Deneyap Kart ile Kriptolu Mesajlaşma: Adım Adım Rehber

Bu rehber, Deneyap Kart 1A ve 1A v2 kullanarak iki kart arasında güvenli mesaj iletimi yapan bir projeyi sıfırdan kurmanız için hazırlanmıştır. Projemizde, bir kart (gönderici) "MERHABA" gibi bir mesajı şifreleyerek diğer karta (alıcı) ESP-NOW protokolüyle gönderir. Alıcı, mesajı çözer ve seri porta yazdırır. Güvenlik için AES-CTR şifreleme ve HMAC doğrulama kullanılır.

Gereksinimler

Donanım

- **2 adet Deneyap Kart (1A veya 1A v2)**: Birisi gönderici, diğeri alıcı olacak.
- **2 adet USB kablosu**: Kartları bilgisayara bağlamak için (mikro USB veya USB-C, kartınıza bağlı).
- **Bilgisayar**: Deneyap Kart IDE'yi çalıştırabilecek bir Windows, Mac veya Linux bilgisayarı.

Yazılım

- **Deneyap Kart IDE**: Deneyap Kartları programlamak için kullanılacak. Deneyap Kart IDE'yi buradan indirin.
- **mbedtls Kütüphanesi**: Şifreleme işlemleri için. Deneyap Kart IDE üzerinden yüklenecek.
- **Deneyap Kart Desteği**: IDE ile birlikte otomatik gelir, ekstra kurulum gerekmez.

Ön Bilgi

- Hiçbir programlama veya elektronik bilgisi gerekmez. Her adımı sıfırdan açıklayacağız.
- Sabırlı olun ve her adımı dikkatlice uygulayın. Hata yaparsanız, geri dönüp kontrol edin.

Adım 1: Deneyap Kart IDE'yi Kurun

1. **Deneyap Kart IDE'yi indirin**:
    - Deneyap Kart resmi sitesine gidin.
    - İşletim sisteminize uygun sürümü seçin (Windows, Mac veya Linux).
    - İndirilen dosyayı çalıştırarak kurulum talimatlarını takip edin.
2. **Deneyap Kart IDE'yi açın**:
    - Kurulum tamamlandıktan sonra programı başlatın. Boş bir kod penceresi (sketch) göreceksiniz.

Adım 2: Deneyap Kart Desteğini Doğrulayın

Deneyap Kart IDE, Deneyap Kart 1A ve 1A v2 için gerekli desteği varsayılan olarak içerir. Ancak, doğru çalıştığından emin olalım:

1. **Deneyap Kart IDE'yi açın**.
2. **Araçlar > Kart** menüsüne gidin.
3. **Deneyap Kart 1A** veya **Deneyap Kart 1A v2**'nin listede göründüğünü kontrol edin.
    - Eğer görünmüyorsa, IDE'yi yeniden yükleyin veya Deneyap Kart destek ekibine ulaşın.

Adım 3: mbedtls Kütüphanesini Yükleyin

Şifreleme için **mbedtls** kütüphanesine ihtiyacımız var. Deneyap Kart IDE üzerinden yükleyeceğiz:

1. **Deneyap Kart IDE'yi açın**.
2. **Araçlar > Kütüphaneleri Yönet** (Manage Libraries) menüsüne gidin.
3. Arama çubuğuna **mbedtls** yazın.
4. **mbedtls** kütüphanesini bulun ve **Yükle** (Install) butonuna tıklayın.
5. Yükleme tamamlandıktan sonra kütüphane otomatik olarak kullanılabilir olacak.

Adım 4: Donanımı Hazırlayın

1. **Deneyap Kartları kontrol edin**:
    - Elinizde 2 adet Deneyap Kart (1A veya 1A v2) olduğundan emin olun.
    - Kartlardan biri **gönderici**, diğeri **alıcı** olacak.
2. **USB kablolarını bağlayın**:
    - Her iki kartı da USB kablolarıyla bilgisayara bağlayın.
    - Kartların üzerindeki LED'lerin yandığını kontrol edin (bu, kartların çalıştığını gösterir).
3. **Kartları etiketleyin** (isteğe bağlı):
    - Karışıklığı önlemek için bir kartı "Gönderici", diğerini "Alıcı" olarak işaretleyin (örneğin, bir etiket yapıştırarak).

Adım 5: Alıcı Kartın MAC Adresini Bulun

Gönderici kartın, alıcı kartın MAC adresini bilmesi gerekiyor. Bunu bulmak için önce alıcı kodunu yükleyeceğiz.

1. **Alıcı kartı bilgisayara bağlayın**:
    - USB kablosuyla alıcı kartı bilgisayara takın.
2. **Deneyap Kart IDE'de kartı seçin**:
    - **Araçlar > Kart** menüsünden **Deneyap Kart 1A** veya **Deneyap Kart 1A v2**'yi seçin (kartınıza göre).
    - **Araçlar > Port** menüsünden kartın bağlı olduğu portu seçin (örneğin, COM3 veya /dev/ttyUSB0).
3. **Geçici bir kod yükleyin**:

Aşağıdaki kodu kopyalayın ve Deneyap Kart IDE'de yeni bir sketch'e yapıştırın:

```
#include <WiFi.h>
void setup() {
  Serial.begin(115200);
  WiFi.mode(WIFI_STA);
  Serial.println("Alıcı kart MAC adresi:");
  Serial.println(WiFi.macAddress());
}

void loop() {}
```

4. **Kodu yükleyin**:
    - **Dosya > Yükle** (File > Upload) butonuna tıklayın.
    - Yükleme sırasında hata alırsanız, kartın doğru bağlandığından ve portun seçildiğinden emin olun.
5. **Seri monitörü açın**:
    - **Araçlar > Seri Monitör** menüsüne gidin.
    - Baud hızını **115200** olarak ayarlayın.
    - "Alıcı kart MAC adresi:" ile başlayan bir satır göreceksiniz, örneğin:
      `Alıcı kart MAC adresi: 7C:87:CE:F8:D3:38`
6. **MAC adresini not edin**:
    - Bu adresi bir yere yazın (örneğin, 7C:87:CE:F8:D3:38). Gönderici kodunda kullanacağız.

Adım 6: Gönderici Kartın Kodunu Yükleyin

Gönderici kart, mesajı şifreleyip alıcı karta gönderir. Aşağıdaki kodu kullanacağız.

Gönderici Kodu

```
#include <esp_now.h>
#include <WiFi.h>
extern "C" {
  #include "esp_wifi.h"
}
#include "mbedtls/aes.h"
#include "mbedtls/md.h"

// Alıcı kartın MAC adresi (Adım 5'te bulduğunuz adresle değiştirin)
uint8_t receiverMac[] = {0x7C, 0x87, 0xCE, 0xF8, 0xD3, 0x38};

// AES anahtarı (16 byte)
const uint8_t AES_KEY[16] = {
  0x1A, 0x2B, 0x3C, 0x4D, 0x5E, 0x6F, 0x70, 0x81,
  0x9A, 0xAB, 0xBC, 0xCD, 0xDE, 0xEF, 0xF0, 0x01
};

// AES-CTR şifreleme fonksiyonu
void encryptAES_CTR(uint8_t* input, size_t len, uint8_t* output, const
uint8_t* key, const uint8_t* iv) {
  mbedtls_aes_context aes;
  mbedtls_aes_init(&aes);
  mbedtls_aes_setkey_enc(&aes, key, 128);
  uint8_t stream_block[16] = {0};
  size_t nc_off = 0;
  uint8_t iv_copy[16];
  memcpy(iv_copy, iv, 16);
  mbedtls_aes_crypt_ctr(&aes, len, &nc_off, iv_copy, stream_block, input,
output);
  mbedtls_aes_free(&aes);
}

// HMAC oluşturma fonksiyonu
void generateHMAC(const uint8_t* data, size_t len, const uint8_t* key,
size_t keylen, uint8_t* output) {
  const mbedtls_md_info_t* md_info =
mbedtls_md_info_from_type(MBEDTLS_MD_SHA256);
  mbedtls_md_context_t ctx;
  mbedtls_md_init(&ctx);
```

```
  mbedtls_md_setup(&ctx, md_info, 1);
  mbedtls_md_hmac_starts(&ctx, key, keylen);
  mbedtls_md_hmac_update(&ctx, data, len);
  mbedtls_md_hmac_finish(&ctx, output);
  mbedtls_md_free(&ctx);
}

// Mesajı şifreleyip gönderme fonksiyonu
void sendEncryptedMessage(const char* plainText) {
  size_t plainLen = strlen(plainText);
  if (plainLen == 0 || plainLen > 250) {
    Serial.println("Hata: Mesaj boş veya çok uzun!");
    return;
  }

  // Rastgele 16 byte IV oluştur
  uint8_t iv[16];
  esp_fill_random(iv, 16);

  // Mesajı şifrele
  uint8_t encrypted[250];
  encryptAES_CTR((uint8_t*)plainText, plainLen, encrypted, AES_KEY, iv);

  // HMAC oluştur
  uint8_t hmac[32];
  generateHMAC(encrypted, plainLen, AES_KEY, 16, hmac);

  // Veri paketini hazırla: IV (16 byte) + şifrelenmiş veri + HMAC (4 byte)
  uint8_t packet[300];
  memcpy(packet, iv, 16);
  memcpy(packet + 16, encrypted, plainLen);
  memcpy(packet + 16 + plainLen, hmac, 4);

  // Seri porta hata ayıklama bilgileri yaz
  Serial.print("Orijinal mesaj: ");
  Serial.println(plainText);
  Serial.print("IV: ");
  for (int i = 0; i < 16; i++) Serial.printf("%02X ", iv[i]);
  Serial.println();
  Serial.print("Şifrelenmiş veri: ");
  for (int i = 0; i < plainLen; i++) Serial.printf("%02X ", encrypted[i]);
  Serial.println();
  Serial.print("HMAC (ilk 4): ");
  for (int i = 0; i < 4; i++) Serial.printf("%02X ", hmac[i]);
  Serial.println();
```

```
  // Mesajı gönder
  esp_now_send(receiverMac, packet, 16 + plainLen + 4);
  Serial.println("Mesaj gönderildi!");
}

void setup() {
  Serial.begin(115200);
  WiFi.mode(WIFI_STA);
  esp_wifi_set_channel(1, WIFI_SECOND_CHAN_NONE);

  // ESP-NOW başlat
  if (esp_now_init() != ESP_OK) {
    Serial.println("ESP-NOW başlatılamadı!");
    return;
  }

  // Alıcıyı eşleştir
  esp_now_peer_info_t peerInfo = {};
  memcpy(peerInfo.peer_addr, receiverMac, 6);
  peerInfo.channel = 1;
  peerInfo.encrypt = false;
  if (!esp_now_is_peer_exist(receiverMac)) esp_now_add_peer(&peerInfo);

  Serial.println("Gönderici hazır. Seri porta mesaj yazın:");
}

void loop() {
  if (Serial.available()) {
    String msg = Serial.readStringUntil('\n');
    msg.trim();
    sendEncryptedMessage(msg.c_str());
  }
}
```

Kodu Yükleme Adımları

1. **Gönderici kartı bilgisayara bağlayın**:
   - USB kablosuyla gönderici kartı bilgisayara takın.
2. **Deneyap Kart IDE'de kartı seçin**:
   - **Araçlar > Kart** menüsünden **Deneyap Kart 1A** veya **Deneyap Kart 1A v2**'yi seçin (kartınıza göre).
   - **Araçlar > Port** menüsünden kartın bağlı olduğu portu seçin.

3. **Kodu kopyalayın**:
   - Yukarıdaki kodu kopyalayın ve Deneyap Kart IDE'de yeni bir sketch'e yapıştırın.
4. **MAC adresini güncelleyin**:
   - Kodda receiverMac[] satırını, Adım 5'te bulduğunuz alıcı kartın MAC adresiyle değiştirin. Örneğin:
     c
     Kopyala
     ```
     uint8_t receiverMac[] = {0x7C, 0x87, 0xCE, 0xF8, 0xD3, 0x38};
     ```
5. **Kodu yükleyin**:
   - **Dosya > Yükle** (File > Upload) butonuna tıklayın.
   - Yükleme sırasında hata alırsanız, kartın doğru bağlandığından ve portun seçildiğinden emin olun.
6. **Seri monitörü açın**:
   - **Araçlar > Seri Monitör** menüsüne gidin.
   - Baud hızını **115200** olarak ayarlayın.
   - "Gönderici hazır. Seri porta mesaj yazın:" mesajını görmelisiniz.

Adım 7: Alıcı Kartın Kodunu Yükleyin

Alıcı kart, gelen şifreli mesajı çözer ve seri porta yazdırır.

Alıcı Kodu

```
#include <esp_now.h>
#include <WiFi.h>
extern "C" {
  #include "esp_wifi.h"
}
#include "mbedtls/aes.h"
#include "mbedtls/md.h"

// AES anahtarı (16 byte, göndericiyle aynı olmalı)
const uint8_t AES_KEY[16] = {
  0x1A, 0x2B, 0x3C, 0x4D, 0x5E, 0x6F, 0x70, 0x81,
  0x9A, 0xAB, 0xBC, 0xCD, 0xDE, 0xEF, 0xF0, 0x01
};

// AES-CTR çözümleme fonksiyonu
void decryptAES_CTR(uint8_t* input, size_t len, uint8_t* output, const
uint8_t* key, const uint8_t* iv) {
  mbedtls_aes_context aes;
```

```
  mbedtls_aes_init(&aes);
  mbedtls_aes_setkey_enc(&aes, key, 128);
  uint8_t stream_block[16] = {0};
  size_t nc_off = 0;
  uint8_t iv_copy[16];
  memcpy(iv_copy, iv, 16);
  mbedtls_aes_crypt_ctr(&aes, len, &nc_off, iv_copy, stream_block, input,
output);
  mbedtls_aes_free(&aes);
}

// HMAC oluşturma fonksiyonu
void generateHMAC(const uint8_t* data, size_t len, const uint8_t* key,
size_t keylen, uint8_t* output) {
  const mbedtls_md_info_t* md_info =
mbedtls_md_info_from_type(MBEDTLS_MD_SHA256);
  mbedtls_md_context_t ctx;
  mbedtls_md_init(&ctx);
  mbedtls_md_setup(&ctx, md_info, 1);
  mbedtls_md_hmac_starts(&ctx, key, keylen);
  mbedtls_md_hmac_update(&ctx, data, len);
  mbedtls_md_hmac_finish(&ctx, output);
  mbedtls_md_free(&ctx);
}

// Gelen mesajı işleme fonksiyonu
void onReceive(const uint8_t *mac, const uint8_t *data, int len) {
  if (len < 20 || len > 270) {
    Serial.println("Hata: Geçersiz veri uzunluğu!");
    return;
  }

  // IV'yi al (16 byte)
  uint8_t iv[16];
  memcpy(iv, data, 16);
  int dataLen = len - 16 - 4;

  if (dataLen <= 0 || dataLen > 250) {
    Serial.println("Hata: Geçersiz veri uzunluğu!");
    return;
  }

  // Şifrelenmiş veriyi al
  uint8_t encrypted[250];
  memcpy(encrypted, data + 16, dataLen);
```

```
// HMAC'ı al (4 byte)
uint8_t receivedHMAC[4];
memcpy(receivedHMAC, data + 16 + dataLen, 4);

// HMAC'ı hesapla
uint8_t calcHMAC[32];
generateHMAC(encrypted, dataLen, AES_KEY, 16, calcHMAC);

// Hata ayıklama bilgileri
Serial.print("Gelen IV: ");
for (int i = 0; i < 16; i++) Serial.printf("%02X ", iv[i]);
Serial.println();
Serial.print("Gelen şifrelenmiş veri: ");
for (int i = 0; i < dataLen; i++) Serial.printf("%02X ", encrypted[i]);
Serial.println();
Serial.print("Gelen HMAC: ");
for (int i = 0; i < 4; i++) Serial.printf("%02X ", receivedHMAC[i]);
Serial.println();
Serial.print("Hesaplanan HMAC (ilk 4): ");
for (int i = 0; i < 4; i++) Serial.printf("%02X ", calcHMAC[i]);
Serial.println();

// HMAC doğrulama
if (memcmp(receivedHMAC, calcHMAC, 4) != 0) {
  Serial.println("Hata: HMAC uyuşmuyor, mesaj çözülemedi!");
  return;
}

// Mesajı çöz
uint8_t decrypted[250];
decryptAES_CTR(encrypted, dataLen, decrypted, AES_KEY, iv);
decrypted[dataLen] = '\0';

// Çözülen verinin geçerli olduğunu kontrol et
bool valid = true;
for (int i = 0; i < dataLen; i++) {
  if (decrypted[i] < 32 || decrypted[i] > 126) {
    valid = false;
    break;
  }
}

if (valid) {
  Serial.print("Alınan mesaj: ");
```

```
    Serial.println((char*)decrypted);
  } else {
    Serial.println("Hata: Çözülen veri geçersiz!");
    Serial.print("Çözülen ham veri: ");
    for (int i = 0; i < dataLen; i++) Serial.printf("%02X ", decrypted[i]);
    Serial.println();
  }
}

void setup() {
  Serial.begin(115200);
  WiFi.mode(WIFI_STA);
  esp_wifi_set_channel(1, WIFI_SECOND_CHAN_NONE);

  // ESP-NOW başlat
  if (esp_now_init() != ESP_OK) {
    Serial.println("ESP-NOW başlatılamadı!");
    return;
  }

  // Gelen mesajları dinle
  esp_now_register_recv_cb(onReceive);
  Serial.println("Alıcı kart hazır.");
  Serial.println(WiFi.macAddress());
}

void loop() {
  // Gelen mesajları pasif bekliyoruz
}
```

Kodu Yükleme Adımları

1. **Alıcı kartı bilgisayara bağlayın**:
   - USB kablosuyla alıcı kartı bilgisayara takın.
2. **Deneyap Kart IDE'de kartı seçin**:
   - **Araçlar > Kart** menüsünden **Deneyap Kart 1A** veya **Deneyap Kart 1A v2**'yi seçin.
   - **Araçlar > Port** menüsünden kartın bağlı olduğu portu seçin.
3. **Kodu kopyalayın**:
   - Yukarıdaki kodu kopyalayın ve Deneyap Kart IDE'de yeni bir sketch'e yapıştırın.
4. **Kodu yükleyin**:
   - **Dosya > Yükle** butonuna tıklayın.

5. **Seri monitörü açın**:
    - **Araçlar > Seri Monitör** menüsüne gidin.
    - Baud hızını **115200** olarak ayarlayın.
    - “Alıcı kart hazır.” mesajını ve MAC adresini görmelisiniz.

Adım 8: Projeyi Test Edin

Artık her iki kart da hazır. Şimdi sistemi test edelim:

1. **Her iki kartı da çalıştırın**:
    - Gönderici ve alıcı kartları USB kablolarıyla bilgisayara bağlı tutun.
    - Her iki kartın da aynı WiFi kanalında olduğundan emin olun (kodda kanal 1 olarak ayarlı).
2. **Gönderici seri monitörünü açın**:
    - Gönderici kartın portunu seçin ve seri monitörü açın (115200 baud).
    - “Gönderici hazır. Seri porta mesaj yazın:” mesajını görmelisiniz.
3. **Bir mesaj gönderin**:
    - Gönderici seri monitörüne “MERHABA” yazın ve Enter’a basın.
    - Seri monitörde şu bilgileri görmelisiniz:
        - Orijinal mesaj: MERHABA
        - IV (rastgele 16 byte)
        - Şifrelenmiş veri
        - HMAC (ilk 4 byte)
        - “Mesaj gönderildi!”
4. **Alıcı seri monitörünü açın**:
    - Alıcı kartın portunu seçin ve seri monitörü açın (115200 baud).
    - Gelen mesajla ilgili şu bilgileri görmelisiniz:
        - Gelen IV
        - Gelen şifrelenmiş veri
        - Gelen HMAC
        - Hesaplanan HMAC
        - “Alınan mesaj: MERHABA”
5. **Farklı mesajlar deneyin**:
    - Göndericiye “TEST”, “Naber” veya başka mesajlar yazın.
    - Alıcıda mesajların doğru çözüldüğünü kontrol edin.

Adım 9: Olası Sorunları Giderme

Eğer proje çalışmazsa, şu kontrolleri yapın:

1. **MAC adresi doğru mu?**:
    - Gönderici kodundaki receiverMac adresinin alıcı kartın MAC adresiyle eşleştiğinden emin olun.
2. **Kartlar aynı kanalda mı?**:
    - Her iki kodda esp_wifi_set_channel(1, WIFI_SECOND_CHAN_NONE) satırı var. Farklı kanallar kullanıyorsanız, aynı kanalı ayarlayın.
3. **Seri monitör hataları**:
    - “ESP-NOW başlatılamadı!” gibi bir hata görürseniz, kartın bağlantısını kontrol edin ve kodu yeniden yükleyin.
    - Alıcıda “HMAC uyuşmuyor” veya “Çözülen veri geçersiz” mesajı görürseniz, MAC adresini veya kodları kontrol edin.
4. **Mesafe ve parazit**:
    - Kartlar birbirine çok uzaksa (örneğin, 10 metreden fazla), sinyal zayıflayabilir. Kartları yakın tutun.
5. **mbedtls kütüphanesi**:
    - Kütüphane doğru yüklenmediyse, Deneyap Kart IDE’den yeniden yükleyin.

Adım 10: Projenizi Geliştirin

Projeniz çalışıyor, tebrikler! Daha fazla özellik eklemek isterseniz:

- **Farklı şifreleme anahtarları** deneyin: AES_KEY dizisini değiştirin (her iki kartta da aynı olmalı).
- **Mesaj uzunluğunu artırın**: Kod şu an 250 byte’la sınırlı, ancak dizileri büyüterek daha uzun mesajlar gönderebilirsiniz.
- **LED bildirimi ekleyin**: Mesaj gönderildiğinde veya alındığında kart üzerindeki LED’leri yakabilirsiniz.
- **Kablosuz test yapın**: Kartları USB’den çıkarıp pil ile çalıştırarak tamamen kablosuz test edin.

Örnek Çıktılar

Gönderici Seri Monitör:

```
Gönderici hazır. Seri porta mesaj yazın:
Orijinal mesaj: MERHABA
IV: 1A 2B 3C 4D 5E 6F 70 81 9A AB BC CD DE EF F0 01
Şifrelenmiş veri: XX XX XX XX XX XX XX
HMAC (ilk 4): YY YY YY YY
Mesaj gönderildi!
```

Alıcı Seri Monitör:

```
Alıcı kart hazır.
7C:87:CE:F8:D3:38
Gelen IV: 1A 2B 3C 4D 5E 6F 70 81 9A AB BC CD DE EF F0 01
Gelen şifrelenmiş veri: XX XX XX XX XX XX XX
Gelen HMAC: YY YY YY YY
Hesaplanan HMAC (ilk 4): YY YY YY YY
Alınan mesaj: MERHABA
```