*

Kullanmış olduğumuz pinler: GPIO 7-8-9-17-18-22-23-24-25.
Bu pinlerin kullanımı şu şekildedir:

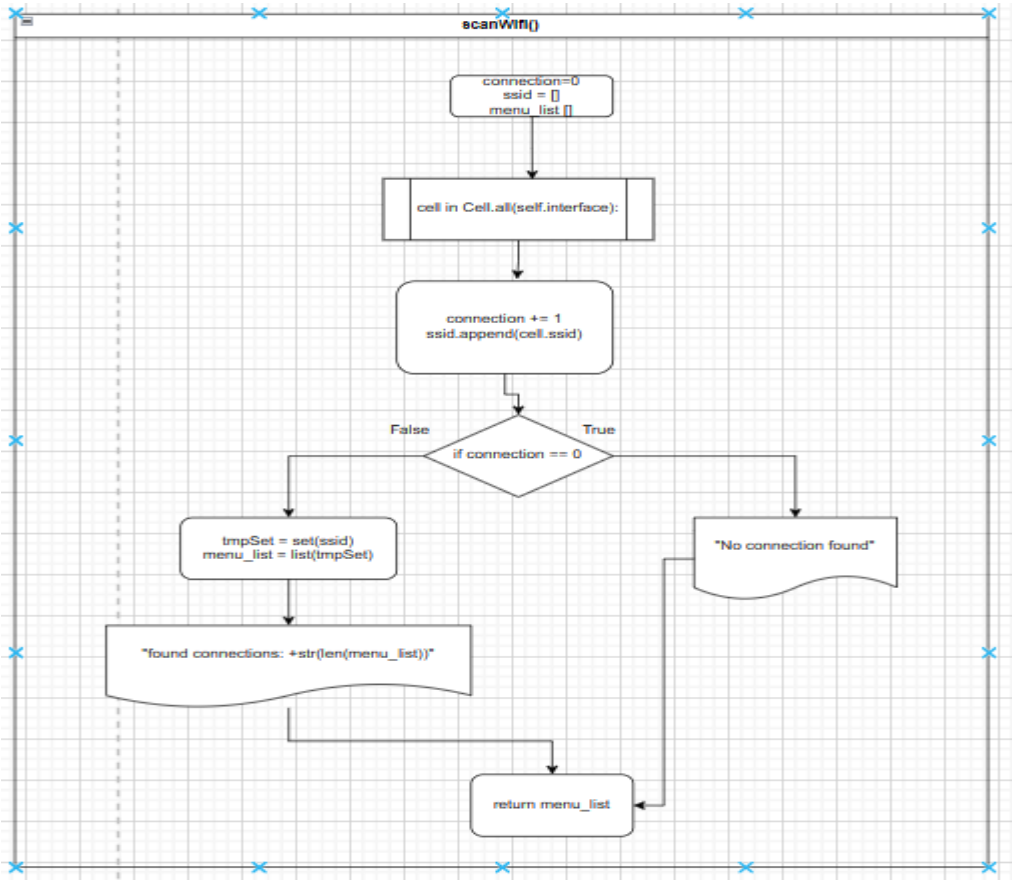
GPIO 7: Select butonu için kullanılmıştır.
GPIO 8: Next butonu için kullanılmıştır.
GPIO 9: Reset butonu için kullanılmıştır.
GPIO 17: Lcd_en pini için kullanılmıştır. Bu pin veri yazma aktifleştirme için kullanılır.
GPIO 18: Lcd_d7 pini için kullanılmıştır.
GPIO 22: Lcd_rs pini için kullanılmıştır. Bu pin komutlardan veri ayırmak için kullanılır.
GPIO 23: Lcd_d6 pini için kullanılmıştır.
GPIO 24: Lcd_d5 pini için kullanılmıştır.
GPIO 25: Lcd_d4 pini için kullanılmıştır.

-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-

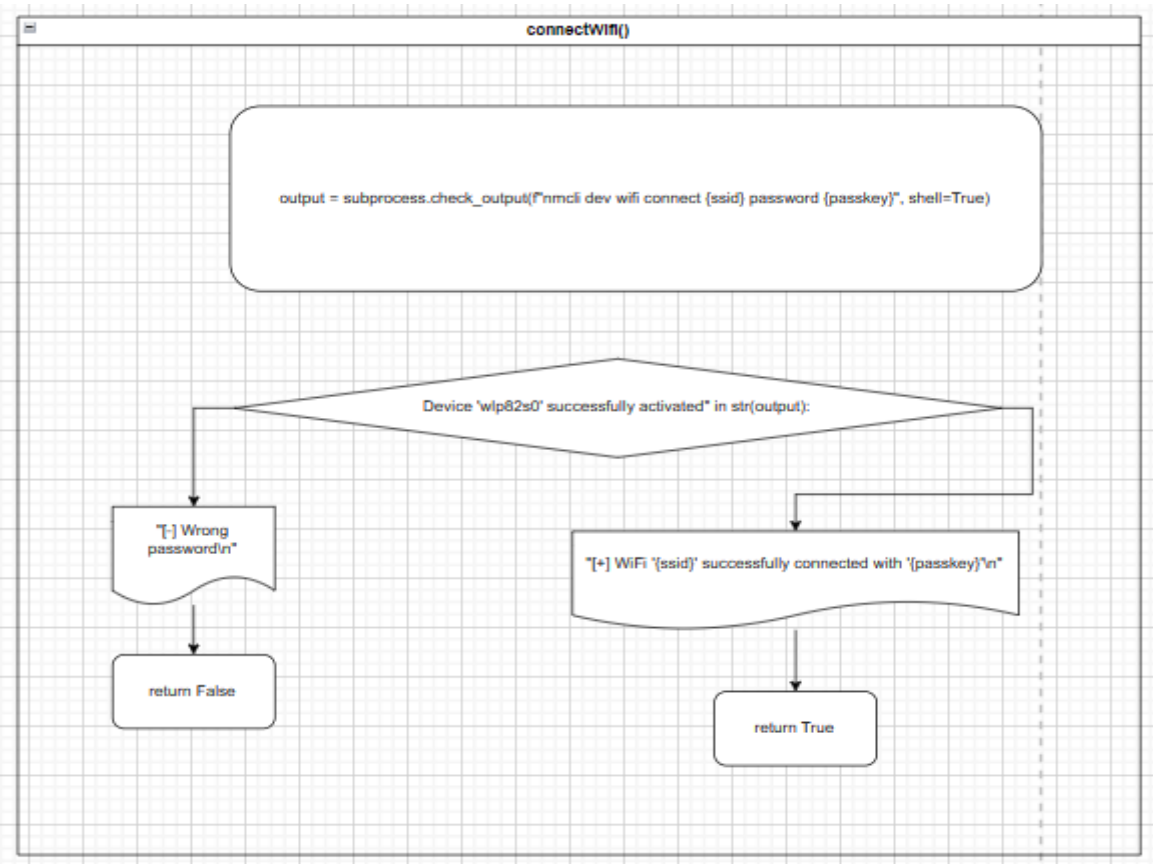
IV. Yazılım Tasarımı

Projemizde kullandığımız yazılım Wifi adaptör ile bulunan ağa sözlük saldırısı yöntemi uygulayarak ağın şifresini bulmaya yöneliktir. Yazılım dili olarak Python dilini kullanıldı. Kodda 5 adet Python dosyası bulunmaktadır. Bu dosyalar şu şekilde ayrışmaktadır: Butonlar için, LCD için, wifi şifre bulma için ayrı olarak yazılmıştır. Bu dosyalar main.py adlı dosyadan kontrol edilmekte ve program bu kod üzerinden çalıştırılmaktadır. Wifi şifre bulma kodunun yaptığı işlem adaptörün bulduğu bütün ağlara Brute-Force yöntemi uygulayarak sözlük listesinde bulunan bütün şifrelerin tek tek denenmesiyle gerçekleşmektedir.

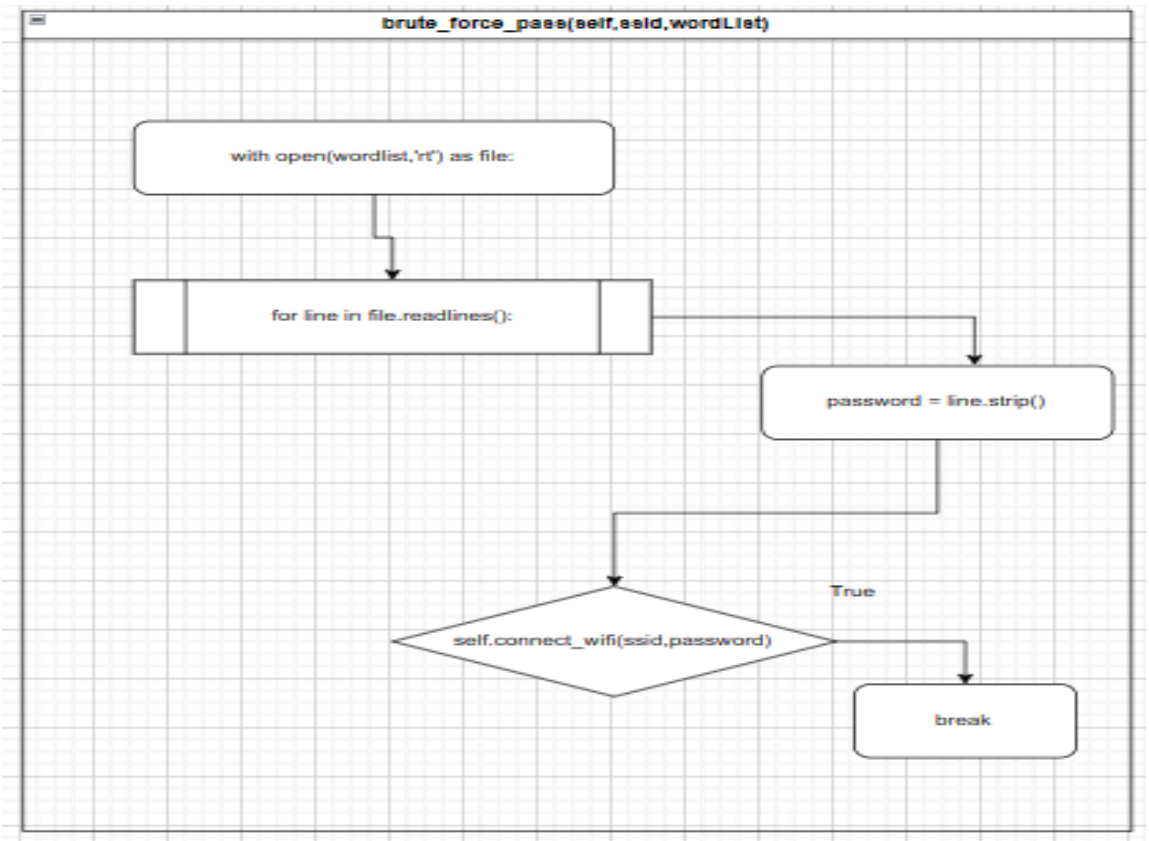
Wifi şifresini bulma dosyasındaki kodun çalışmasını gösteren flowchart aşağıdaki **Şekil 3**'teki gibidir.



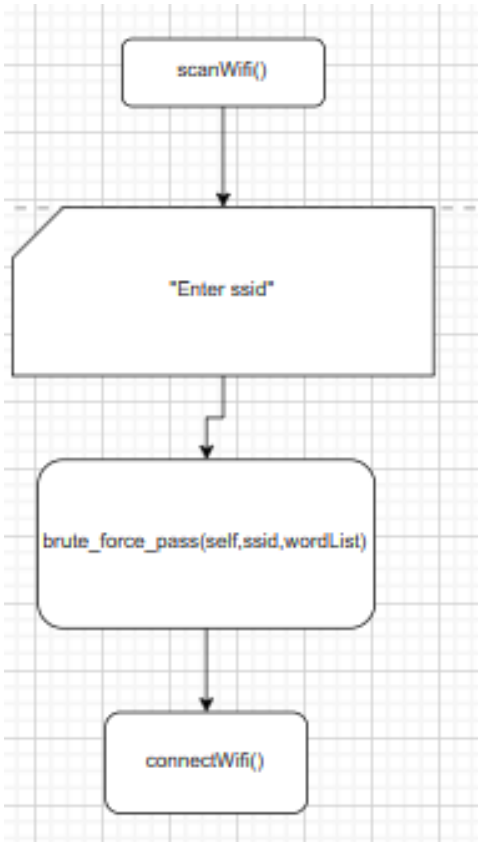
Şekil 3: *scanWifi() fonksiyonu flowchart'ı.*



Şekil 4: *connectWifi() fonksiyonu flow chart'ı.*



Şekil 5: *brute_force_pass() fonksiyonu flow chart'ı.*



Şekil 6: *Fonksiyonların çağırılmasını gösteren flowchart.*

Şifre dosyasının okunup denenmelerin gerçekleştirildiği kod parçacığı bu şekildedir:

```
with
open(f"{os.path.dirname(__file__)}/passwords.txt",'rt'
) as file:

for line in file.readlines():

password = line.strip()

cprint(f"Attempting password: {password}", "yellow")

lcd.message(f"Attempting...", password)

if wifi.connect_wifi(ssid,password):

success = True

break

sleep(10)
```

Butonların çalışmasını sağlayan kod dosyasında ise GPIO modu seçilerek butonlar için olan pinler input ve pud_down modunda ayarlanmaktadır.

```
GPIO.setmode(GPIO.BCM)
GPIO.setup(sel_pin, GPIO.IN, GPIO.PUD_DOWN)
GPIO.setup(dwn_pin, GPIO.IN, GPIO.PUD_DOWN)
GPIO.setup(rst_pin, GPIO.IN, GPIO.PUD_DOWN)
```

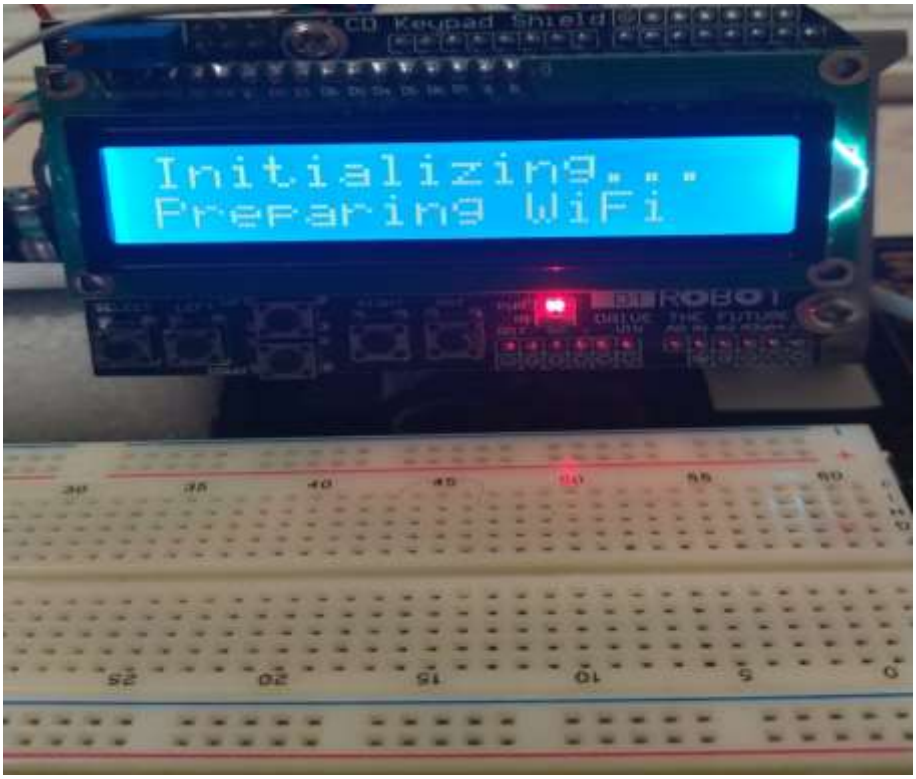
LCD kod dosyasında ise LCD ekranın iki satırda olması ve pinler aşağıdaki gibi ayarlanmıştır:

```
lcd_columns = 16
lcd_rows = 2
lcd_rs = digitalio.DigitalInOut(board.D22)
lcd_en = digitalio.DigitalInOut(board.D17)
lcd_d4 = digitalio.DigitalInOut(board.D25)
lcd_d5 = digitalio.DigitalInOut(board.D24)
lcd_d6 = digitalio.DigitalInOut(board.D23)
lcd_d7 = digitalio.DigitalInOut(board.D18)
```

-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o

V. Sonuçlar, Demo Detayları ve Sunum Linki

Projemizin gerçekleşme sırasından ve sonuç ekranından görüntüler aşağıdaki gibidir: Öncelikle programın çalışması ile ilkleme işlemleri gerçekleniyor. Tarama işlemlerinden sonra saldırı yapılacak ağın seçiminden sonra şifre denenmesi gerçekleniyor. Daha sonra şifre bulunursa başarı mesajı ekranda gösteriliyor. Bu aşamalara ait görüntüler hem aşağıdaki ekran görüntülerinde hem de video linkinde mevcuttur.



Şekil 7: *Programın çalışmaya başlaması*.

Şekil 8: *Wifi ağlarının taranması*.

Şekil 9: *Saldırı yapılacak ağın seçilmesi*.

Şekil 10: *Saldırı yapılacak ağa şifrelerin denemesi*.

Şekil 11: *Başarılı sonucun gösterilmesi*.

Video Linki: https://youtu.be/NF43HL-K-lk

-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-

VI. Referanslar

[1] https://en.wikipedia.org/wiki/Raspberry_Pi

-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o-o