

T.C.
DENİZ HARP OKULU
DENİZ BİLİMLERİ VE MÜHENDİSLİĞİ ENSTİTÜSÜ
ELEKTRONİK SİSTEMLERİ MÜHENDİSLİĞİ ANABİLİM DALI

**KABLOSUZ İLETİŞİM SİSTEMLERİNDE
SİSTEM GİRİŞ GÜVENLİĞİNİN SAĞLANMASI
İÇİN TASARIMLAR**

Yüksek Lisans Tezi

Murat TEKELİ

Tez Danışmanı: Yrd.Doç.Dr. Feyzi AKAR

İstanbul, 2011

© Çalışmanın Tüm Hakları Deniz Bilimleri ve Mühendisliği Enstitüsü'ne aittir,
2011

T.C.
DENİZ HARP OKULU
DENİZ BİLİMLERİ VE MÜHENDİSLİĞİ ENSTİTÜSÜ
ELEKTRONİK SİSTEMLERİ MÜHENDİSLİĞİ ANABİLİM DALI

**KABLOSUZ İLETİŞİM SİSTEMLERİNDE
SİSTEM GİRİŞ GÜVENLİĞİNİN SAĞLANMASI
İÇİN TASARIMLAR**

Yüksek Lisans Tezi

Murat TEKELİ

Tez Danışmanı: Yrd.Doç.Dr. Feyzi AKAR

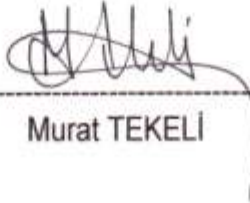
İstanbul, 2011

**KABLOSUZ İLETİŞİM SİSTEMLERİNDE
SİSTEM GİRİŞ GÜVENLİĞİNİN SAĞLANMASI İÇİN TASARIMLAR**

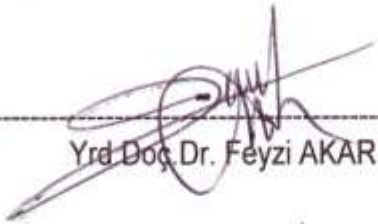
Murat TEKELİ

Mu.Yzb.

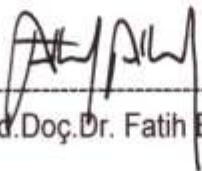
ELEKTRONİK SİSTEMLERİ MÜHENDİSLİĞİ YÜKSEK LİSANS PROGRAMI

Yazar: 
Murat TEKELİ

Sınav Tarihi : 17 Haziran 2011

Onaylayanlar : 
Yrd. Doç. Dr. Feyzi AKAR (Danışman)


Yrd. Doç. Dr. Erol ÖNEN (Sınav Komitesi Üyesi)


Yrd. Doç. Dr. Fatih ERDEN (Sınav Komitesi Üyesi)

TEŞEKKÜR

Tezin hazırlanmasında bana yol gösteren ve her konuda destek olan tez danışmanım Yrd.Doç.Dr.Öğ.Yb. Feyzi AKAR'a,

Yüksek lisans eğitimi süresince desteğini hep yanımda hissettiğim eşim Aynur'a,

Çalışmalarım esnasında yardımlarından dolayı arkadaşlarım Hamdullah, Serkan ve Ömür'e

en kalbi duygularıyla teşekkürü bir borç bilirim.

ÖZET

KABLOSUZ İLETİŞİM SİSTEMLERİNDE SİSTEM GİRİŞ GÜVENLİĞİNİN SAĞLANMASI İÇİN TASARIMLAR

Murat TEKELİ

Elektronik Sistemleri Mühendisliği Yüksek Lisans Tezi, 2011

Danışman: Yrd.Doç.Dr. Feyzi AKAR

**Anahtar Kelimeler : RFID, Araç İmmobiliser, IR Uzaktan Kontrol, PIC
Mikrodenetleyici.**

Bu çalışmada yeni bir IR (infrared, kızılötesi) tabanlı uzaktan kontrol sistemi tasarlanmaktadır. Sunulan sistem verici ve alıcı modülleri arasında güvenli bir şekilde iletişim kurmak için IR (kızıl ötesi) haberleşme kullanır. Uygulamanın güvenliği iki farklı tasarımla sağlanmıştır. İlk tasarımda asenkron (tek-yönlü) iletişim sistemi kullanılmıştır. Bu sistemde şifre üretiminde OTP (one-time password) tekniği kullanılmaktadır. Bu demektir ki kullanılan her şifre geçerliliğini kaybeder. Algoritmalar kullanıcı kimliğine göre tanımlanmaktadır. Böylelikle her bir kayıtlı kullanıcı kendine özel bir şifre üretme algoritmasına sahiptir.

Önerilen ikinci tasarımda senkron (çift-yönlü) iletişim sistemi kullanılmıştır. Kaynak ve kullanıcı her ikisi de verici/alıcı (tranciever) modülüne sahiptir. Başlangıçta kullanıcı özel protokolle oluşturulmuş 32-bit ID kimliğini gönderir. Sunucu sistem bu kimlik numarasının kaydını kontrol eder ve mevcut ise kullanıcıya rastgele bir soru yöneltir. Her iki taraf sorunun cevabını bulmak üzere aynı algoritmayı çalıştırır. Kullanıcı bulmuş olduğu cevabı kaynağa gönderir. Sunucu kendi cevabı ile istemci cevabını karşılaştırır. Gerek görülürse ikinci bir soru sorabilir ya da güvenlik

kontrollerinin yeterli olduğunu düşünerek sistemi açabilir. Burada kullanılan şifre algoritmaları da kullanıcıya özeldir.

Önerilen her iki yaklaşım yazılım ve donanımı ile birlikte prototip olarak üretilmiştir. Sistemler PIC16F877A ve PIC16F628A mikrodenetleyicileri kullanılarak tasarlanmıştır. Maliyet ve boyut olarak efektif hale getirilmiştir. Tasarlanan sistemler günlük hayatta güvenlik gereksinimi olan ev, ofis-büro gibi birimlere güvenli/kayıtlı giriş amacıyla, otomobil immobiliser uygulamaları, PC ve diğer elektronik donanımlara yetkilendirilmemiş kişilerin erişiminin engellenmesi amacıyla kullanılabilir.

ABSTRACT

DESIGNS TO PROVIDING OF SECURITY OF THE SYSTEM INPUT IN WIRELESS COMMUNICATION SYSTEMS

Murat TEKELİ

Master Thesis for Electronics Systems Engineering, 2011

Advisor: Feyzi AKAR, Asst.Prof.Dr. (Ph.D.)

Key Words : RFID, Vehicle Immobilisier, Infrared Remote Control, Anti-Theft, PIC Microcontroller

In this study a new IR-based remote control system is designed. This system, that is presented in this thesis, uses infrared frequency to communicate between the transmitter and receiver modules in a secure way. Application security is provided in two different designs. In the first design, it is used asynchronous communication system. In this system, one-time password (OTP) technique is used in the production of the code. This means that the password used is no longer valid. Algorithms are defined according to the user's identity. Thus, each registered user has a unique password generation algorithm.

The second design is used in synchronous communication system. Both the source and the user has a transceiver (transmitter/receiver) module. Initially, the user (client) sends 32-bit ID created by a special IR protocol to source (server). The server system checks and if there is a record of this identification number, directs to the user a random question. The both sides run the same algorithm to find the answer of the question. Client sends the response that is obtained by the user algorithm to the server. The server compares its response with the answer of the client. If needed, the server

can ask a second question or may think that security controls are enough, and opens the system. The encryption algorithms used here are specific to the user.

Both the proposed approach is produced with software and hardware together as a prototype. Systems are designed using the PIC16F877A and PIC16F628A microcontrollers. Design has been made effective as cost and size. The designed systems can be used in daily life in order to secured and registered login to units such as home or office, and to prevent unauthorized access of people to auto immobiliser applications, PCs and other electronic equipments.

“Bu alıřmada yazarın ortaya koymuř olduėu ifadelerin hibiri T.C. Deniz Kuvvetleri’nin ve Deniz Harp Okulu ile Deniz Bilimleri ve Mühendisliėi Enstitüsü’nün resmi görüşlerini ve politikalarını yansıtmamaktadır.”

İÇİNDEKİLER

JÜRİ ÜYELERİ KABUL VE ONAY SAYFASI..	Error! Bookmark not defined.
TEŞEKKÜR SAYFASI	ii
TÜRKÇE ÖZET.....	iii
İNGİLİZCE ÖZET	v
SORUMLULUK NOTU	vii
İÇİNDEKİLER	viii
TABLolar LİSTESİ.....	x
ŞEKİLLER LİSTESİ	xi
RESİMLER LİSTESİ	xiv
KISALTMALAR LİSTESİ	xv
I. GİRİŞ	1
A. KABLOSUZ İLETİŞİM UYGULAMALARINDA GÜVENLİK	1
B. VERİ İLETİM GÜVENLİĞİ	4
1. Hat Kodlamasının Temel Nitelikleri.....	6
2. Hat Kodlarının Sınıflandırılması	7
3. Sayısal Hat Kodlama Türleri	7
C. ŞİFRELEME	17
1. Simetrik Şifreleme	18
2. Asimetrik Şifreleme.....	19
D. GÜVENLİK SİSTEMİ TASARIMI	20
II. KIZİLÖTESİ (INFRARED) IŞINLAR.....	22
A. KIZİLÖTESİ IŞINLARIN GENEL ÖZELLİKLERİ	22
B. KIZİLÖTESİ IŞINLARIN KULLANIM ALANLARI	25
C. IrDA (INFRARED DATA ASSOCIATION)	26
1. IrDA Protokolleri	27
D. STANDART IR İLETİŞİM PROTOKOLLERİ	30
1. Pulse Coded Protocol.....	31
2. Space Coded Protocol.....	32
3. Shift Coded Protocol.....	33
III. IR İLETİŞİMDE KULLANILAN MİKRODENETLEYİCİLER.....	35
A. MİKRODENETLEYİCİLERİN GENEL ÖZELLİKLERİ	35

B.	PIC MİKRODENETLEYİCİLER.....	36
1.	PIC16F628A Mikrodenetleyici	38
2.	PIC16F877A Mikrodenetleyici	40
IV.	KABLOSUZ İLETİŞİMDE GÜVENLİK.....	42
A.	KİMLİK DOĞRULAMA	43
1.	Sabit Şifre Tekniği	44
2.	Değişken Şifre Tekniği.....	44
3.	Soru-Cevap Tekniği.....	44
B.	SALDIRILAR.....	44
1.	Tarama	45
2.	Tekrarlama	45
3.	İkili Hırsızlık	45
4.	Önceden Tahmin	47
5.	Elektronik Sözlük	47
C.	RFID (RADIO FREQUENCY IDENTIFICATION).....	47
D.	KIZILÖTESİ IŞINLAR İLE RADYO FREKANS DALGALARININ KARŞILAŞTIRILMASI	49
V.	ASENKRON VERİ İLETİŞİM SİSTEMİ	51
A.	IR İLETİŞİM PROTOKOLÜ.....	51
B.	KİMLİK DOĞRULAMA/ŞİFRELEME.....	52
C.	VERİCİ ÜNİTESİ.....	54
D.	ALICI ÜNİTESİ.....	55
VI.	SENKRON VERİ İLETİŞİM SİSTEMİ.....	59
A.	IR İLETİŞİM PROTOKOLÜ.....	59
B.	KİMLİK DOĞRULAMA/ŞİFRELEME.....	59
C.	İSTEMCİ/SUNUCU ÜNİTELERİ	59
D.	SENKRON VE ASENKRON VERİ İLETİŞİM SİSTEMLERİ ARASINDAKİ FARKLAR	65
VII.	SONUÇ	66
	KAYNAKÇA	68
	EKLER.....	76

TABLÖLAR LİSTESİ

TABLÖLAR	SAYFA
1. Tablo 2.1: IrDA İletişim Standartları.	27
2. Tablo 3.1: PIC16F628A Genel Özellikleri.	38
3. Tablo 3.2: PIC16F877A Genel Özellikleri.	40

ŞEKİLLER LİSTESİ

ŞEKİLLER	SAYFA
1. Şekil 1.1: Tek Kutuplu NRZ Kodu.	8
2. Şekil 1.2: Kutupsal NRZ Kodu.	9
3. Şekil 1.3: İki Kutuplu NRZ Kodu.	10
4. Şekil 1.4: Tek Kutuplu RZ Kodu.	11
5. Şekil 1.5: Kutupsal RZ Kodu.	12
6. Şekil 1.6: İki Kutuplu RZ Kodu.	13
7. Şekil 1.7: Manchester Kodu.	14
8. Şekil 1.8: Ayrımsal Manchester Kodu.	15
9. Şekil 1.9: Farklı Hat Kodlarına Ait Dalga Formları.	16
10. Şekil 1.10: Simetrik Şifreleme Modeli.	18
11. Şekil 1.11: Asimetrik Şifreleme Modeli.	20
12. Şekil 2.1: Elektromanyetik Spektrum.	22
13. Şekil 2.2: Tipik Kablosuz İletişim Sistemi.	24
14. Şekil 2.3: IrDA Protokol Yapısı.	28
15. Şekil 2.4 : IrLAP Çerçeve (Frame) Yapısı.	28
16. Şekil 2.5 : Pulse Coded Protocol.	31
17. Şekil 2.6 : Sony Protokolünde Zamanlama Diyagramları.	31

18.	Şekil 2.7 :	Sony Protokolünde Başlangıç Biti, Komut ve Adres Kodları.	32
19.	Şekil 2.8 :	Space Coded Protocol.	32
20.	Şekil 2.9 :	Sharp Protokolünde Başlangıç Biti, Komut ve Adres Kodları.	33
21.	Şekil 2.10 :	Shift Coded Protocol.	33
22.	Şekil 2.11 :	Philips Protokolünde Başlangıç Biti,Komut ve Adres Kodları.	34
23.	Şekil 2.12 :	Philips Protokolünde Zamanlama Diyagramları.	34
24.	Şekil 3.1 :	RISC ve CISC Mimarileri.	37
25.	Şekil 3.2 :	PIC16F628A Mikrodenetleyicisinin Pin Bağlantıları.	38
26.	Şekil 3.3 :	PIC16F628A Mikrodenetleyicisinin Blok Diyagramı.	39
27.	Şekil 3.4 :	PIC16F877A Mikrodenetleyicisinin Pin Bağlantıları.	40
28.	Şekil 3.5 :	PIC16F877A Mikrodenetleyicisinin Blok Diyagramı.	41
29.	Şekil 4.1 :	İkili Hırsızlık Tekniği.	46
30.	Şekil 4.2 :	Üçlü Hırsızlık Tekniği.	46
31.	Şekil 5.1 :	Özel İletişim Protokolü Komut ve Adres Bitleri ve Süreleri.	51
32.	Şekil 5.2 :	Alıcıya Tek Kullanımlık Şifre Gönderilmesi.	56

33.	Şekil 5.3 :	Asenkron Sistem Verici Akış Diyagramı.	57
34.	Şekil 5.4 :	Asenkron Sistem Alıcı Akış Diyagramı.	58
35.	Şekil 6.1 :	Şifreleme Algoritması.	60
36.	Şekil 6.2 :	Şifre Çözme Algoritması.	61
37.	Şekil 6.3 :	Senkron Veri İletişim Sistemi.	62
38.	Şekil 6.4 :	Senkron Sistem İstemci Akış Şeması.	63
39.	Şekil 6.5 :	Senkron Sistem Sunucu Akış Şeması.	64

RESİMLER LİSTESİ

RESİMLER	SAYFA
1. Resim 5.1: Asenkron Verici ve Alıcı Devreleri.	55
2. Resim 6.1: Senkron Verici ve Alıcı Devreleri.	62

KISALTMALAR LİSTESİ

<u>Kısaltmalar:</u>	<u>Açıklama</u>	<u>:</u>
RFID :	Radio Frequency Identification.	
RKE :	Remote Keyless Entry.	
NRZ :	Non-Return to Zero.	
RZ :	Return to Zero.	
DES :	Data Encryption Standard.	
AES :	Advanced Encryption Standard.	
IrDA :	Infrared Data Association.	
CRC :	Cyclic Redundancy Check.	
ARQ :	Automatic Repeat Request.	
LSB :	Least Significant Bit.	
MSB :	Most Significant Bit.	
PIC :	Peripheral Interface Controller.	
RISC :	Reduced Instruction Set Computer.	
CISC :	Complex Instruction Set Computer.	
OTP :	One-Time Password.	

I. GİRİŞ

Kablosuz uzaktan kumanda sistemleri hayatın her alanında sıklıkla kullanılmaya başlanmıştır. Ev ve işyerlerindeki elektronik cihazlar, giriş güvenlik sistemleri (araçlar, garaj ve otoparklar, site girişleri vb.) uzaktan kumanda cihazları ile kontrol edilmektedir. Radyo, televizyon, VCD/DVD oynatıcı gibi cihazların uzaktan kumanda edilmesinde güvenlikle ilgili bir endişe yaşanmasa da söz konusu olan arabalar, ev ve işyerlerindeki garaj kapıları ya da sadece yetkili kişiler tarafından girilmesi gereken yerler olunca; uzaktan kumanda sistemlerinin, kullanımı kolay ve aynı zamanda güvenli sistemler olması bir zorunluluk haline gelmektedir. Teknolojik gelişmelerle birlikte güvenlik seviyesi arttıkça, buna paralel olarak bu güvenliği tehdit edici teknolojiler de ortaya çıkmaktadır.

Güvenli girişi gerektiren ya da yetkisiz erişimin engellendiği sistemlerde kullanılan güvenlik teknolojisi, kullanım yerine ve ihtiyaçlara göre çeşitlilik göstermektedir. Pasif/aktif RFID, dokunmatik alarmlar, hücresel şebeke kullanan sistemler, küresel konumlandırma sistemi (GPS) izleme cihazları, ses tanımlama cihazları bunlardan bazılarıdır [1].

A. KABLOSUZ İLETİŞİM UYGULAMALARINDA GÜVENLİK

Günümüzde güvenlik sistemlerinde uzaktan anahtarsız erişim (Remote Keyless Entry,RKE) yaygın olarak kullanılmaktadır. Özellikle otomotiv sektöründe RKE güvenli ve kullanışlı bir sistem olarak lanse edilmektedir. Son yıllarda kullanıcıların da geniş çaplı olarak kabulünü ve artan talebini dikkate alan üreticiler, RKE'yi yeni modellerde bir standart olarak sunmaya başladılar. Pratikte hiçbir güvenlik sistemi yüzde yüz güvenliği garanti edemez. Güvenlik sistemleri ancak uyguladıkları güvenlik politikaları ile caydırıcı rol oynarlar. Güvenlik sisteminin tasarımında ihtiyaçlar önemlidir. Üreticiler performansa bakmaksızın düşük maliyeti tercih edebilir. Güvenlik ve düşük güç tüketimi önemli olmasına rağmen maliyet en büyük faktör konumundadır. Ayrıca çok yönlülük, esneklik ve fiziksel boyut da önem arz etmektedir.

Verici ile alıcı arasında güvenli iletişimi sağlamak için üç temel gereksinim vardır [2]:

1. İletim hattı, başkalarının mesajı ele geçirmesini önlemelidir (erişim kontrolü).
2. İletimi gerçekleştiren verici ile alıcı birbirini tanımalıdır (kimlik kontrolü).
3. İletim tekniği iletilen veriyi koruyabilmeli, veri bozulmadan alıcıya ulaşabilmelidir (bütünlük).

Güvenlik sisteminde bilgi güvenliği üç bölümde incelenebilir; kimlik doğrulama, veri iletim güvenliği ve şifreleme [3]. Kimlik doğrulama; iletimi gerçekleştiren verici ile alıcının birbirini tanıması, bir başka deyişle alıcı tarafından iletiyi gönderen vericinin yetkili olup olmadığının sınanmasıdır. Bu sınamayı gerçekleştirmek için çeşitli teknikler kullanılmaktadır.

Ben Davis ve Ron DeLong tarafından tasarlanan araç immobiliser sisteminde anahtar ile araçtaki kontrol ünitesi arasında UHF ve LF olarak iki tür kablosuz haberleşme öngörölmüştür [4]. LF bandında haberleşme, anahtar kontağa takılı iken kullanılmakta ve bu haberleşmede kontrol ünitesi tarafından işlem bilgileri anahtara yüklenmektedir. Bu bilgiler bir sonraki uzaktan kumanda safhasında anahtar tarafından tek kullanımlık şifre üretilmek üzere kullanılır. Bir önceki kullanımda anahtara gerekli bilgiler yüklendiği için bir başka anahtar ile sistemin açılması mümkün değildir. Böylelikle alıcı (kontrol ünitesi) vericinin (anahtar) kimlik doğrulamasını yapar. Uzaktan kumanda etmek suretiyle araç kapısını açmak için her seferinde farklı bir şifre üretilmektedir. Anahtar ile uzaktan kumanda işlemi UHF haberleşmesi ile sağlanmaktadır. Radyo frekans bandını kullanan güvenlik sistemleri, özellikle de araçlardaki immobiliser sistemleri yaygın olarak RFID (Radyo Frekans Identification) teknolojisini kullanmaktadır. RFID temel olarak bir otomatik nesne tanımlama teknolojisidir. Bu sistemde etiket ve etiket okuyucu bulunmaktadır [5]. Etiket ile etiket okuyucu arasındaki sinyal alışverişi radyo frekans bandı kullanılarak gerçekleştirilir. RFID sistemleri genel olarak HF, VHF ve UHF bantlarında çalışmaktadır [6].

Literatürde RFID terimi ile pasif, düşük maliyetli RFID etiketleri üzerine odaklanılsa da, aslında genel bir terim olarak RFID, çeşitli radyo frekans tabanlı tanımlama teknolojilerini ifade etmektedir [7,8]. Dünya genelinde ticari ve endüstriyel alanda etkin bir şekilde kullanılan sahtecilik ya da hırsızlık olaylarına karşı umut verici bir çözüm olarak RFID teknolojisi potansiyelini korumaktadır [9-12].

RFID 1970'lerden itibaren ticari sektörde sıkça kullanılmaya başlanmıştır. Elektronik pasaport (e-pasaport) uygulamaları [13], ürün takip sistemleri [14], taşıma ve ulaşım ödemeleri [15], hayvan tanımlama sistemleri (çiftçilikte ya da doğal hayatı koruma amaçlı araştırmalarda) [16], ilaç sahteciliğini önleme [17], araç immobiliser sistemleri [1], araç tanıma ve takip sistemleri [18] ve otoyollarda kullanılan (OGS) otomatik geçiş sistemleri [19], RFID teknolojisinin kullanıldığı alanlardan bazılarıdır. RFID hakkında temel bilgiler bölüm IV-C'de sunulmuştur.

Xiaohu Fan ve Yulin Zhang (Jinan Üniversitesi,Çin) tarafından yapılan bir araç kontrol sisteminde aracın park yerine giriş ve çıkışı kontrol altına alınmıştır [20]. RFID tabanlı çalışan sisteme çeşitli işlevler eklenerek güvenlik seviyesi artırılmıştır. Bu işlevler; park yerinden ayrılırken infrared uzaktan kumanda ile şifre girilmesi, aracın gece saatlerinde park yerinden ayrılması durumunda araç sahibine GSM ile bilgilendirme mesajının gönderilmesi ve aracın kaçırılması durumunda devreye giren sessiz alarm sistemidir.

Moratuwa Üniversitesi (Sri Lanka)'nde yapılan bir çalışmada RFID tabanlı çalışan immobiliser sistemi ile entegre edilmiş bir araç güvenlik sistemi geliştirilmiştir [1]. Bu sistemde, aracı çalınan bir araç sahibi 200 m. mesafeye kadar anahtarındaki devre dışı bırakma butonuna basarak özgün etiket bilgisini araçtaki kontrol ünitesine göndermektedir. Aracın ateşleme sistemi, güç ünitesi ve otomatik vites değiştirme sistemine entegre edilmiş olan kontrol ünitesi, gönderilen özgün bilgiyi alınca aracın hızını emniyetli bir

şekilde adım adım sıfıra indirmektedir. Aracın tekrar çalışması için araç sahibinin anahtarındaki etkinleştirme butonuna basılması gerekir.

Ford firması tarafından 1993 yılında ilk olarak Escort modelinde kullanılan PATS (Passive Anti Theft Security) sisteminde anahtar üzerindeki transponder ile araçtaki transceiver arasında RF iletişim gerçekleştirilmektedir [21]. Ancak burada anahtar üzerinde basılması gereken herhangi bir buton bulunmamaktadır. Anahtar kontağa takıldığında araç tarafından anahtara bir sinyal gönderilmekte, anahtar bu sinyale cevap olarak üretim esnasında hafızasına yüklenmiş olan kodu göndermektedir. Araçta bulunan kontrol modülü bu kodu çözerek yine üretim esnasında hafızasına yüklenmiş olan numara ile karşılaştırmakta ve uyumlu olduğu takdirde elektronik kontrol ünitesi, ateşleme sistemi ve yakıt pompasını aktif hale getirmektedir.

80'li yılların sonunda Nissan firmasının lüks modellerde uygulamaya koyduğu anahtarsız sistemde; araç sahibinin cebinde ya da çantasında taşıdığı RFID özellikli bir kart ile araçtaki kontrol ünitesi arasında yukarıdakine benzer şekilde bir iletişim gerçekleşmektedir [22]. Burada iki ünite arasındaki iletişim, araç sahibi aracın kapı kolunu çekince başlamaktadır. Ancak bu sistemde olası girişimleri önlemek amacıyla kontrol ünitesi ile RFID kart arasındaki iletişim mesafesinin kısa (700 mm.) tutulması, ilave mühendislik tasarımı ve maliyeti beraberinde getirmektedir.

B. VERİ İLETİM GÜVENLİĞİ

Güvenli iletişimde bütünlük ilkesinin gereği olarak iletilen verinin korunması, bozulmadan alıcıya ulaşması önemlidir. Alıcı ile verici arasındaki iletim ortamı, iletilen verinin türü gibi etkenler veri iletim tekniğini belirleyici unsurlardır. Örneğin tüm dünyada internet erişimi için kullanılan TCP/IP protokolü bir iletim tekniğidir. Televizyon uzaktan kumandaları gibi infrared iletişimi ile çalışan cihazlar çeşitli infrared iletişim protokolleri kullanır.

Veri iletim tekniklerinin yanı sıra sayısal haberleşme sisteminde kaynak kodlama ve kanal kodlama teknikleri bulunmaktadır [23]. Kaynak kodlamasının amacı, bilgi işaretinde bir sıkıştırma gerçekleştirerek iletilmesi gereken veri miktarının azaltılması sonucu haberleşme kaynaklarının daha verimli kullanılmasını sağlamaktır. Değişik yöntemler ile bilgi kaybına neden olmadan veya kabul edilebilir bir bilgi kaybı ile sıkıştırma sağlanarak, iletilmesi gereken veri miktarı azaltılabilmektedir. Bu sayede işaretin bant genişliği azaltılmakta ve işaretin daha verimli şekilde iletimi mümkün olmaktadır. Kanal kodlaması ise işareti haberleşme kanalının istenmeyen etkilerine dayanıklı hale getirmektedir. Bu amaçla işaret şekli haberleşme kanalının fiziksel özelliklerine uygun olarak biçimlendirilebilmektedir. Kanal kodlamasının temel amacı iletim hatalarını azaltmak olduğundan, bu doğrultuda yapılan kodlamalar hata kontrol kodlaması olarak da adlandırılmaktadır [24]. Sayısal bir verinin iletimi için hat kodlaması sıkça kullanılır. Hat kodlama iletilecek olan sinyali iletim ortamının özelliklerine uygun biçime getirerek iletişim ortamındaki gürültü, zayıflama, bozulma ve girişim gibi bozucu etkenlerden daha az etkilenmesini sağlamak amacıyla uygulanır. Örneğin; örneklenmiş ve nicelenmiş bir sinyal iletim ortamı üzerinden gönderilmek için uygun biçimde değildir. Böyle bir sinyalin nicelenmiş örnekleri kodlanarak sinyal iletişim için daha uygun biçime getirilebilir.

Hat kodlama; kullanılacak iletişim kanalının özelliklerine uygun şekilde yapılmalıdır. Örneğin, metal kablolardan oluşan iletişim ortamları alçak frekans geçiren özellik gösterir. Bu tür ortamlarda yapılan iletişimlerde hat kodlaması genellikle iletişimden önce yapılan son işlemdir. Fiber optik ya da radyo sistemleri gibi band geçiren kanallar üzerinden yapılan iletişimlerde hat kodlaması ya iletişimden hemen önce yapılır ya da modülasyonla birlikte yapılır [25].

Vericideki hat kodlayıcı ve alıcıdaki kod çözücü vericinin sembol gönderme hızında çalışmalıdır. Bu nedenle, kodlayıcı tasarımının oldukça basit olması özellikle yüksek hızlarda önem kazanır. Darbe treninin

(özel/belirli) spektral karakteristiklere sahip olması için sayısal temel band sinyaller hat kodlamasını kullanmaktadır.

Temel band, sayısal darbelerin ayrıca bir modülasyon olmadan iletimini mümkün kılmaktadır. Geniş band haberleşme sistemlerinde birden çok sinyalin eş zamanlı gönderilebilmesi için sinyaller farklı frekanslarda olmalıdır. Bu şekilde sinyaller modüle edilmiş olarak frekans bölmeli çoklama tekniği ile gönderilir. Temel band haberleşmesinde ise kanalın tamamı darbelerin (bitlerin) gönderimi için tahsis edilir. Birden fazla veri grubunun eşzamanlı gönderimi zaman bölmeli çoklama kullanılarak gerçekleştirilir [26].

1. Hat Kodlamasının Temel Nitelikleri

- Gereksinim Duyulan İletim Bant Genişliği: İletim bant genişliğinin kısıtlayıcı olduğu durumlarda çok düzeyli hat kodları kullanarak iletilecek olan sinyalin bant genişliği azaltılır. Böylece iletilen semboller birden fazla sayıda bilgi biti içerirler. Çok düzeyli kodlama aynı bit hata oranı için ikili kodlamaya göre daha düşük sinyal-gürültü oranına (SNR) ihtiyaç duyar.

- Alçak Frekanslardaki Spektrum: Kodlamada sinyalin doğru akım bileşeninin olabildiğince sifıra yakın tutulması gerekir. Çünkü iletim ortamında bağlaşım için kullanılan transformatörler ve kapasitörler işaretin alçak frekans bileşenini zayıflatırlar ve doğru akım bileşeninin geçmesine izin vermezler.

- Zamanlama İçeriği: Alıcının karar verme devrelerinin zamanlamasının yapılabilmesi için saat bilgisini iletilen sinyalden güvenilir bir şekilde elde edebilmesi gerekir. Bunun için hat kodunun iletilen sinyalde yeteri kadar yoğunlukta “geçiş” sağlaması gerekir. Burada “geçiş” düzey değişikliği anlamında kullanılmıştır. İkili sinyaldeki geçişler 1’den 0’a ya da 0’dan 1’e olan düzey değişiklikleridir.

- Hata Gözleme: Hat kodu; iletilen bilgi dizisine “fazlalık ya da artıklık” ekleyerek iletim hattındaki hata oranının gözlenmesini sağlayabilir. Örneğin,

hat kodlaması bazı sembol dizilerini oluşturmayacak şekilde yapılır, eğer bu geçersiz sembol dizileri iletim sırasında oluşursa alıcı bunları iletim hataları olarak algılar ve bunların sayısına bağlı olarak hattın performansını belirler.

• Verimlilik: Hat kodlamasının yukarıda açıklanan özellikleri sağlayabilmesi için genellikle iletilen bilgi sinyaline ek bilgiler ilave edilmesi gerekir. “Fazlalık ya da artıklık” olarak tanımlanan bu ek bilgiler hat kodunun verimliliğinin düşmesine sebep olur.

2. Hat Kodlarının Sınıflandırılması

Kodlama yöntemi olarak kutup sayısına göre ya da sıfıra dönüp dönmemeye göre çeşitli yöntemler kullanılabilir. Bu yöntemlerin sınıflandırılması aşağıdaki gibidir.

- Kutup sayısına göre :
 - Tek Kutuplu Kodlama (Unipolar)
 - İki Kutuplu Kodlama (Bipolar)
- Sıfıra dönüp dönmemeye göre :
 - Sıfıra Dönmeyen Kodlama(NRZ: non-return to zero)
 - Sıfıra Dönen Kodlama (RZ: return to zero)

Bit süresi ortasında geçiş olan yöntemler kenar tetiklemeli yöntem olarak adlandırılır.

3. Sayısal Hat Kodlama Türleri

Yaygın olarak kullanılan hat kodları aşağıda açıklanmıştır.

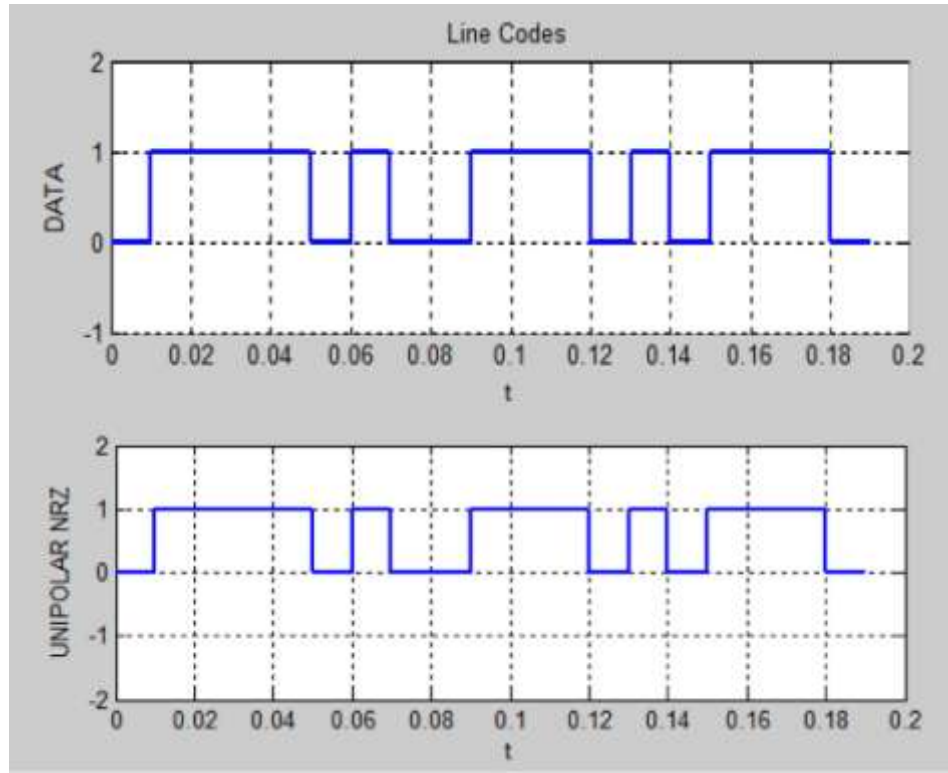
a. Tek Kutuplu NRZ Kodu (Unipolar NRZ Code)

“NRZ(Non Return To Zero)” ifadesi T saniyelik bit aralığı süresi içinde gerilim düzeyi sıfıra geri dönmeyen, yani bit aralığında gerilim düzeyi

değişmeyen kod anlamına gelir. Tek kutuplu NRZ kodu ve T saniyelik bit aralığı süresi Şekil 1.1'de gösterilmiştir. Tek kutuplu NRZ kodunda 0 ve 1 bitleri aşağıdaki gibi kodlanır. Tek bir sinyal seviyesi bulunmaktadır. Mesafe kısa olduğu için makine içi haberleşmesinde kullanılmaktadır. İşaretin spektrumu DC bileşeni içerir. Alıcıya gelen işareten saat darbelerinin elde edilmesi olanaksızdır.

0 bit : T saniye süreli 0 gerilim düzeyi ile kodlanır.

1 bit : T saniye süreli + V gerilim düzeyi ile kodlanır.



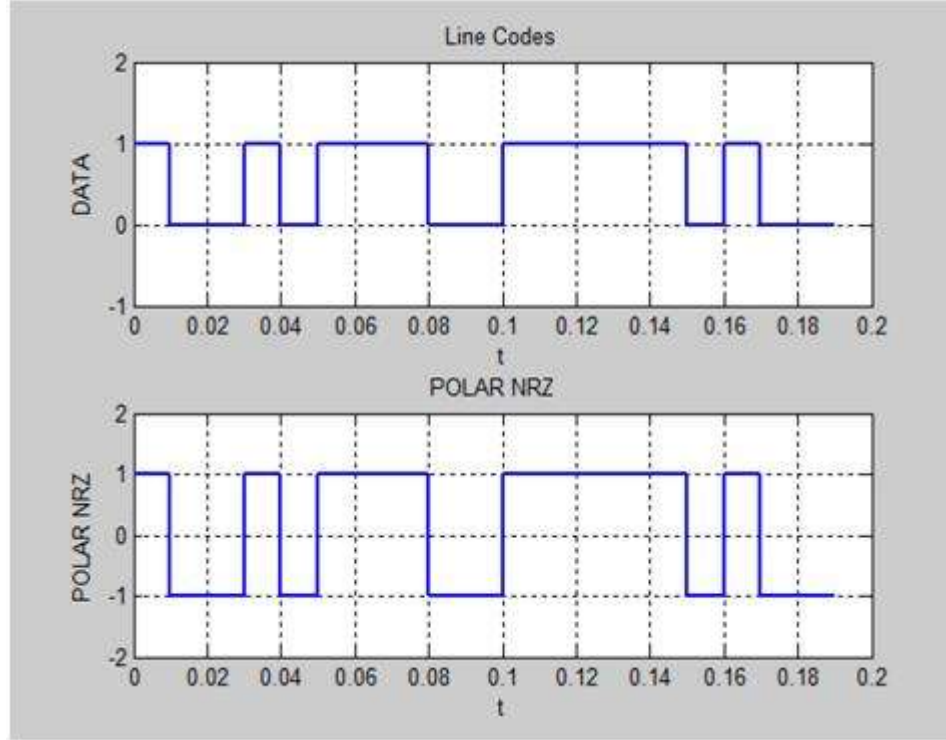
Şekil 1.1: Tek Kutuplu NRZ Kodu

b. Kutupsal (Polar) NRZ Kodu

Kutupsal NRZ kodunda 0 ve 1 bitler aşağıdaki gibi kodlanır. Kutupsal NRZ kodu ve T saniyelik bit aralığı süresi Şekil 1.2'de gösterilmiştir. İşaretin spektrumunda DC bileşeni yoktur. Alıcıya gelen işareten saat darbelerinin elde edilmesi olanaksızdır.

0 bit : T saniye süreli - V gerilim düzeyi ile kodlanır.

1 bit : T saniye süreli + V gerilim düzeyi ile kodlanır.



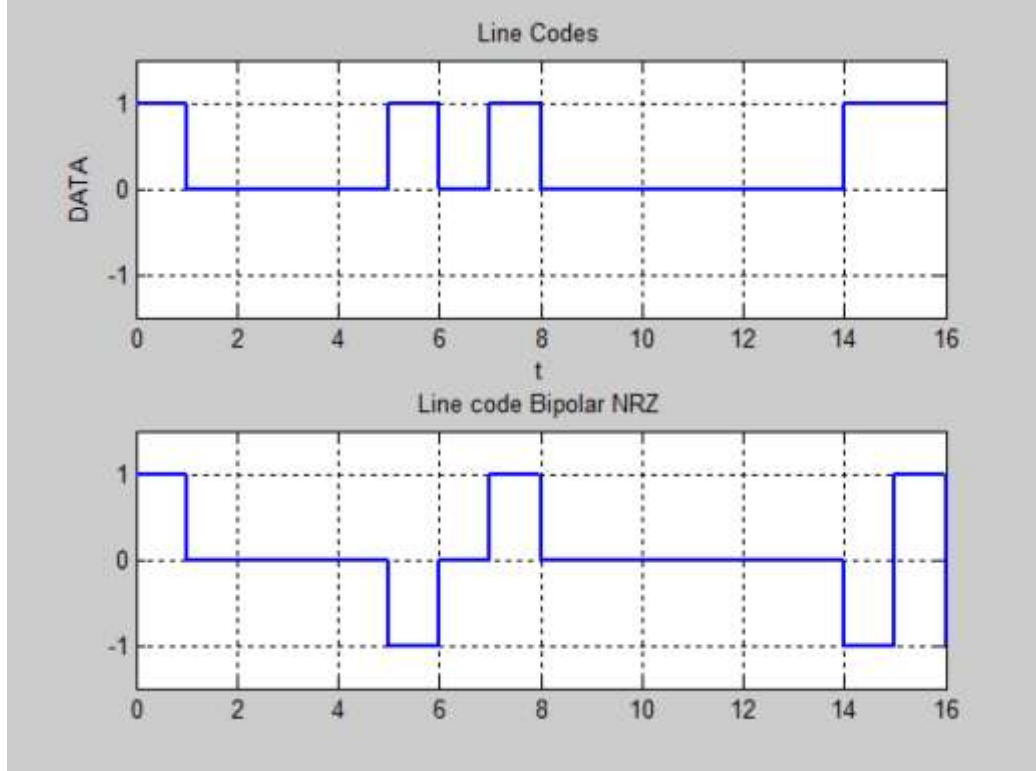
Şekil 1.2: Kutupsal NRZ Kodu

c. İki Kutuplu (Bipolar) NRZ Kodu

İki kutuplu NRZ kodu Şekil 1.3'de gösterilmiştir. İki kutuplu NRZ kodunda 0 ve 1 bitler aşağıdaki gibi kodlanır. Birbiri ardına gelen 0 ve 1 'ler problem yaratmaktadır. İşaretin spektrumunda DC bileşeni yoktur. Art arda gönderilen 0 bitler alıcıya gelen işaretten saat darbelerinin elde edilmesini olanaksız kılar.

0 bit : T saniye süreli 0 gerilim düzeyi ile kodlanır.

1 bit : T/2 saniye süreli dönüşümlü olarak +V ve -V gerilim düzeyi ile kodlanır.



Şekil 1.3: İki Kutuplu NRZ Kodu

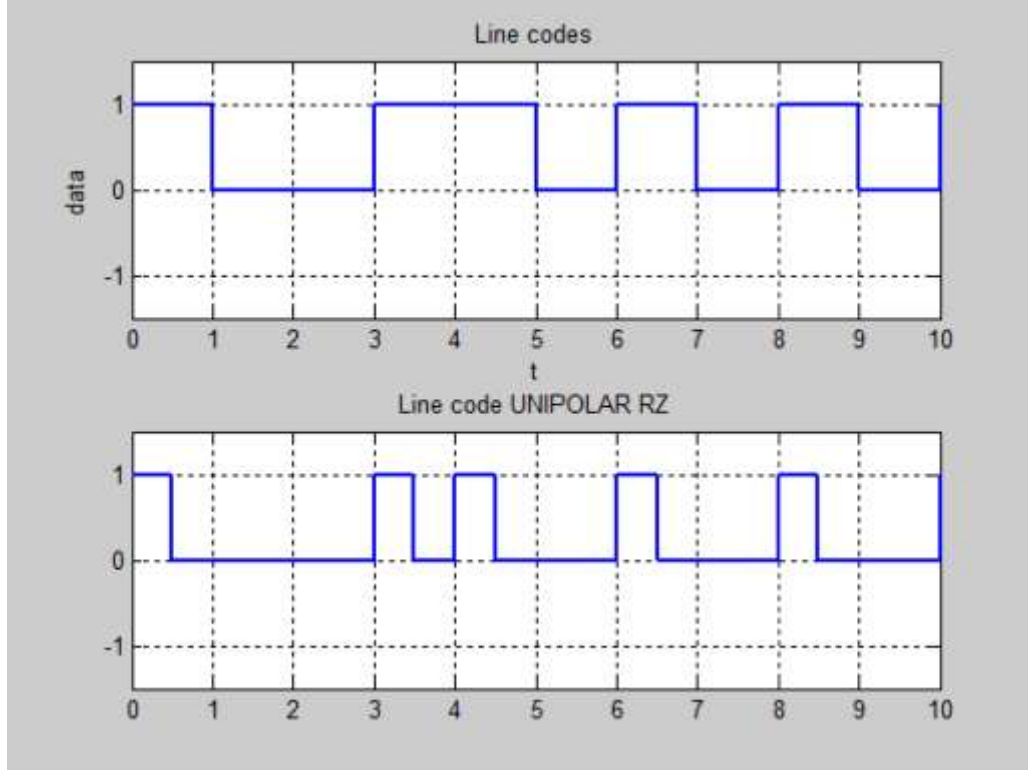
NRZ bit periyodu boyunca sıfıra geçiş yapmaz, bit periyodu boyunca seviyesinde sabit kalır, bu sebeple spektral olarak daha avantajlıdır ancak senkronizasyonu daha kötüdür.

d. Tek Kutuplu (Unipolar) RZ Kodu

“RZ (Return to zero) kodu” ifadesi T saniyelik bit aralığı içinde gerilim düzeyi 0’a geri dönen yani bit aralığının ilk yarısında $+V$ ya da $-V$ olan, gerilim düzeyinin bit aralığının ikinci yarısında sıfır gerilim düzeyine düşmesi anlamına gelir. Tek kutuplu RZ kodunda 0 ve 1 bitler aşağıdaki gibi kodlanır. Bit aralığı süresi boyunca sembol sıfırdan farklı bir değer alacaksa bu sürede tekrar sıfıra dönüş yapar. Tek Kutuplu RZ kodu Şekil 1.4’de gösterilmiştir.

0 bit : T saniye süreli 0 gerilim düzeyi ile kodlanır.

1 bit : T saniyelik bit aralığının $T/2$ sn’lik bölümünde kodun türüne bağlı olarak $-V$ yada $+V$ gerilim düzeyi ile ve onu izleyen $T/2$ saniyelik diğer bölümünde sıfır gerilim düzeyi ile kodlanır.



Şekil 1.4: Tek Kutuplu RZ Kodu

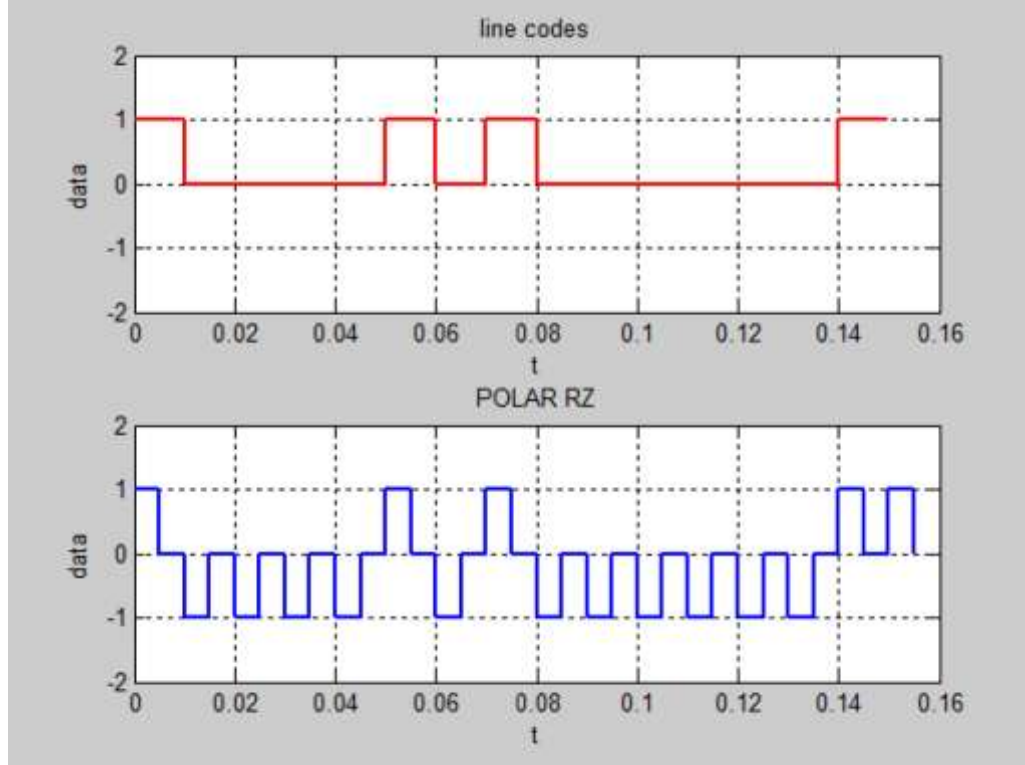
Art arda gönderilen 1 bitler alıcıda saat darbelerinin elde edilmesini sağlar. İşaretin spektrumu DC bileşeni içerir. Art arda gönderilen 0 bitler alıcıda saat darbelerinin elde edilmesini olanaksız kılar. NRZ'ye kıyasla iletişimde iki kat fazla bant genişliğine gereksinim duyulur.

e. Kutupsal (Polar) RZ Kodu

Kutupsal RZ kodunda 0 ve 1 bitler aşağıdaki şekilde kodlanır. İşaretin spektrumunda DC bileşeni yoktur. Alıcıya gelen işaretten saat darbeleri elde edilebilir. NRZ 'ye kıyasla iki kat daha fazla bant genişliğine ihtiyaç duyulur. Kutupsal RZ kodu Şekil 1.5'de gösterilmiştir.

0 bit : T saniyelik bit aralığının T/2 saniyelik bölümünde -V gerilim düzeyi ile ve onu izleyen T/2 saniyelik diğer bölümünde sıfır gerilim düzeyi ile kodlanır.

1 bit : T saniyelik bit aralığının T/2 saniyelik bölümünde +V gerilim düzeyi ile ve onu izleyen T/2 saniyelik diğer bölümünde sıfır gerilim düzeyi ile kodlanır.



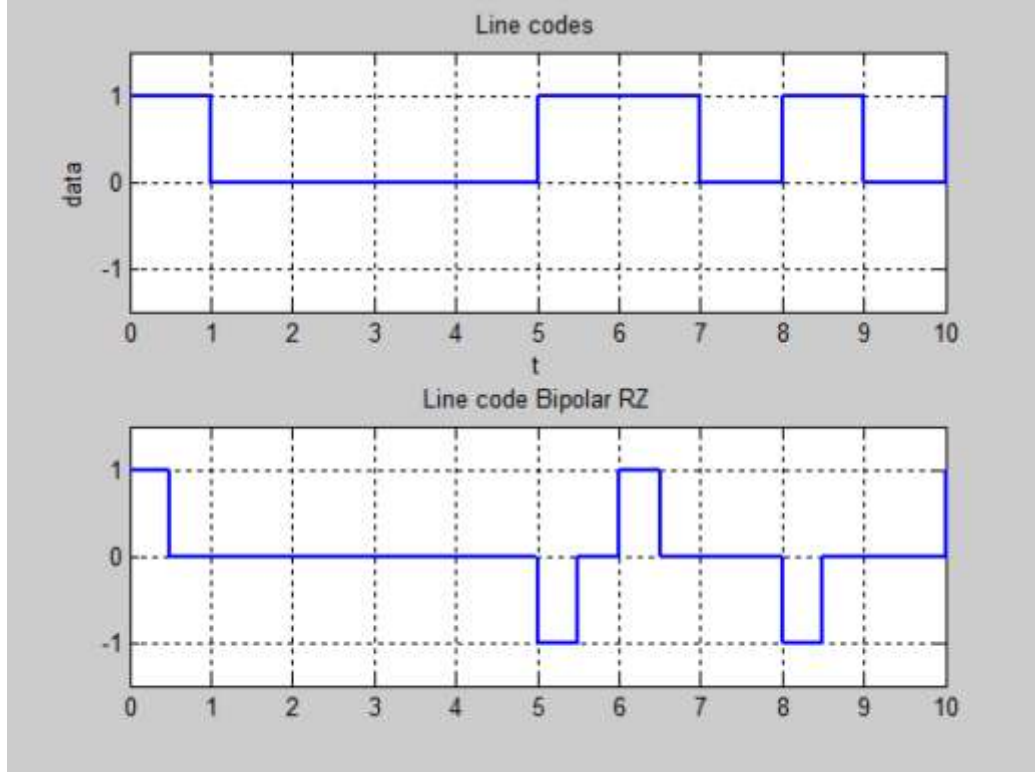
Şekil 1.5: Kutupsal RZ Kodu

f. İki Kutuplu (Bipolar) RZ Kodu (AMI)

Bu kod genellikle AMI kodu ya da “Bipolar AMI code” olarak bilinir. İki kutuplu RZ kodunda 0 ve 1 bitler aşağıdaki şekilde kodlanır.

0 bit : T saniye süreli 0 gerilim düzeyi ile kodlanır.

1 bit : T saniyelik bit aralığının T/2 saniyelik bölümünde dönüşümlü olarak +V ve -V gerilim düzeyi ile ve onu izleyen T/2 saniyelik diğer bölümünde sıfır gerilim düzeyi ile kodlanır. Yani pozitif ve negatif darbeler 1 sembolü için kullanılır. Sıfır için sıfır gönderilir.



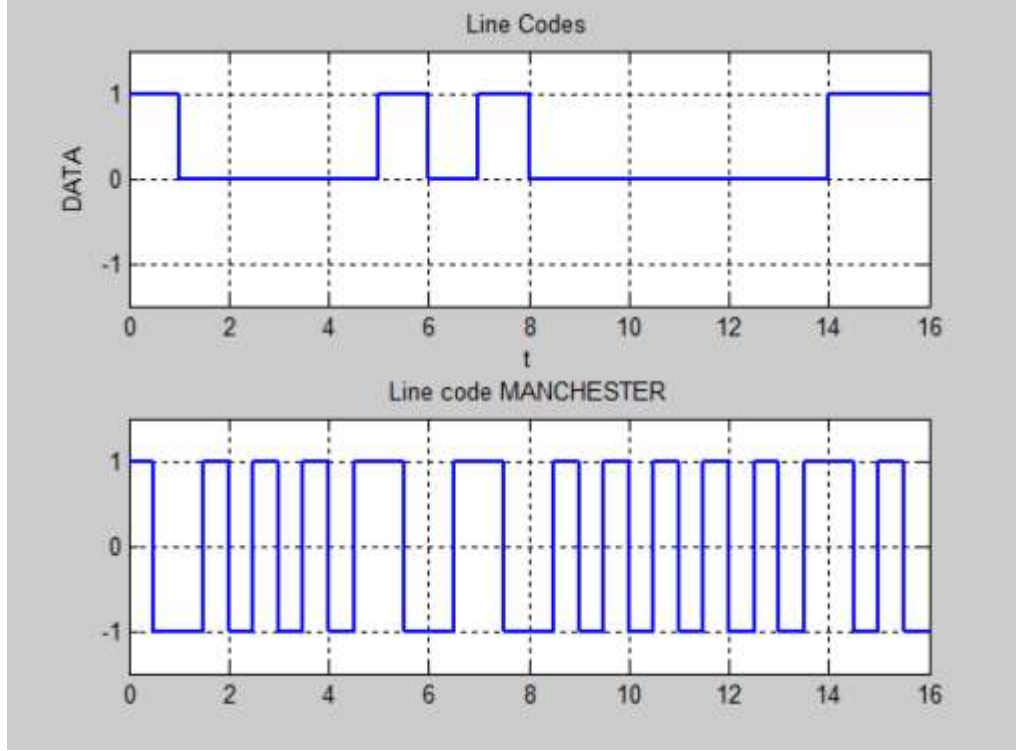
Şekil 1.6: İki Kutuplu RZ Kodu

İşaretin spektrurumunda DC bileşeni yoktur. Alıcıya gelen işaretten saat darbelerinin elde edilmesi olanaksızdır. NRZ 'ye kıyasla iki kat daha fazla bant genişliğine ihtiyaç duyulur. RZ kodlama her bit periyodunda sıfıra dönmektedir. Bu işlem, spektrumun genişlemesine sebep olurken, zamanlama senkronizasyonunu düzenler. İki kutuplu RZ kodu Şekil 1.6'da gösterilmiştir.

g. *Manchester (Split Phase) Kodu*

İki kutuplu NRZ türü bir kod olan Manchester kodu faz kodlaması olarak da bilinir. Manchester kodunun örneği Şekil 1.7'de gösterilmiştir. 1 biti ve 0 biti için +5V ve 0V seviyelerini kullanmak çeşitli sorunlara neden olabilir. Örneğin bir sessizlik periyodundan sonra kanalda 0001000 bitlerinin bu kodlamayla gönderilmesi durumunda alıcılar baştaki 0'ların paketin bir parçası mı yoksa sessizlik mi olduğunu bilemezler. Bunu çözmek için +5V-5V seviyeleri kullanılabilir ancak alıcı ve gönderici zamanlayıcıları arasındaki ufak bir fark, bit zamanlamasında kaymaya neden olur. Bu nedenle her bitte

hem yukarıdaki 0-1 ayrımının yapılması hem de zamanlama bilgisinin gönderilmesi gerekir. İşaretin spektrumunda DC bileşeni yoktur. NRZ 'ye kıyasla iki kat daha fazla bant genişliğine ihtiyaç duyulur.



Şekil 1.7: Manchester Kodu

Manchester kodunda 0 ve 1 bitler aşağıdaki şekilde kodlanır.

0 Bit : 01 ile kodlanır. Başka bir ifadeyle T saniyelik bit aralığının ilk yarısında $-V$ gerilim düzeyi ile, onu izleyen $T/2$ saniyelik ikinci yarısında $+V$ gerilim düzeyi ile kodlanır. Böylece 0 bitler için bit aralığının orta noktasında daima eksiden artıya geçiş yapılmış olur.

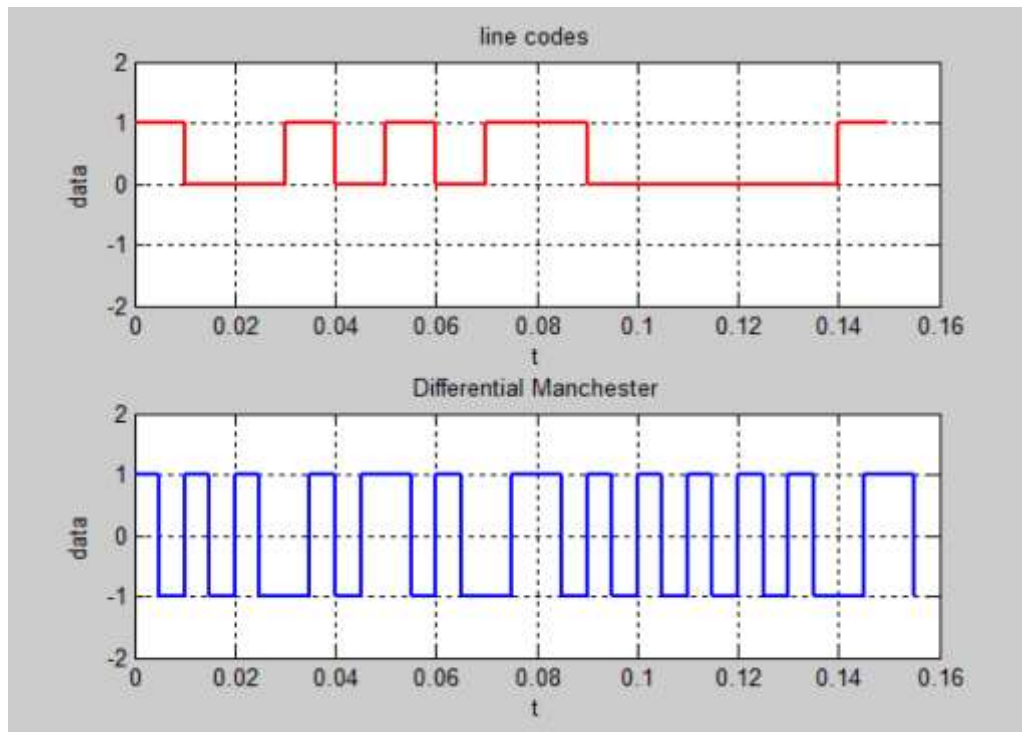
1 Bit : 10 ile kodlanır. Başka bir ifadeyle T saniyelik bit aralığının ilk yarısında $+V$ gerilim düzeyi ile, onu izleyen $T/2$ saniyelik ikinci yarısında $-V$ gerilim düzeyi ile kodlanır. Böylece 1 bitler için bit aralığının orta noktasında daima artıdan eksiye geçiş yapılmış olur.

h. Ayrimsal Manchester Kodu

Ayrımsal Manchester kodunda 0 ve 1 bitler aşağıdaki şekilde kodlanır. İki kutuplu NRZ türü bir kod olan Ayrımsal Manchester kodunun örneği Şekil 1.8’de gösterilmiştir.

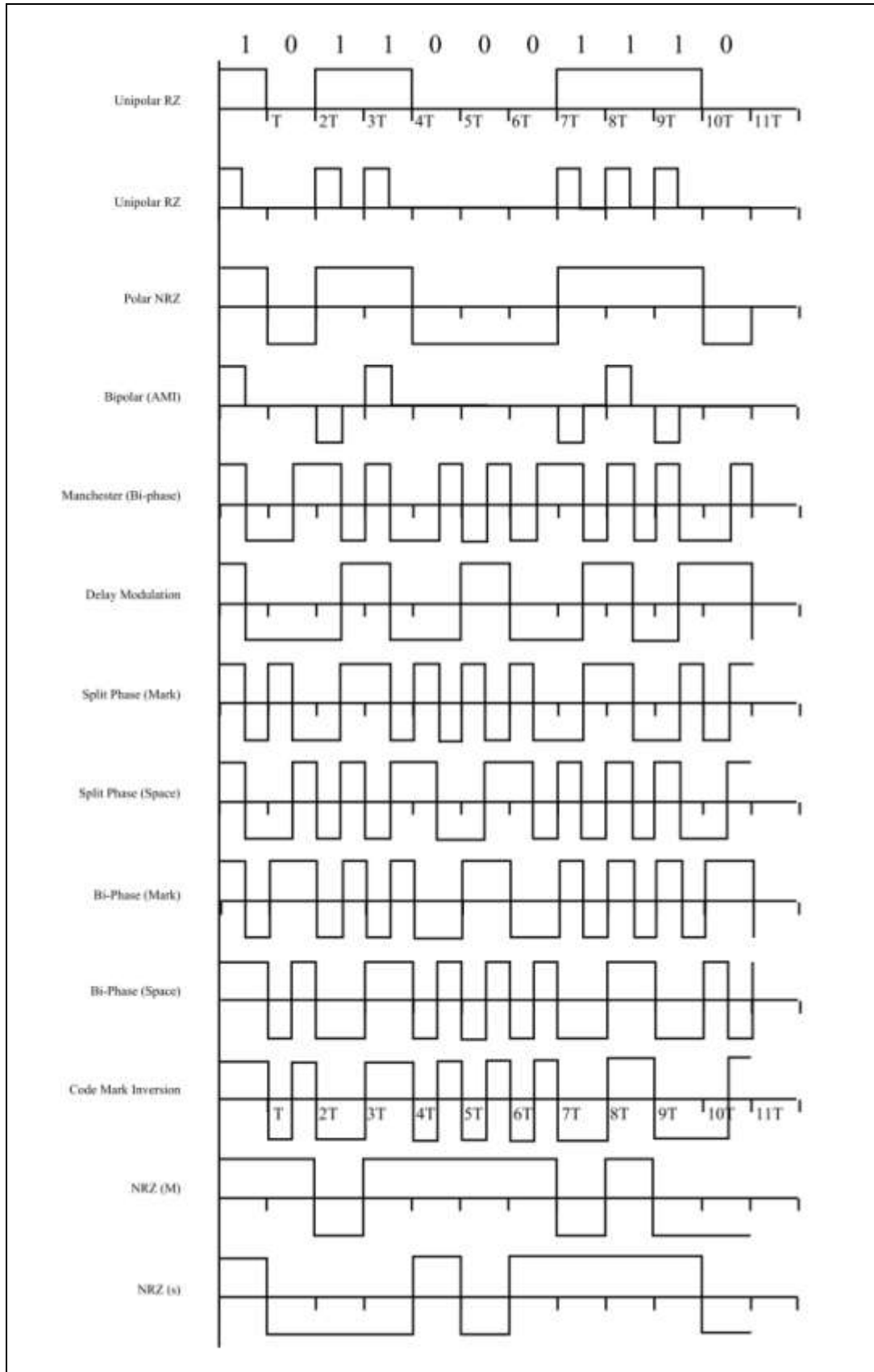
0 bit : Bit aralığının hem başında hem ortasında gerilim düzeyi değişikliği yapılarak kodlanır.

1 bit : Bit aralığı başında gerilim düzeyi değişikliği yapmadan sadece bit aralığı ortasında gerilim düzeyi değişikliği yapılarak kodlanır.



Şekil 1.8: Ayrımsal Manchester Kodu

İşaretin spektrumunda DC bileşeni yoktur. Alıcıya gelen işaretten saat darbelerinin elde edilmesi mümkündür. Gürültü bağışıklığı Manchester koduna göre daha iyidir. NRZ 'ye kıyasla iki kat daha fazla bant genişliğine ihtiyaç duyulur. Manchester koduna göre daha karmaşık bir kodlama yöntemidir [25].



Şekil 1.9: Farklı Hat Kodlarına Ait Dalga Formları [25]

Bunların dışında darbelerin gerilim düzeyleriyle ilişkili olarak ayrıca dipolar, HDBn (High Density Bipolar substitution), CMI (Coded Mark Inversion) gibi kodlama türleri de bulunmaktadır. Şekil 1.9'da farklı kodlama türlerine ait dalga formları gösterilmiştir.

Kızılötesi (infrared) iletişim için tek kanal kullanılır ve seri iletişim gerçekleştirilir. Seri iletişimde bilgi sinyali ile saat bilgisi beraber gönderilir, alıcıda bu bilgiler ayrıştırılır. Bunun için hat kodlama teknikleri kullanılır [27].

C. ŞİFRELEME

Bir güvenlik tekniği olarak, şifreleme tekniği bilgi güvenliğinin temeli olarak varsayılabilir. Şifreleme işlevinin en geleneksel kullanımı belirli kişilerden saklanması amacını güden kullanımdır. Bir bilginin şifrelenmesi, yetkisiz kişilerce ele geçirilse dahi kolayca anlaşılamayacak, çözölemeyecek şekle dönüştürülmesi anlamına gelir. Dönüştürme işleminin sahip olması gereken önemli bir özellik yetkili alıcının şifreli mesajı kolayca ve kısa sürede çözebilmesidir. Şifreleme bilginin depolanması ve taşınması sürecinde kullanılır. Korunması gereken bilgi birçok yöntemlerle şifreli hale getirilir. Şifreli bilgi depolanma veya taşıma esnasında ele geçirilse bile çözülmesi çok zordur. Bu zorluk şifreleme algoritması ve anahtar uzunluğuna bağlıdır.

Shannon şifre sistemleri tasarımı için beş kriter önermiştir [28]:

- Gizliliğin miktarı : Şifreli bilgi, deşifre işlemi hakkında fikir verecek nitelikte olmamalıdır.
- Anahtar uzunluğu : Anahtarın, taşınması ve depolanması açısından mümkün olduğu kadar kısa olması beklenir.
- Şifreleme ve şifre çözme işlemlerinin karmaşıklığı : İşlemlerin karmaşık ve uzun olması zaman kaybı ve hata oranının artmasına neden olur.

- Hata yayılımı : Şifreleme ya da şifreli bilginin gönderimi esnasında yapılan bir hata, şifre çözme işleminde daha büyük hatalara yol açabilir. Bu tür hataların minimize edilmesi istenen durumdur.

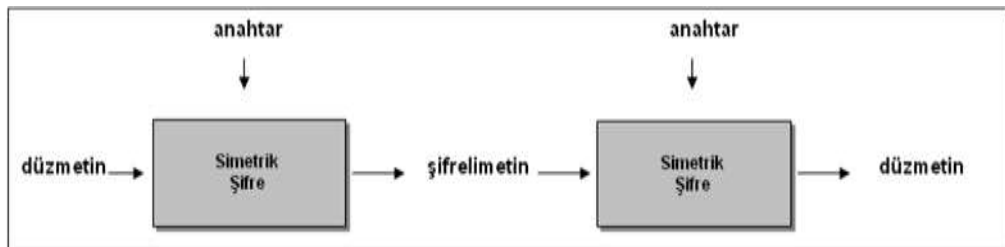
- Mesaj büyümesi : Şifreleme işlemi bazen mesajın boyutunun büyümesine yol açabilir. İyi bir şifrelemede mesaj boyutunun büyümesi mümkün olduğunca önlenmelidir.

Bu kriterler şifreleme sisteminin tasarımında göz önüne alınması gereken temel parametreler olarak kabul görmüştür [29,30].

Veri şifreleme temel olarak şifreleme ve şifre çözme işleminde kullanılan anahtarın türüne göre iki gruba ayrılır. Bu iki grup simetrik ve asimetrik şifreleme tekniğidir.

1. Simetrik Şifreleme

Simetrik şifre, şifreleme için kullanılan anahtarın şifreyi çözmek için kullanılan anahtara denk olduğu şifredir. Tüm klasik şifreler bu şekilde tasarlanmıştır. DES (Data Encryption Standard) ve AES (Data Encryption Standard), en çok bilinen simetrik şifreleme algoritmalarıdır [3].



Şekil 1.10: Simetrik Şifreleme Modeli

1970'li yıllarda IBM tarafından geliştirilen, Amerikan Gizli Servisi (National Security Agency, NSA) tarafından gözden geçirilen ve o zamanki adı NBS (National Bureau of Standards) olan ABD'deki Ulusal Standartlar ve Teknoloji Enstitüsü tarafından ulusal şifreleme standardı olarak kabul edilen

şifre yöntemi (DES), temelde 64 bitlik bir anahtar kullanılarak düzmetnin yer değiştirme, transpoze etme, tekrar yer değiştirme,... işlemlerine belli bir adım sayısı kadar tabi tutulmasına dayanır [31,32]. DES şifreleme algoritması günümüzdeki bilgi işlem gücü ve matematiksel analiz yöntemler göz önünde bulundurulduğunda artık yeterince güvenli olarak kabul edilmemektedir. Bununla birlikte bu algoritmanın düzmetne üç kez üst üste uygulanmasından ibaret olan varyantı 3-DES (Triple DES) halen pek çok bilgisayar uygulamasında güvenlik gerektiren kısımlarda kullanılmaktadır.

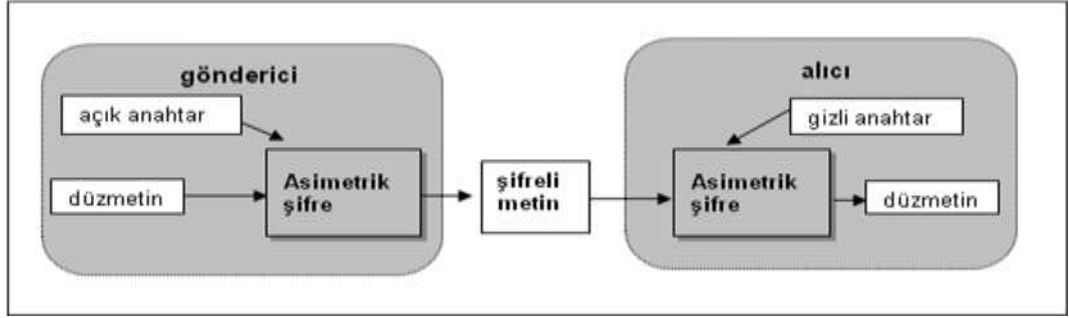
ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST, National Institute of Standards and Technology) tarafından 2002 yılında İleri Seviyeli Şifreleme Standardı (AES – Advanced Encryption Standard) olarak kabul edilen Rijndael, Belçika'lı iki araştırmacı, Joan Daemen ve Vincent Rijmen tarafından geliştirilmiştir [33,34]. Söz konusu algoritma yüksek güvenlik ve hızlı şifreleme gerektiren pek çok uygulamada kullanılmaya başlanmış olup, 128, 192 veya 256 bitlik anahtarlar kullanıp 128, 192 veya 256 bitlik blok şifreleme yapabilmektedir.

2. Asimetrik Şifreleme

Aslında, 1975 yılına dek başka türde bir şifre tasarlanabileceği düşünülüyordu. 1975-1978 yılları arasında Merkle ve Hellman asimetrik şifre sistemlerine dair ilk fikirleri ve tasarımları ortaya koydular [35,36]. Bu modele göre şifreleme anahtarı açık anahtar (public key) olarak anılır ve kamuoyuna açıktır, şifreyi çözmek için kullanılan anahtar gizli anahtar (private key) olarak anılır ve sadece şifreyi çözmeye yetkili kişinin bilgisi dahilindedir.

Açık anahtar şifreleme olarak da bilinen asimetrik şifreler aynı zamanda matematiksel analiz bakımından da oldukça ilginçtirler, çünkü bu şifrelerin çözümünün zorluğu doğrudan bazı önemli matematiksel problemlerin çözümünün zorluğu ile bağlantılıdır. Simetrik şifreler, matematiksel bakımdan, asimetrik şifrelere kıyasla daha basittirler. Buna

karşılık asimetrik şifreleme tekniği işlem yükünden dolayı simetrik şifrelemeye kıyasla 1000 kat yavaş çalışır. Başlıca açık anahtar şifreleme yöntemleri Diffie-Hellman anahtar değiş tokuşu [37], RSA (Rivest, Shamir, Adleman) [38], ElGamal [39] ve Eliptik Eğri Şifrelemesidir [40].



Şekil 1.11: Asimetrik Şifreleme Modeli

Her iki yöntemin avantajlı yönlerinden faydalanmak için genellikle karışık bir teknik kullanılır. Gizli anahtar alışverişinde asimetrik şifreleme kullanılırken, verici ile alıcı arasında veri transferi esnasında simetrik şifreleme kullanmak bu yöntemlerden birisidir [3].

D. GÜVENLİK SİSTEMİ TASARIMI

Bu tez çalışmasında yeni bir infrared tabanlı uzaktan kumanda sistemi tasarlanmıştır. Tasarlanan bu sistemde verici ve alıcı modülleri arasındaki iletişim ortamı kızılötesi (IR) frekans bandıdır. İkinci bölümde IR ışınlar, IR standartları ve IR iletişim protokolleri hakkında genel bilgiler verilmektedir.

Sistem tasarımı esnasında donanım gerçekleştirmesi PIC16F628A ve PIC16F877A mikrodenetleyiciler kullanılarak yapılmış, maliyet ve boyut olarak etkinlik sağlanmıştır. Mikrodenetleyicilerin kullanım alanları ve tasarlanan sistemde kullanılan PIC mikrodenetleyicileri hakkında bilgiler üçüncü bölümde yer almaktadır.

Bir sonraki bölümde ise kablosuz uzaktan kumandalı güvenlik sistemlerinde kullanılan temel yöntemlerden birisi olan RFID hakkında özet bilgi verilmiştir. Ayrıca IR ile RF arasında kısa bir karşılaştırma yapılmıştır.

Tasarlanan uzaktan kumanda sisteminde iki farklı yöntem kullanılmıştır. İlk yöntemde asenkron (tek-yönlü) iletişim söz konusudur. İletişim güvenliğini sağlamak için ikinci bölümde bahsedilen “pulse coded protocol” ile uyumlu standart dışı özel bir iletişim protokolü kullanılmıştır. Ayrıca bilginin iletilmesinde tek kullanımlık şifre (OTP, one-time password) tekniği kullanılmaktadır. Algoritmalar kullanıcı kimliğine göre tanımlanmaktadır. Böylelikle her bir kayıtlı kullanıcı kendine özel bir şifre üretme algoritmasına sahiptir [41]. Önerilen asenkron veri iletişim sistemi beşinci bölümde ayrıntılı olarak anlatılmaktadır.

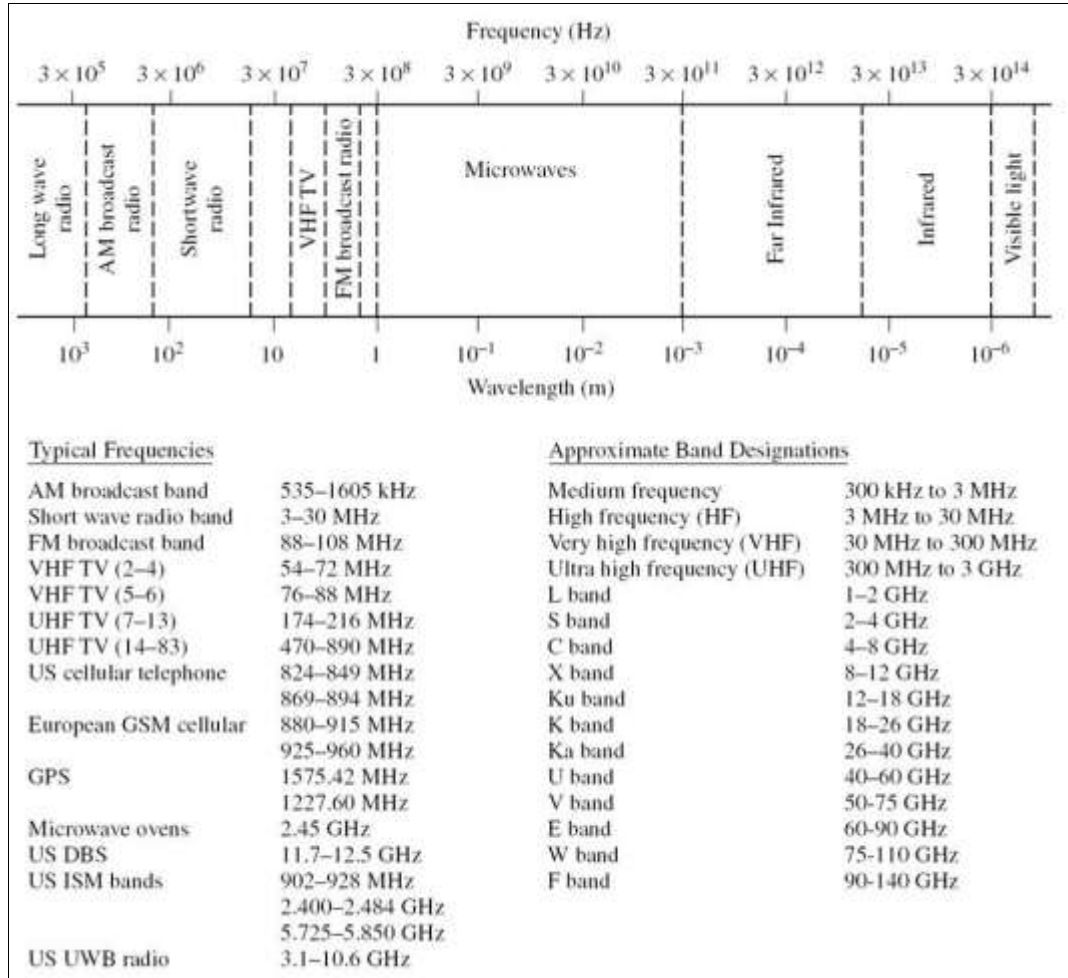
İkinci tasarım yöntemi olan senkron (çift-yönlü) iletişim sistemi hakkında ayrıntılı olarak bilgi altıncı bölümde verilmektedir. Bu yöntemde kaynak ve kullanıcı her ikisi de verici/alıcı (transceiver) modülüne sahiptir. Burada kullanılan şifre algoritmaları da kullanıcıya özeldir.

Son bölümde tasarlanmış olan her iki yöntemin uygulamaları ve bu uygulamalar sonucunda elde edilmiş veriler analiz edilerek sistemin güvenliği konusunda değerlendirme yapılmaktadır.

II. KIZILÖTESİ (INFRARED) IŞINLAR

A. KIZILÖTESİ IŞINLARIN GENEL ÖZELLİKLERİ

Kablosuz iletişim, bilginin tel veya kablo kullanılmadan iki cihaz arasında iletilmesidir. Kablosuz klavye, kablo kullanmadan bilgisayara bilgi gönderir; bir cep telefonu telefon kablosu kullanmadan başka bir telefona bilgi gönderir. Televizyon kanallarını değiştirme, garaj kapsını açma/kapatma ve başka bir bilgisayara dosya aktarımı kablosuz iletişim teknolojisini kullanarak yapılabilir. Tüm bu durumlarda bilginin gönderilmesi ve alınması elektromanyetik enerji kullanılarak yapılmaktadır. Elektromanyetik spektrum, frekans veya dalga boyuna göre elektromanyetik enerjiyi sınıflandırır.



Şekil 2.1: Elektromanyetik Spektrum [42]

Infrared, yani kızılötesi ışınlar; elektromanyetik spektrumda görülebilen ışıkla mikrodalga arasındadır. Görülebilen kırmızı ışıktan daha uzun dalga boyuna sahip, gözle görülmeyen ışınlardır ve dalga boyları 0.75 ile 1000 μm arasındadır.

Kızılötesi ışınların kaşifi, Sir Frederick William Herschel (1738-1822)'dir. Güneş ışığının ısı etkisi üzerinde çalışırken bir üçgen prizma ile güneşten gelen ışığı kırmış, termometre ile yaptığı ölçümlerde mordan kırmızıya doğru renklerin ısılarının yükseldiğini görmüştür. Bu tespit 1777'de Ladriani tarafından yapılmış ve daha sonra defalarca tekrarlanmıştır [43]. Ancak Herschel kırmızıdan sonraki karanlık bölümde ısının yükselmeye devam ettiğini ve bu bölgede görülemeyen ışının olduğunu tespit etmiştir. Herschel, bu ışınımı "kalorifik ışınlar" adını vermiştir, "infrared" terimini kullanmamıştır ve 1880'lere kadar literatürde de bu terime rastlanmaz [44,45].

Uluslararası Aydınlatma Komisyonu (Commission internationale de l'éclairage, CIE) kızılötesi ışınımı aşağıdaki bantlara ayırmayı teklif etmiştir:

- IR-A: 700 nm–1400 nm
- IR-B: 1400 nm–3000 nm
- IR-C: 3000 nm–1 mm

Yaygın olarak kullanılan bölümlere şu şekildedir:

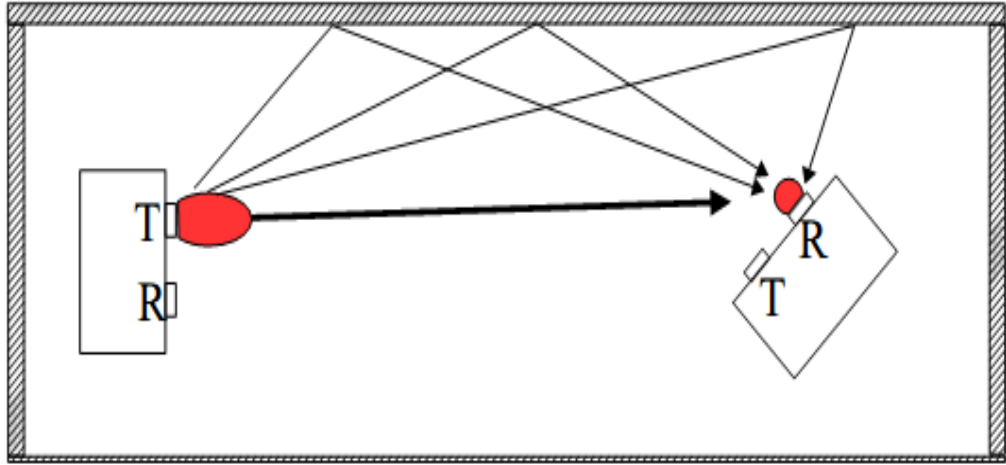
– Yakın kızılötesi (NIR, IR-A) : 0.75-1.4 μm dalgaboyları arasındadır. Düşük kayıp miktarı yüzünden genellikle fiberoptik iletişimde kullanılmaktadır. Gece görüş ekipmanları da genellikle bu dalgaboyunu kullanır.

– Kısa dalga kızılötesi (SWIR, IR-B) : 1.4–3 μm dalgaboyları arasındadır. Özellikle 1.53-1.56 μm sınırlarında uzun mesafeli haberleşmeye imkan verirler.

– Orta dalga kızılötesi (MWIR, IR-C): 3-8 μm . G d ml  f ze teknolojisinde kullanılmaktadır.

– Uzun dalga kızıl tesi (LWIR, IR-C): 8–15 μm . Dışarıdan bir ışınım kaynağına gerek duymadan sadece nesnelerin yaydığı ısıyla  alışan termal g r nt leme cihazları bu bandı kullanır.

– Uzak kızıl tesi (FIR): 15-1000 μm . Patlayıcı ve kimyasal silah detekt rleri bu bandı kullanmaktadır.



 ekil 2.2: Tipik Kablosuz İletişim Sistemi [46]

Kızıl tesi iletişimde, bir LED g r n r olmayan ışık patlamaları halinde kızıl tesi sinyal g nderir. Alıcıda bir fotodiyot veya fotoresept r ışık darbelerini algılar ve yakalar, sonra i erdikleri bilgiyi almak i in i leme tabi tutar. Kablosuz kızıl tesi iletişim, bir aktarım ortamı olarak yakın kızıl tesi bantta ışık dalgalarının serbest uzay yayılımını iletişim i in kullanmasıdır. İletişim bir taşınabilir cihaz ile başka bir taşınabilir cihaz arasında olabileceği gibi, taşınabilir cihaz ile sabit cihaz arasında da olabilir [46].

B. KIZILÖTESİ IŞINLARIN KULLANIM ALANLARI

Yeni nesil elektronik bilgi sistemleri geliştikçe, tüm insanların bilgiye, bu sistemler üzerinden erişimleri daha önemli hale gelmektedir. Kızılötesi teknolojisi, giderek artan uygulamaları ile bilgi kaynaklarına erişmede büyük bir potansiyele sahiptir.

Kızılötesi teknolojisinde bazı yaygın uygulamalar aşağıda listelenmiştir [47].

- Araba kilitleme sistemleri
- Bilgisayarlar (fare, klavye, disket sürücü, yazıcı)
- Acil müdahale sistemleri
- Çevre kontrol sistemleri (pencereler, kapılar, ışıklar, perdeler, yataklar, radyolar vs.)
- Kulaklıklar
- Ev güvenlik sistemleri
- Navigasyon sistemleri
- Telefonlar
- TV, VCR, CD çalarlar
- Elektronik Oyuncak Sektörü

Kızılötesi ışınların kullanım yerleri son yıllarda yaygınlaşmıştır. Pek çok maddenin kimyasal analizi bu tür ışınların yardımıyla gerçekleştirilmektedir. Özellikle İkinci Dünya Savaşında yansıyıp gelen kızılötesi ışınların görünür hale getirilmesiyle, karanlıktaki cisimler fark edilmiştir. Bu tür ışınların ısı etkisini kullanan fırınlar ve cilt hastalıkları tedavisinde kullanılan lambalar yapılmıştır. Geliştirilen yeni hassas filmlerle, ışık vermeyen fakat sıcak cisimlerin fotoğrafını çekmek mümkün olmaktadır. Bu tür fotoğraflar gün ışığında olabildiği gibi, karanlıkta da çekilebilir. Özellikle askeri sahada kullanılması gün geçtikçe artmaktadır.

Ayrıca vücudun sıcaklık durumunun araştırılmasında, sanayide ve gözle görülemeyen yıldızların tespitinde, astronomide kullanılır. Bunun

yanında polisiye olaylarda görülmeyen yazıların, parmak izlerinin ve lekelerinin tespitinde de istifade edilir.

Bu uygulamalar temel başlıklar altında toplanabilir.

- İki kullanıcı arasında kısa vadeli kablosuz bilgi alışverişi. Örnek; IrDA (Infrared Data Association) sistemleri.
- Bina içi kablosuz yerel alan şebekeleri. Örnek; IEEE 802.11 standardı.
- Yüksek hızlı şebeke ya da kampus alan ağı erişimi.
- Kablosuz giriş veya kontrol cihazları. (Kablosuz klavye ve fareler, uzaktan kumandalar vb.)

C. IrDA (INFRARED DATA ASSOCIATION)

1993 yılında, iletişim ve bilgisayar sektöründeki liderler kızılötesi kablosuz veri aktarımı için standart oluşturmak amacı ile "Infrared Data Association" (IrDA) şemsiyesi altında toplandılar. Günümüzde dünya genelinde 150'nin üzerinde üyesi bulunmaktadır.

IrDA, kablosuz iletişim teknolojisinde düşük maliyetli, birlikte çalışabilir, kolay kullanımlı cihazlar için standartlar oluşturmaktadır. IrDA tarafından her yıl 40 milyonun üzerinde IR data haberleşmesi yapan cihaz (PC, PDA, dijital kamera, mobil telefon, printer vb.) tanımlanmaktadır.

IrDA standartları serbest uzayda kızılötesi haberleşme linklerini kullanan cihazlar arasında noktadan noktaya ya da çoklu iletişimi kolaylaştırmak için tasarlanmıştır. Temel ihtiyaçlar olarak, bir cihaza IR özelliğinin eklenmesi için marjinal maliyetin 5 USD olması, IrDA haberleşmesinin 10 cm-1 m arasında gerçekleşmesi, veri hızının 115 kb/s üzerinde olması, görüş açısının 15-30 derece olması tespit edilmiştir [48]. IrDA iletişim standartları Tablo 2.1'de gösterilmiştir.

Tablo 2.1: IrDA İletişim Standartları

Versiyon	Link Tipi	Link Menzili	Veri Hızı	Modülasyon
1.3	noktadan noktaya	1 m	2.4-115.2 kb/s	RZ-3/16
1.3	noktadan noktaya	1 m	576 kb/s 1152 kb/s	RZ-1/4 RZ-1/4
1.3	noktadan noktaya	1 m	4 Mb/s	4-PPM
VFIR/1.4	noktadan noktaya	1 m	16 Mb/s	OOK
AIR (Advanced IR)	ağ	4m 8m	4 Mb/s 250 Mb/s	

1. IrDA Protokolleri

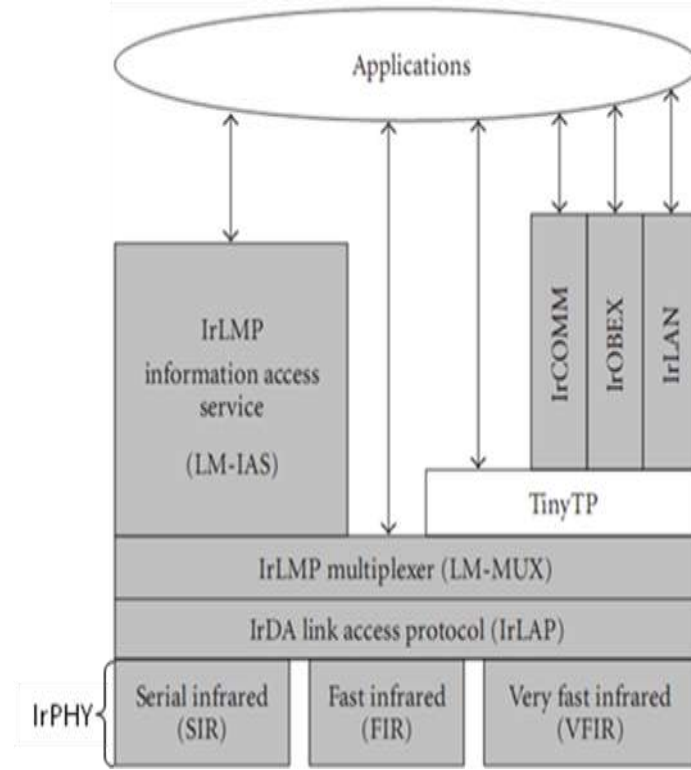
a. IrPHY (Infrared Physical Layer)

Kablosuz kızılötesi ortamda verilerin iletimi ve alımı için optik, optoelektronik ve elektronik bileşenleri sağlar. Çoğu yazılım bileşenleri olarak uygulanmasına rağmen, fiziksel katman çerçeve yapısını ve döngüsel artıklık denetimini (CRC) kullanan hata algılama fonksiyonlarını içerir. CRC başarısız olan çerçeveler atılır ve bir üst katmana (IrLAP) geçemez [49].

b. IrLAP (Infrared Link Access Protocol)

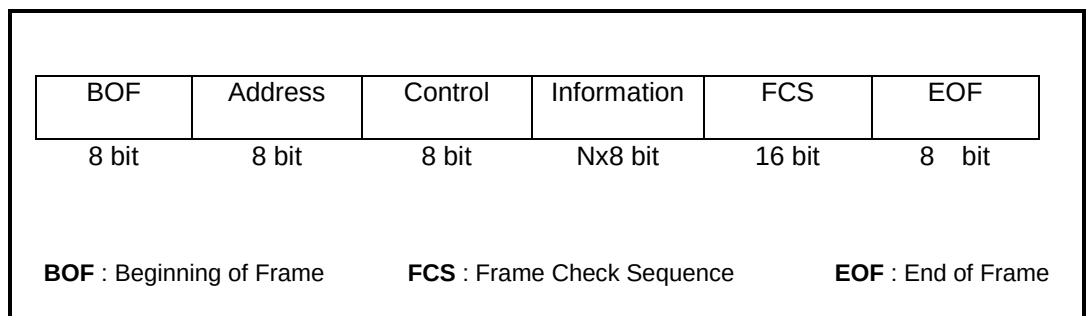
İlk uygulamaya konulduğunda (High Level Data Link Control in Normal Response Mode (HDLC-NRM)) olarak adlandırılmıştır. Genel olarak çerçeve (frame) yapısı içinde haberleşme olur ve IrDA cihazlarının kendi aralarında anlaşmazlığa düşmesini engeller. Kritik haberleşme parametreleri (iletilecek veri hızı, maksimum paket uzunluğu, minimum ve maksimum aralıklar vb.) haberleşme süresince karşılıklı olarak kontrol edilir. Tüm görüşmeler ve bağlantı trafiği 9600 b/s hızında gerçekleşir [50]. Temel olarak link kurma, adres bulma, bağlantı başlatma, veri alışverişi, link kapatma,

adres uyuşmazlık çözümü, yeniden iletim için otomatik tekrar isteği (ARQ) prosedürleri vardır [51].



Şekil 2.3: IrDA Protokol Yapısı [52]

IrLAP, iki alt katmandan oluşur : IrMAC (IR Media Access Control) ve IrLC (IR Link Access Control). IrMAC katmanı taşınabilir cihazlar arasındaki IR ortama erişimi koordine etmekle sorumludur. IrLC katmanı link kurulumu ve adres bulma prosedürlerini belirler.



Şekil 2.4: IrLAP Çerçeve (Frame) Yapısı

c. IrLMP (Infrared Link Management Protocol)

Dizüstü bilgisayar, PDA gibi cihazların yaygın olarak kullanımıyla birlikte IrLAP çoklu uygulamalarda yetersiz hale gelmeye başlayınca IrLMP doğmuştur. IrLMP amacı veri akışını kontrol ve farklı yeteneklerdeki daha fazla cihazın konfigürasyonudur. Birkaç uygulamanın haberleşmesini çoklama, link yönetimi ve servis bulmayı kapsayan çoklu yazılım uygulamalarının her düğümde bağımsız olarak çalışmasını sağlar. IrLMP, LM-MUX (Link Management Multiplexer) ve LM-IAS (Link Management Information Access Service) katmanlarından oluşmaktadır.

d. TTP (Tiny Transport Protokol)

Bu katman cihazlar arasında sanal kanalları yönetir, hata düzeltmeleri (paket kayıpları vs.) yapar, verileri paketlere böler ve paketleri birleştirerek orijinal veriyi elde eder. Bağlantı akış kontrolü ile en iyi durumdaki verinin iletilmesini sağlar. Uçtan uca veri iletimi uygulamaları için önemlidir [48,52].

e. IrCOMM (Infrared Communications Protocol)

Kızılötesi cihazın bir seri bağlantı noktası gibi davranmasını sağlar. Kızılötesi ortam half-duplex yapıya sahiptir. Yani aynı anda sadece bir yöne veri akışı gerçekleştirilebilir. IrCOMM veri aktarmak için seri bağlantı noktası sürücüsü olarak uygulanır. Mobil telefonlarda geniş bir uygulama alanı bulmuştur.

f. IrLAN (Infrared Local Area Network Protocol)

Kızılötesi cihaza yerel alan ağına bağlanma olanağı sağlar. Tıpkı ağ bağlantı kartı sürücüsü gibi davranır.

g. IrOBEX (Infrared Object Exchange)

Kızılötesi cihazlar arasında veri nesnelerinin alışverişini gerçekleştirir. IrDA'nın http'si olarak düşünülebilir. Veri nesnelerini, üstverileri (meta-data) de içeren başlık kısımlarıyla birlikte transfer eder.

D. STANDART IR İLETİŞİM PROTOKOLLERİ

IR, bir cihazı görülebilen bir mesafeden uzaktan kontrol etmenin en ucuz ve kullanışlı yollarından birisidir. IR ile gönderilen bilgi sıklıkla ikili (binary) diziler halindedir. Genellikle iletişim için tek kanal kullanılır ve seri iletişim gerçekleştirilir.

Modülasyon ile IR ışık kaynağı 40 KHz. gibi belirli bir frekansta yayım yapar. IR alıcı modülü de aynı frekansa ayarlı olduğundan bunun dışındaki tüm frekansları filtrelemektedir. IR uzaktan kumandalı haberleşme için 32-40 KHz. arasında modüleli kare dalga işaretini kullanır. Bu devreler ışık içerisinden 1-4 KHz. dijital işaretleri göndermek için kullanılırlar. Bu durumda maksimum ulaşılabilir hız 1000-4000 bps olmaktadır. Verici osilatörü belirli bir lojik seviye uygulayarak, IR verici LED inin açma/kapama işlemlerini sürmektedir. Burada uzaktan kumanda devresi bir vericidir.

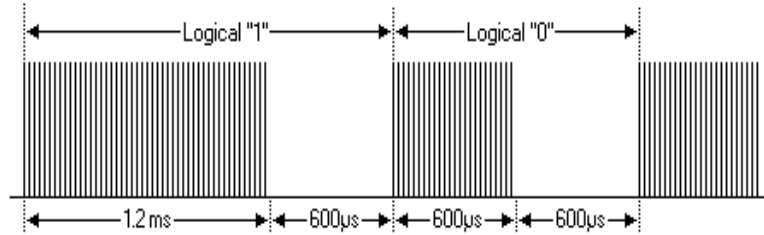
Alıcı tarafında bir foto diyot vericinin gönderdiği IR dalgasını alır. Alıcıdaki entegre devre 32-40 KHz. arasında belirli bir frekansa akorlanmışır. Çıkış ise demodüle edilmiş dijital giriştir. Bir uzaktan kumanda modülü ile gönderilen IR sinyalinin algılanabilmesi için farklı uzaktan kumanda modüllerinin gönderme bilgilerinin bilinmesi gerekir. Bunun için çeşitli metot ve protokoller geliştirilmiştir [27].

Temel olarak üç tip IR protokolü vardır, bu protokoller :

- Pulse coded protocol
- Space coded protocol
- Shift coded protocol

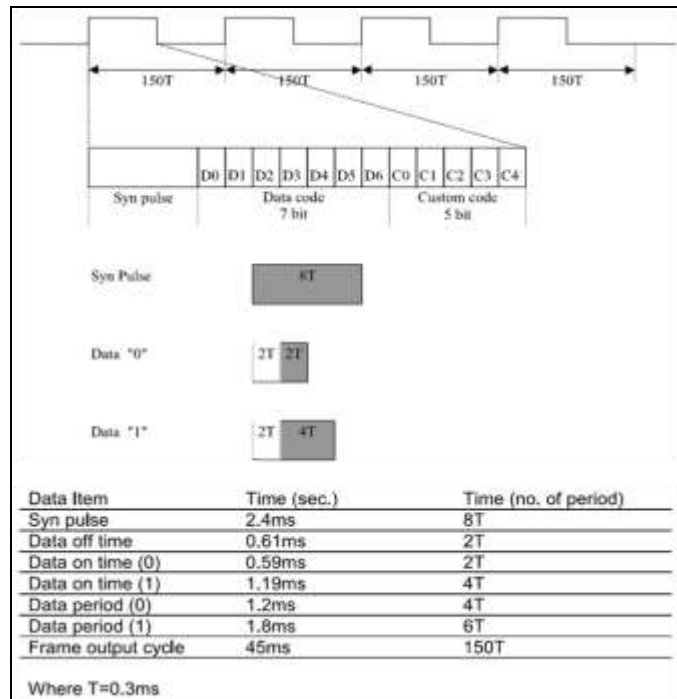
1. Pulse Coded Protocol

Pulse coded protokolünde bir palsin seviyelerinin uzunluğu değiştirilerek "0" ve "1" seviyeleri oluşturulmaktadır [41].



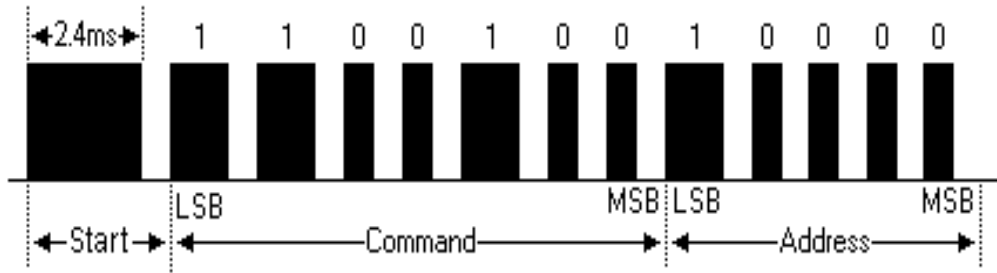
Şekil 2.5: Pulse Coded Protocol

Sony protokolü pals kodlu protokollerden birisidir. Genellikle 480 KHz. lik sinyalin 1/12'si olarak 40 KHz. modüleli taşıyıcı frekansını 1/3 duty cycle ile kullanır. 40 KHz. taşıyıcı üzerinde toplam 12-bit bilgi bulunmakta olup, bunun beş biti adresleme için (TV, VCR, DVD gibi farklı cihazları işaret etmek üzere), yedi biti ise komutlar için (uzaktan kumanda üzerindeki butonları göstermek üzere) ayrılmıştır.



Şekil 2.6: Sony Protokolünde Zamanlama Diyagramları

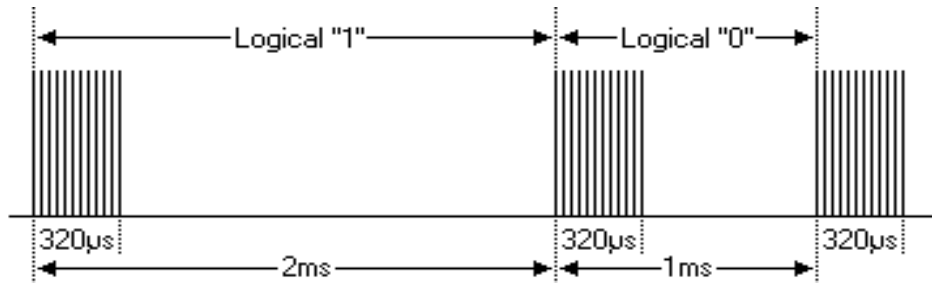
Kodlar 2.4 ms. start bitinden sonra başlamaktadır. Pals genişliği lojik “1” için 1.2 ms. olup, lojik “0” için ise 0.6 ms. süreye sahiptir. Uzaktan kumanda tuşu basılı tutulduğu sürece her 45 ms.’de bir komutlar tekrar tekrar gönderilir. Hem adres hem de komut kodları için seri iletişimde LSB ilk gönderilen bit iken MSB biti en son gönderilir. Şekil 2.7’de Sony protokolüne ait bir sinyal bilgisi görülmektedir.



Şekil 2.7: Sony Protokolünde Başlangıç Biti, Komut ve Adres Kodları

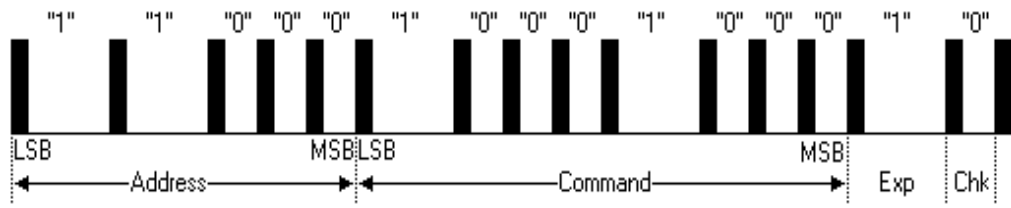
2. Space Coded Protocol

Space coded protokolünde palsler arasındaki boşlukların uzunluğu değiştirilerek “0” ve “1” seviyeleri elde edilir.



Şekil 2.8: Space Coded Protocol

Sharp bu protokolü uygulamaktadır. Sharp protokolü Sharp VCR kullanımı için geliştirilmiş olan 38 KHz. taşıyıcı frekansına sahip olan 13-bit protokoldür. Bunun dışında kod çözme işleminde kullanılmayan “expansion” ve “check” adında iki ilave bit daha vardır. İlk beş bit adresleme için, kalan sekiz bit ise komut kodları için ayrılmıştır. Şekil 2.9’da Sharp protokolüne ait bir sinyal bilgisi görülmektedir.

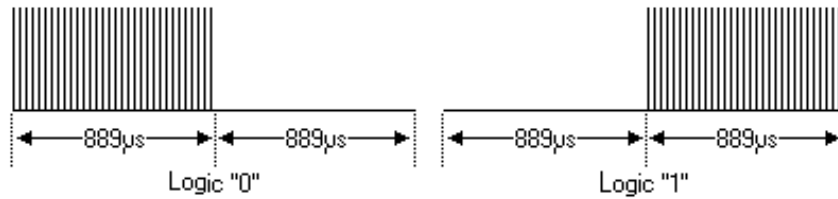


Şekil 2.9: Sharp Protokolünde Başlangıç Biti, Komut ve Adres Kodları

Bu protokolde “1” ve “0” lojik seviyeleri iki boşluk palsi arasındaki HIGH sürenin uzunluğu tarafından belirlenir. Pals genişliği 0.68 ms. ise lojik “0”, 1.68 ms.ise lojik “1” olarak belirlenmektedir. Palsler arasında standart olarak 0.32 ms. aralık bırakılmaktadır. Herhangi bir tuşa basıldığında 40 ms. gecikme ile kod iki kez gönderilir.

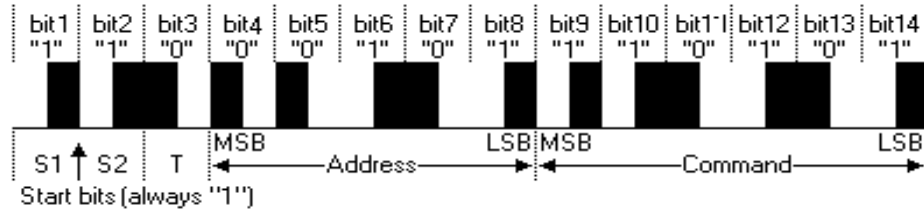
3. Shift Coded Protocol

Shift coded protokolünde ise geçişlerin yönü “0” ve “1” seviyelerini oluşturur ve tüm bitler sabit periyot süresine sahiptir [41].



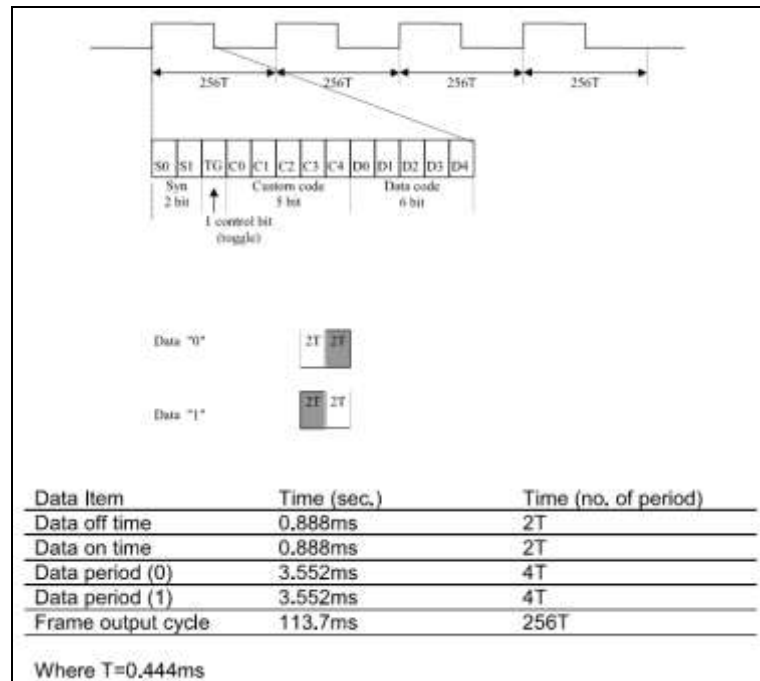
Şekil 2.10: Shift Coded Protocol

Philips bu protokolü kullanmaktadır [53]. Philips protokolü 36 KHz. taşıyıcı frekansına sahip olan 11-bit protokoldür. Bir bit süresi 1.778 ms. dir. Uzaktan kumanda tuşu basılı tutulduğu sürece her 113.7 ms.'de bir komutlar tekrar tekrar gönderilir. Beş bit adres, altı bit komutlar için ayrılmıştır. Şekil 2.11'de Philips protokolüne ait bir sinyal bilgisi görülmektedir.



Şekil 2.11: Philips Protokolünde Başlangıç Biti, Komut ve Adres Kodları

İlk iki bit start biti olup ikisi de lojik "1" dir. Üçüncü bit ise kontrol bitidir. Bu bit uzaktan kumandanın tuşuna basıldığında ya da bırakıldığında her defasında değişir. Bu sayede alıcı, vericinin tuşuna basılı kaldığını ya da tekrar basıldığını algılayabilir. Hem adres hem de komut kodları için seri iletişimde MSB ilk gönderilen bit iken LSB biti en son gönderilir.



Şekil 2.12: Philips Protokolünde Zamanlama Diyagramları

III. IR İLETİŞİMDE KULLANILAN MİKRODENETLEYİCİLER

A. MİKRODENETLEYİCİLERİN GENEL ÖZELLİKLERİ

Bir mikrodnetleyici ierisinde bir merkezi iřlem birimi (CPU), RAM (random-access memory), ROM (read-only memory), I/O (giriř/ıkıř hatları), seri ve paralel portlar, zamanlayıcılar, Analog/Sayısal dnřtrcler ve Sayısal/Analog dnřtrcler gibi yerleřik evresel arabirimler bulunmaktadır. Mikrodenetleyicilerin en nemli zellięi bir programı saklayabilmesi ve alıřtırabilmesidir. Bir mikrodnetleyici ile mikroıřlemciyi ayıran temel fark, tek bir yonga ierisinde CPU, RAM ve I/O nitelerinin yerleřtirilmiř olmasıdır.

Bir PC ve onu oluřturan mikroıřlemciyle karřılařtırıldıęında; fiziksel boyutunun kk olması, dřk g tknetimi, ucuz olması ve de yksek performansa sahip olması gibi belirgin avantajlara sahiptir. Mekatronik uygulamaları, endstriyel elektronik, biyomedikal, otomasyon sistemleri gibi farklı disiplinlerde ok eřitli uygulama alanlarında; otomobillerde, cep telefonlarında, kameralarda, fotokopi cihazlarında, LCD monitr uygulamalarında, ev elektronięinde, amařır/bulařık makinesi ve fırın gibi cihazlarda, telefon, faks, modem, elektronik oyuncak sektr gibi alanlarda yaygın olarak kullanılmaktadır.

Mikrodenetleyicilerin tek bařlarına programları alıřtırabilme ve depolama yetenekleri sayesinde ok ynl uygulamalarda kullanılabilen ucuz bir kontrolr durumuna getirmiřtir. Yapılan bir program ile nceden belirlenen durumlar yerine getirilirken istenen fonksiyonlar oluřturulup gereken kararlar aldırılabilir [54].

Neredeyse her mikroıřlemci (CPU) reticisinin rettięi birkaç mikrodnetleyicisi bulunmaktadır. Bu denetleyicilerin mimarileri arasında ok kk farklar olmasına raęmen ařaęı yukarı aynı iřlemleri yapabilmektedirler. Her firma rettięi yongaya bir isim ve zelliklerini birbirinden ayırmak iin de

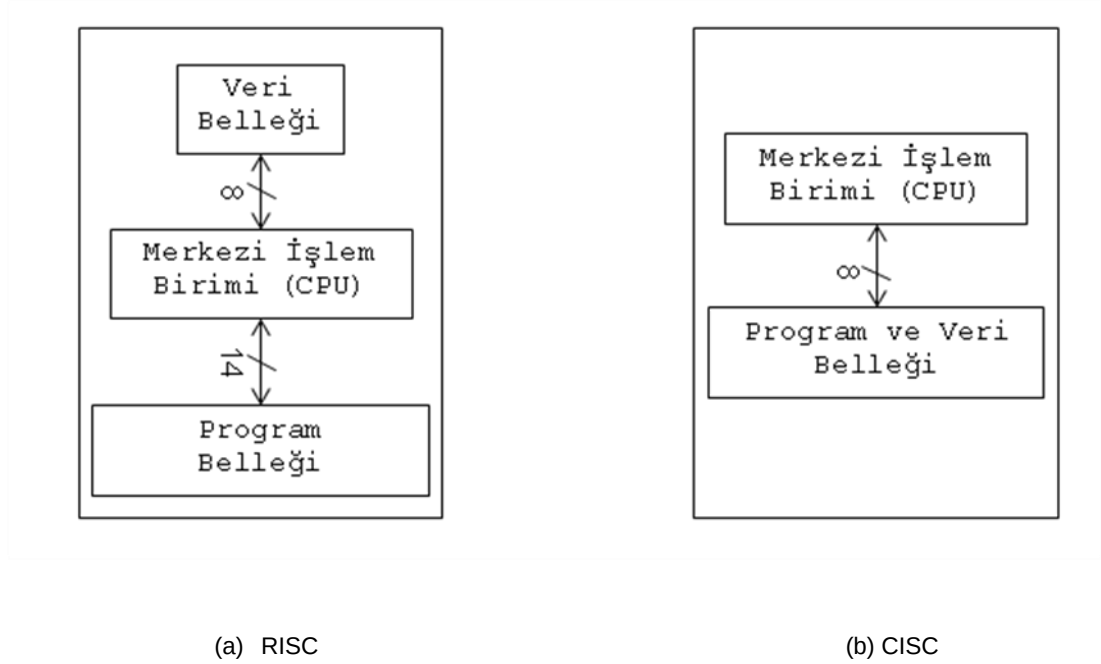
para numarası vermektedir. rneęin Microchip Technology firması rettiklerine PIC adını, para numarası olarak da 12C508, 16C84, 16F84, 16C711 gibi kodlamalar verir. Intel ise rettięi mikrodenetleyicilere MCS-51 ailesi adını vermektedir. Genel olarak bu adla anılan mikrodenetleyici ailesinde farklı zellikleri bulunan rnleri birbirinden ayırt etmek iin para numarası olarak da 8031AH, 8051AH, 8751AHP, 8052AH, 80C51FA gibi kodlamalar kullanılmaktadır. Bir uygulamaya bařlamadan nce hangi firmanın rn kullanılacağına, daha sonra da hangi numaralı denetleyicinin kullanılacağına karar vermek gerekir. Bunun iin mikrodenetleyici gerektiren uygulamada hangi zelliklerin olması gerektięi nceden bilinmesi gereklidir. Ařaęıda bu zellikler sıralanmıřtır:

- Programlanabilir dijital paralel giriř/ıkıř.
- Programlanabilir analog giriř/ıkıř.
- Seri giriř/ıkıř (senkron, asenkron ve cihaz denetimi gibi).
- Motor veya servo kontrol iin pals sinyali ıkıřı.
- Harici giriř vasıtasıyla kesme.
- Timer vasıtasıyla ile kesme.
- Harici bellek arabirimi.
- Harici bus arabirimi (PC ISA gibi).
- Dahili bellek seenekleri(ROM, EPROM , PROM ve EEPROM).
- Dahili RAM seeneęi.
- Kayan nokta hesaplaması.

B. PIC MİKRODENETLEYİCİLER

Microchip Technology firması tarafından retilen mikrodenetleyici yongaları PIC (Peripheral Interface Controller) “evresel Arabirim Denetleyicisi” olarak adlandırılmaktadır ve programlanabilen arabirim kontrolr olarak grev yapmaktadır. PIC, evresel niteler adı verilen lamba, motor, role, ısı ve ıřık sensr gibi I/O elemanların denetimini ok hızlı olarak yapabilecek řekilde dizayn edilmiř bir yongadır. Yapısında kullanılan mimariye baęlı olarak iki tr mikrodenetleyiciden sz edilebilir. “RISC

mikrodenetleyici” ve “CISC mikrodenetleyici”. RISC mimarisi terimine bilgisayar literatüründe yaygın olarak rastlanmaktadır. Açılımı “Reduced Instruction Set Computer” olup Harvard Mimarisi bu grubu oluşturmaktadır. Bu yapıda veri ve adres yolları ayrı ayrıdır. Daha hızlı bir şekilde ve daha fazla veriyi bir defada taşıyabilmek için tasarlanmış olan bu mimaride veri yolu 8-bit olup program belleğine ise 14-bit genişliğindeki farklı bir yol ile erişilir. Bu sebeple 16F84, 16F628 ve 16F87X mikrodenetleyicilerinde komut kodları 14-bittir.

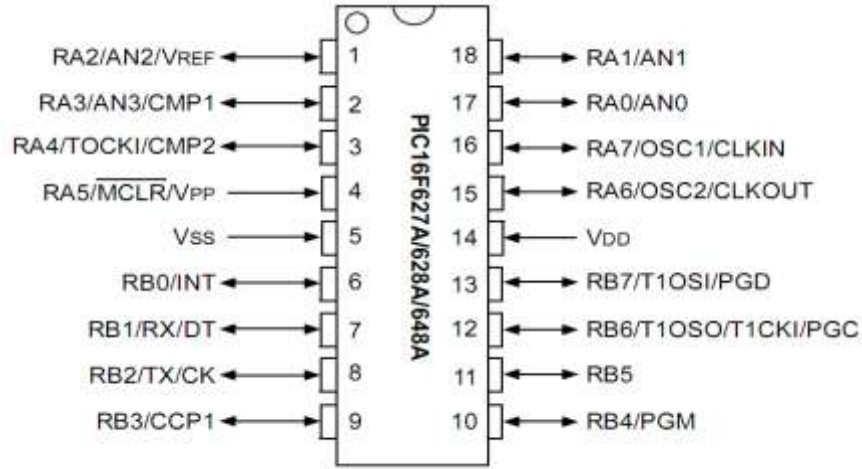


Şekil 3.1: RISC ve CISC Mimarileri

Diğer yapı “Complex Instruction Set Computer”, von Neumann mimarisini kullanmaktadır. Bu mimaride veri ve program belleğine sekiz bit genişliğinde aynı yol ile erişilmektedir.

Mikrodenetleyici veri ve adres bilgilerini içeren sözcükleri yazmaçlarda binary sayı formatında saklamaktadır. Program çalışırken bu yazmaçların içeriğine erişilebilir. Bazı yazmaçlara okuma/yazma yapılırken, bazı yazmaçların belirli bitleri sadece okuma amaçlı olarak belirlenmiştir [55].

1. PIC16F628A Mikrodenetleyici



Şekil 3.2: PIC16F628A Mikrodenetleyicisinin Pin Bağlantıları

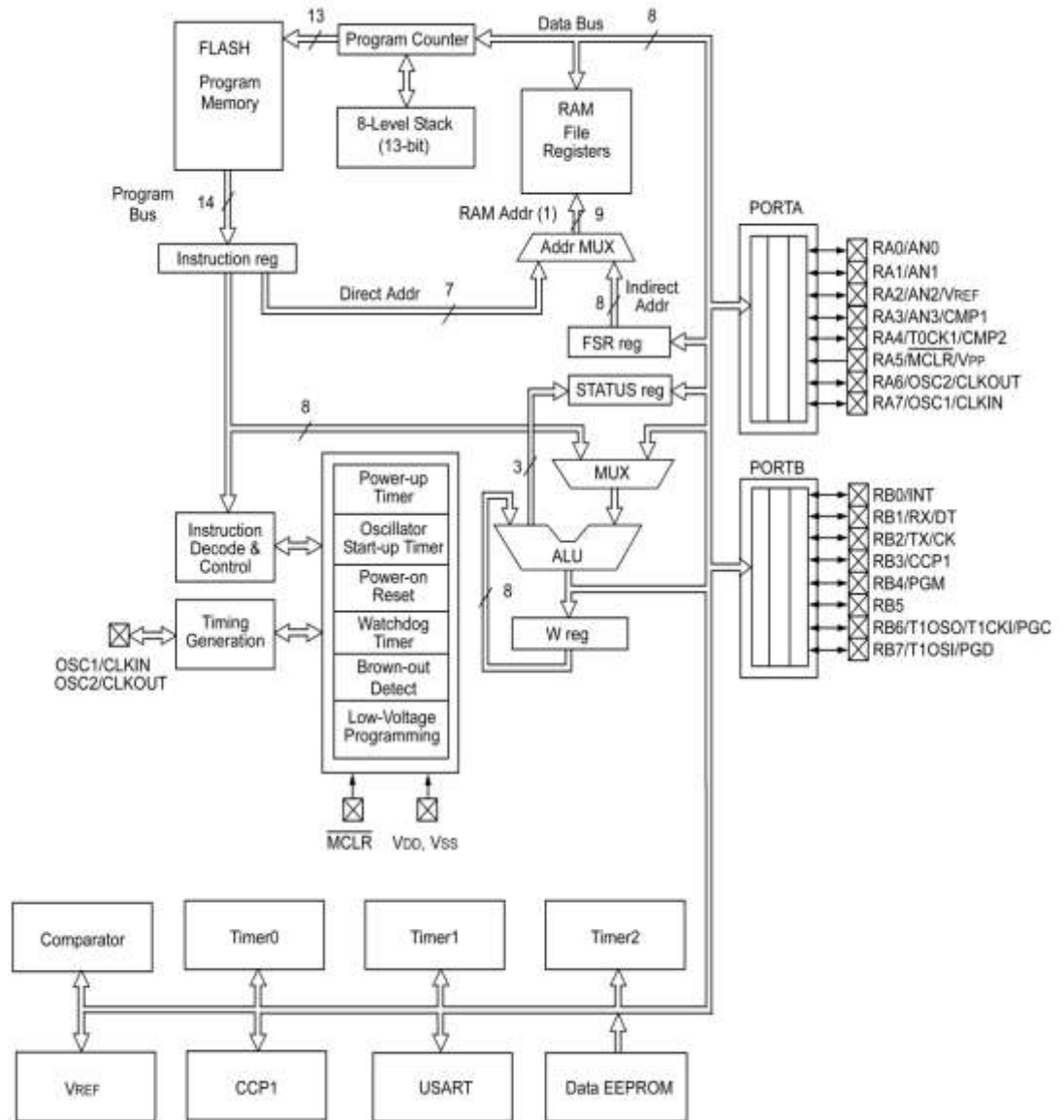
PIC16F628A, diğer mikrodenetleyiciler gibi RISC yapısı üzerine kurulu Harvard mimarisi ile üretilmiştir ve flaş program belleğine sahip PIC16CXX ailesinden sekiz bitlik bir mikrodenetleyicidir. PIC16F628'in mimari yapısından dolayı program ve veri bellekleri fiziksel olarak ayrı birimlerdedir ve bu belleklere farklı veri yolları ile erişilmektedir. Tablo 3.1'de PIC16F628'in genel özellikleri görülmektedir.

Tablo 3.1: PIC16F628A Genel Özellikleri

Saat Frekansı	En Yüksek Çalışma Frekansı	20 MHz
Bellek	Flash Program belleği	2 K
	RAM Belleği	224 byte
	EEPOM Belleği	128 byte
Çevresel Birimler	Zamanlama (TIMER) modülleri	TMR0, TMR1, TMR2
	Analog Karşılaştırıcı	2
	Yakala/Karşılaştırm/PWM Modülü	1
	Seri Haberleşme	USART
Diğer Özellikleri	Kesme Kaynağı	10
	Giriş/Çıkış Uç Sayısı	16
	Çalışma Gerilimi Aralığı	3-5.5V
	Brown-out Reset	Var
	Kılıf (Package) Biçimi	18-pin DIP, SOIC 20 pin SSOP

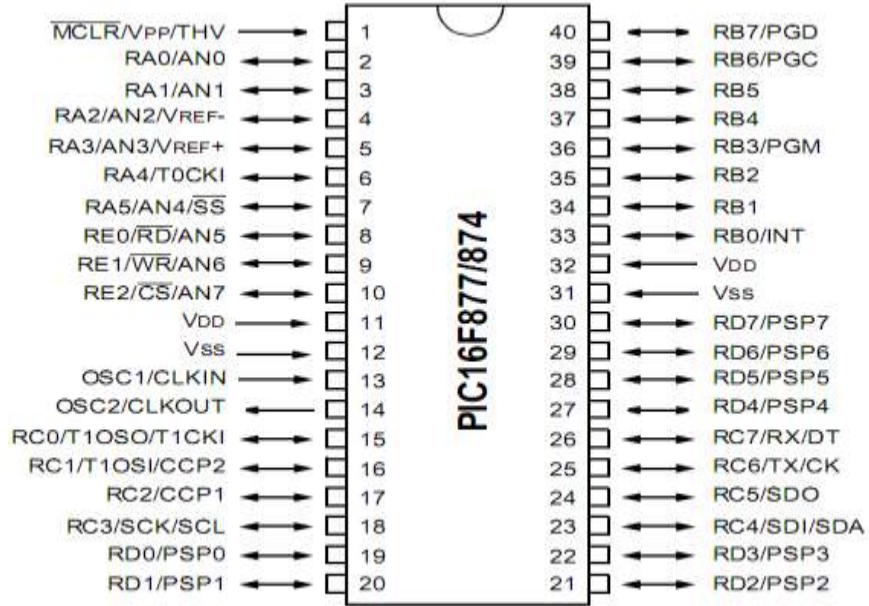
16F serisi diğer mikrodeneleyicilerde olduğu gibi 35 komut ile programlanabilir, dallanma komutları dışındaki tüm komutları tek komut saykılında işletebilir, işletim hızı DC-20 MHz.lik giriş zamanı, DC-200 ns.lik komut periyodudur.

16F628A mikrodeneleyicisi 2K x 14-bit flaş program belleğine sahiptir. Bu belleğe 100.000 kere program yazılıp silinebilir. 224 x 8 byte veri belleği (RAM) vardır. EEPROM belleği ise 128 x 8 byte olup 1.000.000 kez veri yazılabilir ve yazılan veri 100 yıl bellekte tutulabilir [56,57].



Şekil 3.3: PIC16F628A Mikrodeneleyicisinin Blok Diyagramı

2. PIC16F877A Mikrodenetleyici



Şekil 3.4: PIC16F877A Mikrodenetleyicisinin Pin Bağlantıları

PIC16F628A, RISC yapısı üzerine kurulu Harvard mimarisi ile üretilmiş mikrodenetleyicidir. Tablo 3.2’de PIC16F877A’nın genel özellikleri görülmektedir.

Tablo 3.2: PIC16F877A Genel Özellikleri

Çalışma Frekansı	20 MHz
Sıfırlama ve Gecikme	POR, BOR (PWRT,OST)
Flash Program Belleği (14-bit)	8 K
RAM Belleği	368 byte
EEPOM Belleği	256 byte
Kesme Kaynağı	10
Giriş/Çıkış Portları	Ports A,B,C,D,E
Zamanlayıcı	3
Analog Karşılaştırıcı	2
Yakala/Karşılaştır/PWM Modülü	2
Seri Haberleşme	MSSP,USART
Paralel Haberleşme	PSP
10-bit Analog/Dijital Modül	8 giriş kanalı
Komut Seti	35 komut
Kılıf (Package) Biçimi	40-pin PDIP, 44-pin PLCC, 44-pin TQFP, 44-pin QFN

IV. KABLOSUZ İLETİŞİMDE GÜVENLİK

Burada bahsedilecek olan kablosuz iletişim, bir sistemi uzaktan kumanda cihazı ile kontrol etmektir. Uzaktan kumandanın ilk örneklerinden biri, 1893 yılında Nikola Tesla tarafından geliştirilmiştir. 1903 yılında Leonardo Torres Quevedo, Telekino'yu Paris Bilim Akademisinde deneysel bir gösteri ile tanıttı. Telekino, elektromanyetik dalgalarla iletilen komutları yerine getiren bir robottu. Telekino uzaktan kumanda alanında bir öncü ve dünyanın ilk radyo kontrol cihazı olarak kabul edilmektedir.

Torres, 1906 yılında Bilbao Limanında kralın ve büyük bir kalabalığın önünde bir botu sahilden uzaktan kumanda ile başarılı bir şekilde yönlendirdi. İlk uzaktan kumandalı uçak 1932 yılında uçtu ve uzaktan kumanda teknolojisi yoğun olarak 2. Dünya Savaşı süresince askeri amaçlarla kullanıldı.

İlk televizyon uzaktan kumandası 1950'lerin ilk yarısında Zenith Radyo Şirketi tarafından geliştirildi. Bu uzaktan kumanda televizyona bir kablo ile bağlanmıştı. Bu ağır uzaktan kumandayı daha kullanışlı hale getirmek için 1955 yılında "Flashmatic" denen kablosuz uzaktan kumanda geliştirildi. Flashmatic'in çalışma prensibi bir fotoelektrik hücresi üzerine ışın demeti gönderilmesiydi.

1956 yılında Robert Adler, "Zenith Uzay Kumandası" adıyla kablosuz bir uzaktan kumanda geliştirdi. Kanalı ve ses şiddetini değiştirmek için mekanik ve ses ötesi tekniğini kullanıyordu. Kullanıcı uzaktan kumanda üzerinde bir düğmeye bastığında mekanik olarak meydana gelen çarpma sesi (her bir kanal için farklı frekansta) televizyon tarafından tespit edilip kanalın değiştirilmesini sağlıyordu. Transistörün bulunmasıyla piezoelektrik kristalleri içeren uzaktan kumandaların geliştirilmesi ile bu teknik daha ucuz ve kullanılabilir hale geldi. Ancak, ksilofon ve benzeri ses çıkaran aletlerin uzaktan kumanda ile aynı frekansta çalışabildiği ve istemsiz kanal değişikliklerine sebep olması nedeniyle bu tekniğin çok kullanışlı olmadığı anlaşıldı.

Televizyon kumandalarında daha fazla özellik arayışı, BBC'nin Ceefax teleteks servisini geliştirmesiyle 1970'lerin sonlarına doğru ortaya çıktı. Çoğu uzaktan kumanda, sınırlı sayıda özellik sunuyordu. Bazı kumandalarda sadece dört tane tuş vardı: sonraki kanal, önceki kanal, ses yükseltme ve ses azaltma. Bu tür kontroller, üç basamaklı sayılarla ifade edilen teleteksin sayfalarının ihtiyacını karşılamıyordu. Bir sayfanın görüntülenebilmesi için bir uzaktan kumandanın, sıfırdan dokuza rakam tuşlarına ve buna benzer başka kontrol tuşlarına ihtiyacı vardı. Önceleri kablolu olan uzaktan kumandanın sürekli kullanılması sonucu kablosuz olmasına ihtiyaç duyulmuştur. Bu nedenle BBC mühendisleri, bazı televizyon üreticisi firmalarla görüşerek 1977-78 yıllarında daha çok özellik içeren ilk kablosuz uzaktan kumanda örneklerini geliştirdiler. Bu şirketlerden bir tanesi olan ITT daha sonra kendi adıyla anılacak olan ITT kızılötesi iletişim protokolünü geliştirmiştir.

1980'lerin başından itibaren infrared teknolojisi ile çalışan uzaktan kumanda cihazları üretilmeye başlanmıştır. Kablosuz uzaktan kumanda sistemleri hayatın her alanında sıklıkla kullanılmaya başlanmıştır. Günlük hayatta güvenlik gereksinimi olan ev, ofis, garaj gibi birimlere güvenli/kayıtlı giriş sistemleri uzaktan kumanda cihazları ile kontrol edilmektedir. Hedef sisteme istenilen bilgiyi göndermek için kullanılan temel teknikler infrared ya da RFID tabanlı teknolojilerdir [27].

A. KİMLİK DOĞRULAMA

Kablosuz iletişimde güvenliği tehdit edici faktörler; yetkisiz kişilerin sisteme girerek gönderilen iletiyi ele geçirmesi, sahte kaynaklardan ileti gönderilmesi, kaynaktan gönderilen iletinin alıcıya doğru olarak iletilememesi olarak sıralanabilir. Bu tür tehditlerin önüne geçebilmek için çeşitli kimlik doğrulama teknikleri kullanılmaktadır.

1. Sabit Şifre Tekniği

Bu teknikte kaynaktan alıcıya önceden tanımlanmış olan sabit bir şifre gönderilir. Alıcı şifreyi aldığı anda şifrenin doğruluğunu kontrol eder, eğer doğru ise önceden tanımlanmış olan işlevi yerine getirir.

2. Değişken Şifre Tekniği

Bu teknikte ise kaynak, her gönderim için farklı bir şifre kullanır. Ayrıca bu teknikte kullanılan bir de sıralama sayacı vardır. Bu sayacın içeriği her kullanımda bir artmaktadır. Alıcı kısmında da bir sayaç işletilir. Alıcı şifreyi aldığı anda kendi belleğindeki şifreler ile karşılaştırır. Eğer şifre doğru ise şifrenin sıra numarasını kendi sayaç numarası ile karşılaştırır. Her iki numara arasındaki fark daha önceden belirlenmiş belirli bir sınırın içerisinde ise alıcı kaynağın kimliğini doğrular ve istenilen işlevi yerine getirir.

3. Soru-Cevap Tekniği

Bu teknik immobilizer sistemlerinde geniş ölçüde kullanılır. Kısaca IFF (identify friend or foe) olarak da bilinmektedir [60]. Kaynak ve alıcının her ikisinde de aynı gizli şifreleme anahtarı bulunur. Alıcının bulunduğu sistem açılmak istendiğinde (örneğin, otomobilin kapı kolu çekildiğinde), alıcı sorgulama için kaynağa rastgele bir bilgi gönderir. Kaynak bu bilgiyi şifreleme anahtarı ile şifreledikten sonra alıcıya tekrar gönderir. Alıcı da göndermiş olduğu bilgiyi kendisindeki anahtar ile şifreler ve kaynaktan gelen şifreli bilgi ile karşılaştırır. Her iki şifreli bilgi aynı ise alıcı, kaynağı tanır ve istenilen işlevi yerine getirir.

B. SALDIRILAR

Kimlik doğrulama tekniklerine karşılık kablosuz iletişim ortamında sisteme dışarıdan müdahale etmek isteyenler tarafından kullanılan çeşitli

saldırı teknikleri vardır. Bu teknikler temel başlıklar altında aşağıdaki gibi toplanmıştır [61].

1. Tarama

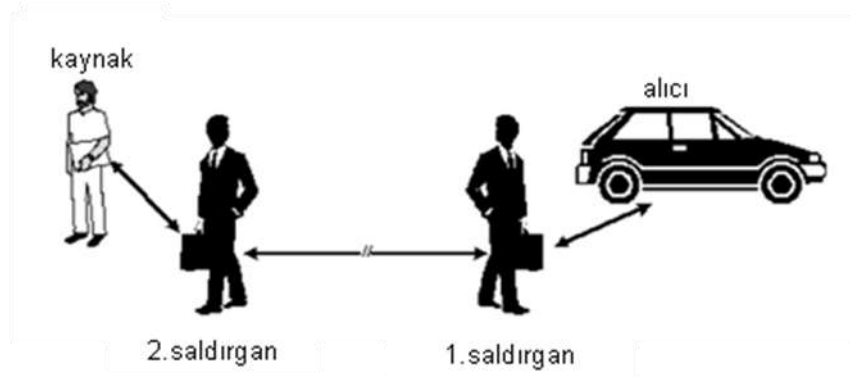
Değişken şifre tekniğinde kaynak her seferinde farklı bir şifre göndermektedir. Sisteme girmek isteyen saldırgan aynı şifreyi defalarca göndererek alıcının belleğindeki şifrelerden birini yakalamaya çalışır. Burada saldırganın deneme yapma şansı alıcıdaki sıralama sayacına, sayaç yoksa şifreyi oluşturan bit sayısına bağlıdır. Sabit şifre tekniği kullanan bir sistemde ise saldırgan her seferinde farklı şifre kombinasyonlarını dener. Saldırganın doğru şifreyi bulma olasılığı şifrenin bit sayısına bağlıdır.

2. Tekrarlama

Kaynak şifreyi gönderirken saldırgan iletim ortamına girerek şifreyi kaydeder. Kaydettiği bu şifreyi daha sonra sisteme girmek için kullanır. Ancak bu teknik her defasında aynı şifreyi kullanan sistemler için başarılı sonuç verebilir.

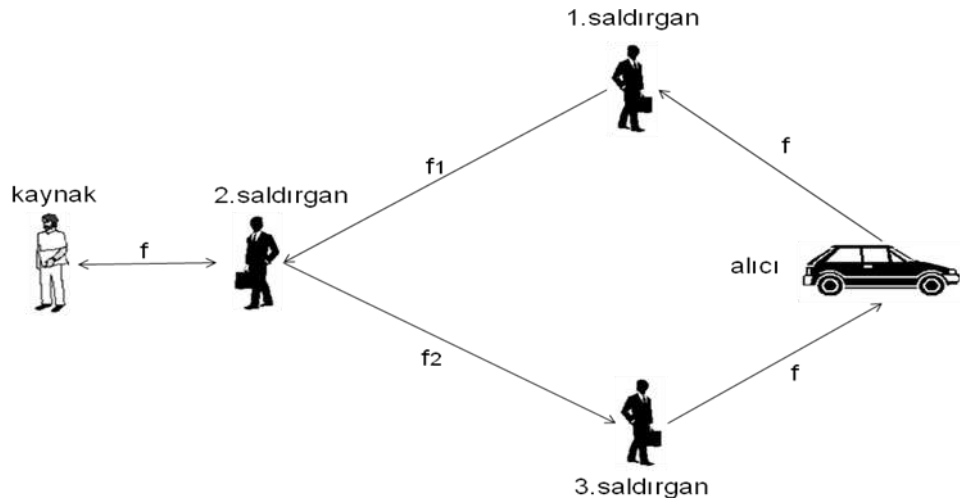
3. İkili Hırsızlık

Bu tür saldırılar soru-cevap tekniği kullanılan sistemlere karşı sıklıkla kullanılan bir yöntemdir. İki kişi kaynak ile alıcı arasında elektronik bir köprü oluşturur. Kaynağın alıcıdan uzak olduğu bir sırada birinci saldırgan alıcının hemen yanında, ikincisi ise kaynağın yanında durur. Alıcının yanındaki saldırgan sisteme girmeye çalışarak alıcının sorgu sinyalini göndermesini sağlar. Gönderilen sinyali yükselterek ikinci saldırgana gönderir. İkinci saldırgan aldığı sinyali istenilen seviyeye düşürerek kaynağa iletir. Kaynaktan gelen cevabı birinci saldırgana iletir, birinci saldırgan da bu sinyali alıcıya ileterek sistemi açar. Saldırganların bu teknikle başarılı olmaları için sinyalin izlediği yol içerisinde bozulmalara uğramaması gerekir. Bu nedenle uygun elektronik donanıma sahip olmaları zorunludur.



Şekil 4.1: İkili Hırsızlık Tekniği

Sinyali bozulmalardan korumak için ikili yerine üçlü hırsızlık denilen tekniğin kullanımı da söz konusudur. Buradaki amaç saldırırlar arasında oluşturulan köprü iletişimde farklı frekans kullanarak kaynak ve alıcının kullandığı frekansta bozulmaların önüne geçmektir [62].



Şekil 4.2: Üçlü Hırsızlık Tekniği

4. Önceden Tahmin

Bu teknikte saldırgan alıcının önceki sorgu mesajlarını dikkate alarak sıradaki sorunun ne olabileceğini tahmin eder. Bu soruyu alıcıdan uzak bir noktada iken kaynağa ileterek cevabını kaydeder. Sisteme girmeye çalışarak alıcıdan sorgu mesajının gelmesini bekler. Gelen sorgu önceden tahmin ettiği sorunun aynısı ise kaynaktan alarak kaydettiği cevap ile sistemi açar.

5. Elektronik Sözlük

Bu teknikte ise saldırgan bir elektronik sözlük oluşturur. Sözlüğü oluşturmak için kaynağın yakınında bulunarak alternatif sorgu mesajları üretir ve her dafsında kaynağın verdiği cevapları kaydeder. Böylece soru-cevap ikilisinden oluşan geniş bir elektronik sözlük oluşturur. Daha sonra alıcının yanına giderek sistemi açmaya çalışır ve alıcıdan sorgu mesajının gelmesini bekler, gelen mesaja karşılık olarak sözlükten cevabı bulur ve bu cevapla sisteme giriş yapar.

C. RFID (RADIO FREQUENCY IDENTIFICATION)

RFID bir otomatik nesne tanımlama teknolojisidir. Bu sistemde etiketler ve etiket okuyucuları bulunmaktadır. Etiketler kişi ya da nesnelerin üzerine yerleştirilen, kimlik niteliğindeki küçük işaretlerdir. Etiket okuyucusu ise etiketle iletişim sağlayan elektronik cihazdır. Temel olarak RFID teknolojisini pasif ve aktif olarak ikiye ayırmak mümkündür. Pasif RFID sistemlerde etiketin besleme kaynağı yoktur, göndermiş olduğu sinyal vasıtasıyla anteni uyaran okuyucudan güç alırlar. Aktif RFID sistemlerde ise etiketi besleyen bir güç kaynağı vardır ve bu güç kaynağı sayesinde okuyucuya sinyal gönderilir. Okuyucu etiket üzerine bir radyo sinyali gönderir, etiketten yansıyan kimlik bilgisini alır [5].

EPC (Electronic Product Code) denilen kimlik bilgisi, etiketi taşıyan kişi ya da nesnenin tanımlayıcısıdır. Ancak bu tanımlayıcı ticari sektörde yaygın olarak kullanılmakta olan barkod sistemi gibi sadece nesneyi

tanımlayan bir yapıda değildir. Kişi ya da nesnenin temel tanımlayıcı bilgilerinin yanında açıklayıcı ek bilgileri de bu etikette saklamak mümkündür [63]. RFID, frekans bantlarına göre ise 13.56 MHz, 433 MHz, 860-960 MHz, 2.45 GHz olarak ayrılabilir [6].

RFID teknolojisi ilk kez 2. Dünya Savaşında kullanıldı. İngilizler müttefik uçaklarına birer verici yerleştirdiler. Yerden gönderilen radar sinyalinin alan verici sinyal yayınına başlıyor ve böylece radar, uçağın dost olduğunu anlayabiliyordu. Bu, tarihte bilinen ilk aktif RFID uygulamasıdır [64]. RFID 1970'lerden itibaren ticari sektörde de uygulama alanları bulmuştur.

Son yıllarda günlük hayatımızda da pasif RFID uygulamaları yer almaya başlamıştır (temassız kredi kartları, otoyollardaki otomatik geçiş sistemleri, toplu ulaşım araçlarında kullanılan ödeme kartları vb.).

Radyo frekansının görüş hattı olmaksızın uzun mesafeden iletişime olanak sağlamasına rağmen bazı dezavantajları da beraberinde getirdiğini söylemek mümkündür. Bunların en başında gelenler; yayınlanan RF sinyallerinin ortamda kolayca yakalanabilmesi ve benzer frekansları kullanan cihazların iletimi engelleme imkanının olmasıdır.

RFID teknolojisine alternatif olarak kullanılan bir diğer yöntem ise infrared sistemlerdir. Elektronik ev aletleri, giriş güvenlik sistemleri (ev, ofis, garaj kapısı vb.) ve daha bir çok alanda kullanılan uzaktan kumanda sistemleri genellikle IR teknolojisiyle çalışan sistemlerdir. IR tabanlı sistemler kısa mesafelerde güçlü, güvenilir ve maliyet-etkin çözümler sunabilmektedir. IR sistemlerinde alıcı ile verici arasında görüş hattı olması gerektiğinden sisteme dışarıdan girişler çok daha zor olmaktadır.

D. KIZILÖTESİ IŞINLAR İLE RADYO FREKANS DALGALARININ KARŞILAŞTIRILMASI

Kızılötesi teknolojinin kablosuz iletişimin bir formu olarak sunduğu önemli avantajlar vardır. Kızılötesi (IR) ile radyo frekansı (RF) avantaj ve dezavantajları aşağıda sunulmuştur [47,65,66].

IR Avantajları:

- Düşük güç gereksinimleri. (bu yüzden cep telefonları, dizüstü bilgisayarlar ve kişisel dijital asistanlar (PDA) için idealdir.)
- Düşük maliyet.
- Basit devre. (Özel bir donanım gerektirmez. Bir ürünün entegre devresi içine dahil edilebilir.)
- Yüksek güvenlik. (Işının yönlülüğü bilginin yakındaki cihazlara sızmasını engeller.)
- Taşınabilir.
- Uluslar arası düzenleyici kısıtlamalar. (IrDA fonksiyonel cihazlar uluslar arası seyahatlerde nerde olursa olsun kullanılabilir.)
- Yüksek gürültü bağışıklığı. (Diğer cihazların sinyal girişimi olası değil.)

IR Dezavantajları:

- Görüş hattı. (alıcı ve verici iletişim için birbirlerine doğrudan hizalanmalıdır.)
- İnsanlar, duvarlar, bitkiler vb. iletimi engelleyebilir.
- Kısa menzil.
- Işık, hava duyarlı. (doğrudan güneş ışığı, yağmur, sis, toz iletimi etkileyebilir.)
- Düşük hız. (Veri iletim hızı kablolu iletimden daha düşüktür.)

RF Avantajları:

- Görüş hattı gerekli değildir.
- Çevredeki materyallerden etkilenmez, bir çok katı maddeden ve duvardan geçebilir.
- Uzun menzilde haberleşmek mümkündür.
- Işık hassasiyeti yoktur.
- Çevre ve hava şartlarından etkilenmez.

RF Dezavantajları:

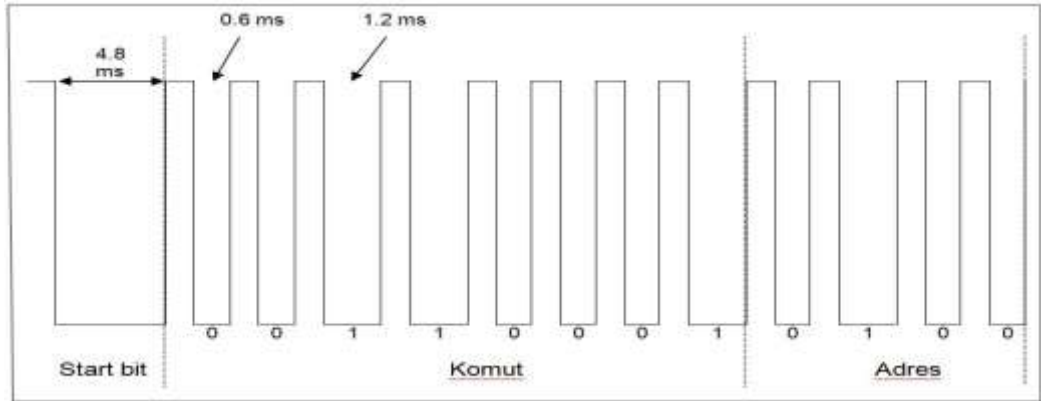
- Girişim. (Benzer frekansları kullanan cihazlar iletimi engelleyebilir.)
- Güvenlik eksikliği. (Yayınlanan RF sinyalleri kolaylıkla yakalanabilir.)
- Maliyeti kızılötesine göre daha yüksektir.
- Bazı RF cihazları için lisans gerekebilir.
- Düşük hız. (Veri iletim hızı kablo ve kızılötesine göre daha düşüktür.)

V. ASENKRON VERİ İLETİŞİM SİSTEMİ

A. IR İLETİŞİM PROTOKOLÜ

Bu çalışmada gerçekleştirilmiş olan IR uzaktan kumanda sisteminde pals kodlu protokol ile uyumlu, standart dışı özel bir iletişim protokolü tasarlanmıştır. 40 KHz. lik taşıyıcı sinyal üzerinde 12 bit bilgi bulunmakta olup, bunun dört biti adresleme için, sekiz biti ise komutlar için ayrılmıştır. Kodlar 4.8 ms start bitinden sonra başlamaktadır.

Pals genişliği lojik “1” için 1.2 ms olup, lojik “0” içinse 0.6 ms süreye sahiptir. Palsler arasında da 0.6 ms bekleme süresi vardır [41]. Şekil 5.1’de komut ve adres bitleri ve 4.8 ms start biti görülmektedir.



Şekil 5.1: Özel İletişim Protokolü Komut ve Adres Bitleri ve Süreleri

Bir komut paketinin gönderim süresi, gönderilen bilginin içeriğine bağlı olarak şu şekilde hesaplanabilir:

Komut ve adres kısmı olarak toplam 12 bit gönderilmekte ve her bitten önce de (toplam 12 defa) 0.6 ms beklenmektedir. Ayrıca ilk başta 4.8 ms start biti bulunmaktadır.

Tüm bitlerin 0 olduğu düşünülürse;

Start bit	: 4.8 ms.
Komut+Adres bitleri(12x0.6)	: 7.2 ms.
Bitler arası bekleme(12x0.6)	: 7.2 ms.

Toplam	: 19.2 ms.

Tüm bitlerin 1 olduğu düşünülürse;

Start bit	: 4.8 ms.
Komut+Adres bitleri(12x1.2)	: 14.4 ms.
Bitler arası bekleme(12x0.6)	: 7.2 ms.

Toplam	: 26.4 ms.

Ortalama olarak bir paketin gönderim süresi 22.8 milisaniyedir.

Tasarlanan iletişim protokolü yazılımsal olarak, PIC assembly komutları kullanılarak gerçekleştirilmiştir. Verici ünitesi için yazılmış olan kaynak kodu EK-A'da ve alıcı ünitesi için yazılmış olan kaynak kodu EK-B'dedir.

Tasarlanan sistemde bu şekilde bir özel iletişim protokolü kullanılarak sisteme dışarıdan müdahale etmek isteyenlere karşı bir güvenlik perdesi oluşturulmuştur. Gönderilen bilginin üçüncü kişilerce elde edilebilmesi için öncelikle IR iletim hattına girilmeli, daha sonra ise bu iletişim protokolü çözülerek sinyal bilgisi sağlıklı şekilde elde edilebilmelidir.

B. KİMLİK DOĞRULAMA / ŞİFRELEME

Kablosuz uzaktan kumanda ile kontrol edilen sistemlerde giriş güvenliğini sağlamak üzere değişik kimlik doğrulama teknikleri (sabit şifre, tek kullanımlık şifre, soru-cevap vb.) bulunmaktadır. Uzaktan kontrol sistemlerinde sabit şifre tekniği kullanıldığında, şifrenin gönderimi esnasında

yetkisiz kişilerce şifrenin ele geçirilmesi ve kopyalanarak daha sonra sisteme giriş için kullanılması (playback attack) mümkündür. RFID uygulamalarında benzer şekilde güvenlik zafiyeti olduğundan kısmen bahsedilebilir. RFID etiketlerinde bulunan bilgiler sabit tanımlayıcı bilgilerdir. Örneğin Ford firmasının geliştirdiği PATS (Passive Anti Theft Security System) sisteminde kullanıcının anahtarında sabit bir ID kodu bulunmakta ve bu kodu alıcıya göndererek sistemi aktif hale getirmektedir [21].

Güvenlik teknolojileri geliştikçe sabit şifre uygulamasının yerini tek kullanımlık şifreler almaya başlamıştır. Örneğin günümüz internet bankacılığında internet şubesine girilmek istenildiğinde kullanıcıdan tek kullanımlık şifre (OTP, one-time password) istenmektedir. Kullanıcılar banka tarafından kendilerine verilen özel şifre üretme cihazı ile ya da cep telefonuna şifre üretme yazılımını yükleyerek sisteme her girişte tek kullanımlık şifre üretebilmektedir (cep telefonunun yazılım desteği olmalıdır). Bu şekilde üretilen şifreler aynı algoritma kullanılarak banka merkezi tarafında da üretilmekte ve kullanıcının bilgisayardan girdiği şifre ile karşılaştırılmaktadır. Bir diğer yol da her girişte banka tarafından kullanıcının sistemde kayıtlı cep telefonu numarasına SMS ile şifrenin gönderilmesidir.

Araç hırsızlıklarına karşı geliştirilen tedbirlerden biri olan immobiliser sistemlerinin bir kısmında kullanıcı anahtarı araçtaki kontrol merkezine bir şifre gönderir. Bu şifre kullanıldıktan sonra silinir ve kontrol merkezi anahtara bir sonraki kullanım için yeni şifre verir. Anahtar bu şifreyi belleğinde bir sonraki kullanıma kadar saklar. Böylelikle her şifre bir kez kullanılır [4,67].

Geliştirilen asenkron (tek yönlü) veri iletişim sisteminde de yetkisiz kullanıcıların sisteme girişini engellemek amacıyla OTP şifreleme tekniği kullanılmaktadır. Bu yöntemde, yetkili kullanıcıya özel algoritma ile üretilen her bir şifrenin geçerliliği tek kullanımla sınırlıdır. Bu durumda kullanılan şifre geçerliliğini kaybederek çöpe atılmaktadır. Aynı şifrenin bir daha kullanılması söz konusu değildir. Şifreler özel bir şifreleme algoritması ile rastgele olarak üretilmektedir [41]. Temel olarak alıcı ile verici aynı şifreleme algoritmasını kullanarak şifre üretmektedirler.

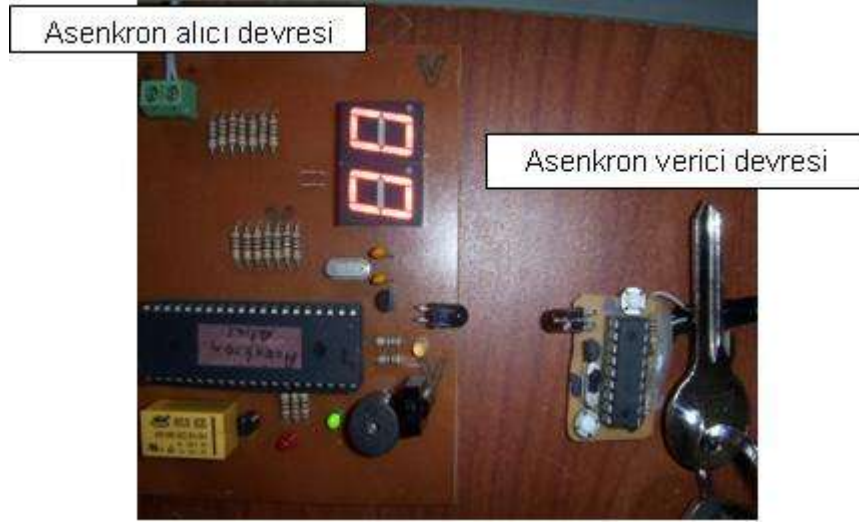
C. VERİCİ ÜNİTESİ

Bu sistemde tasarlanmış olan verici ünitesi herhangi bir ev, ofis ya da araba kapısını açmak için kullanılan bir anahtar olarak düşünülebilir. Verici üzerinde bulunan tek bir butona basılmak suretiyle her defasında değişik şifre gönderilir. Burada herhangi bir tuş takımı kullanarak şifre girilmemekte, otomatik olarak üretilen şifre tek bir tuş ile alıcıya iletilmektedir. Böylece şifrenin kopyalanması olasılığı azalmaktadır. Ayrıca yetkisiz kişilerce kopyalama işlemi gerçekleşse dahi kopyalanan şifrenin geçerliliği olmadığından (OTP sistemi) herhangi bir güvenlik açığı oluşturmamaktadır. Tam tersine ilave bir güvenlik duvarı örülmektedir.

Gönderilen şifreyi elde etmenin tek yolu iletim hattına girerek IR sinyali almak ve kullanılan IR protokolünü çözmektir. Bu girişim de herhangi bir işe yaramaz. Zira gönderim esnasında şifrenin kopyalanması başarlısa bile aynı şifreyi tekrar kullanmak mümkün değildir.

Verici sekiz bitlik üç adet kaynaktan oluşan 24-bitlik bir şifre oluşturur. Butona basıldığında bu şifreyi sekizer bitlik komutlar ve dörder bitlik adresler halinde alıcıya gönderir. Şifreyi gönderdikten sonra şifreleme algoritmasını kullanarak sekiz bitlik üç adet yeni şifre kaynağı oluşturur ve bunu EEPROM'a yazar. Böylece alıcıya gönderilmiş (yani kullanılmış) olan şifre silinir. Verici kısmında yapılan işlemlerin akış diyagramı Şekil 5.3'te görülmektedir.

Her defasında farklı olmak üzere üretilebilecek 24-bitlik şifre sayısı $2^{24} = 16.777.216$ 'dır. Sisteme yabancı / yetkisiz bir kişinin ilk denemede giriş yapabilme olasılığı (aynı IR iletişim protokolünü kullanmak koşuluyla) 5.96×10^{-8} 'dir. Kullanılan iletişim protokolünde şifre üç paket halinde gönderilmektedir. Her bir paketin gönderim süresi ortalama 22.8 ms. olduğundan 24-bitlik şifre 68.4 ms.de gönderilmektedir. Olası tüm şifreleri aralıksız olarak denemek 318.77 saat (yaklaşık 13 gün) sürmektedir. Bu süreye alıcının sırasıyla her bir şifre için tepki verme zamanı dahil değildir.

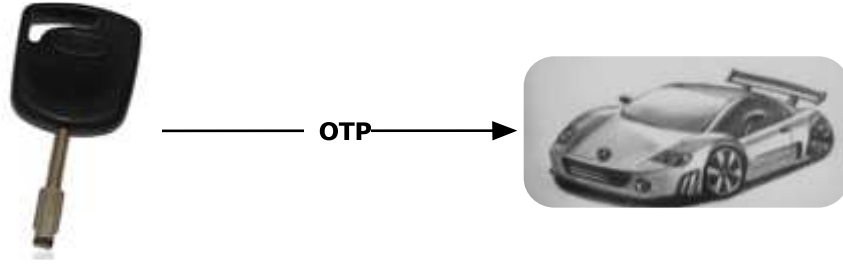


Resim 5.1: Asenkron Verici ve Alıcı Devreleri

D. ALICI ÜNİTESİ

Alıcı tarafında şifre kaynağını oluşturan aynı algoritma kullanılarak 10 adet 24 bitlik şifre oluşturulur ve EEPROM belleğe yazılır. Buradaki amaç vericinin butonuna alıcıdan uzak bir noktada iken birkaç kez basılması halinde üretilen şifreler değişeceğinden, verici ile alıcı arasındaki senkronizasyonu sağlamaktır. Yani alıcıdan uzak bir noktada (alıcı tarafından algılanamayan ya da alıcıdan farklı bir ortamda) vericinin butonuna dokuz defa basıldıktan sonra, alıcının kapsama alanında onuncu kez basıldığında vericinin ürettiği şifre alıcı tarafından kabul edilecektir. Alıcı kısmında yapılan işlemlerin akış diyagramı Şekil 5.4'te görülmektedir.

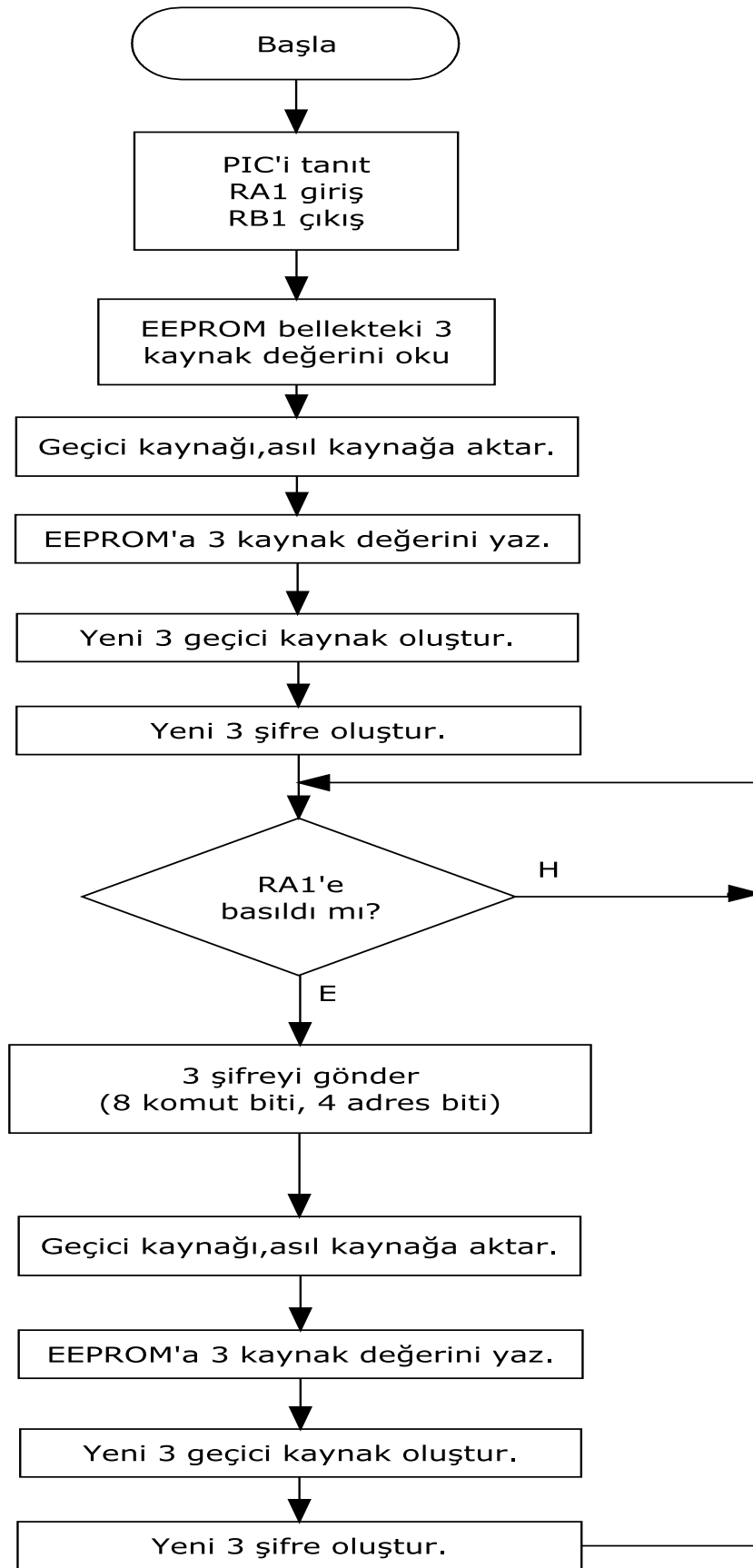
Alıcı 10 adet şifreyi ürettikten sonra vericiden sinyal gelmesini bekler. Vericiden sinyali aldığı anda bu sinyali çözerek sekizer bitlik üç adet komuttan oluşan 24-bitlik şifreyi okur. Okuduğu bu şifreyi kendi ürettiği şifreler ile sırasıyla karşılaştırmaya başlar. Eğer kendi ürettiği 10 şifreden hiçbirisi ile aynı değilse sistemin kilidini açmaz ve vericiden tekrar sinyal gönderilmesini beklemeye başlar. Eğer vericiden gelen şifre kendi ürettiği şifrelerden biri ile aynı ise sistemin kilidini açar.



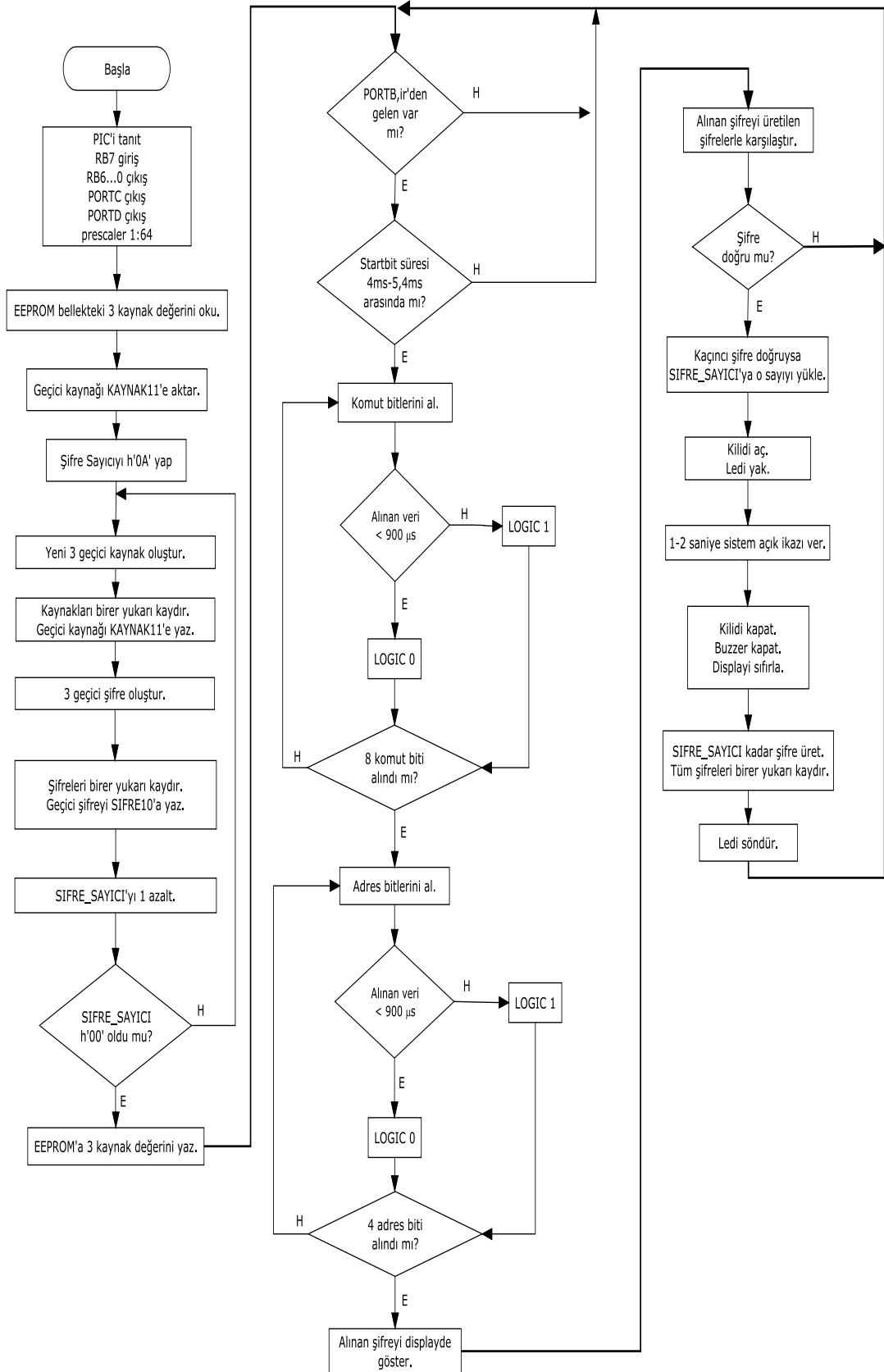
Şekil 5.2 : Alıcıya Tek Kullanımlık Şifre Gönderilmesi

10 şifre içinden kaçınıcı şifre kilidi açmak için kullanılmışsa, o şifreyle beraber kendisinden önceki diğer şifreler de silinir. Daha önceki şifrelerin silinmesinin nedeni, bu şifrelerin alıcıdan uzak bir noktada vericinin butonuna basılarak kullanılmış ve artık geçerliliğini yitirmiş olmasıdır. Butona basılarak harcanmış olan bu şifreler herhangi bir şekilde kopyalanmış olma ihtimaline karşı tekrar kullanılmaz [41].

Silinen şifre sayısı kadar yeni şifre üretilerek EEPROM'a yazılır. Bu işlem esnasında kullanılmayan şifreler bir üste kaydırılarak sıralama bozulmaz. Sıralama bozulduğu takdirde vericinin üreteceği şifreler alıcının ürettiği şifrelerden farklı olmaya başlayacaktır. Alıcı yeni şifre/şifreler üreterek üretilmiş şifre sayısını 10'a çıkardıktan sonra tekrar vericiden sinyal gelmesini beklemeye başlar.



Şekil 5.3: Asenkron Sistem Verici Akış Diyagramı



Şekil 5.4: Asenkron Sistem Alıcı Akış Diyagramı

VI. SENKRON VERİ İLETİŞİM SİSTEMİ

A. IR İLETİŞİM PROTOKOLÜ

Senkron (çift-yönlü) veri iletişim sisteminde asenkron sistemde kullanılan IR iletişim protokolü kullanılmaktadır. İstemci ünitesi için yazılmış olan kaynak kodu EK-C'de ve sunucu ünitesi için yazılmış olan kaynak kodu EK-D'dedir.

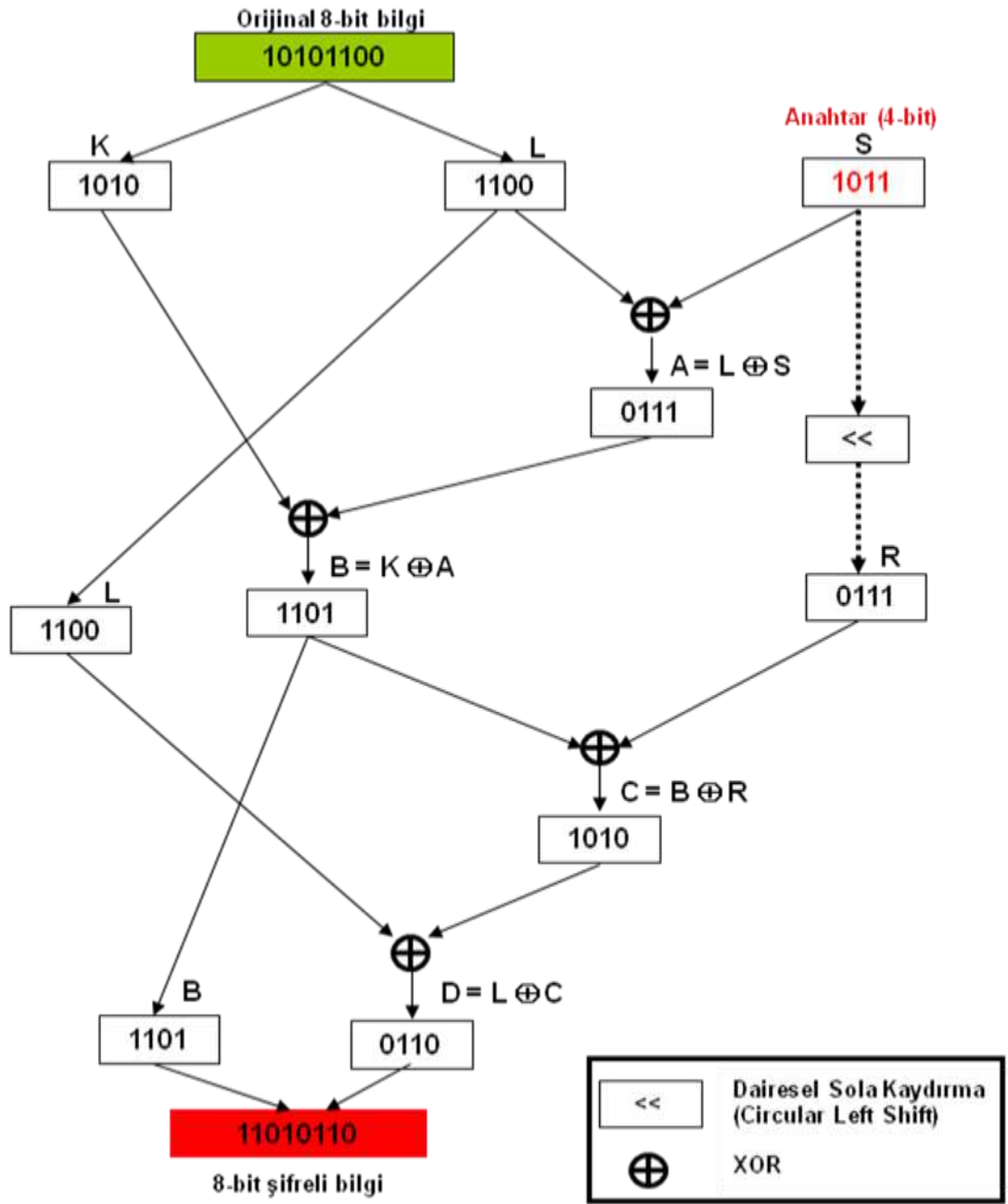
B. KİMLİK DOĞRULAMA/ŞİFRELEME

Senkron veri iletişim sisteminde istemci-sunucu mantığıyla çalışan bir yapı tasarlanmıştır. Bu sistemde birden fazla istemci tanımlanabilir ve sunucu ile her istemci arasında farklı bir şifreleme algoritması kullanılır. Burada istemci ile sunucu arasında karşılıklı veri alışverişi söz konusudur. Bu nedenle kaynak ve kullanıcı her ikisi de verici/alıcı (transceiver) modülüne sahiptir. Soru-cevap tekniği olarak adlandırılan sorgulamaya benzer bir kimlik doğrulama tekniği kullanılmıştır. Öncelikle her istemcinin özel protokolle oluşturulmuş 32-bit ID kimliği bulunmaktadır.

C. İSTEMCİ / SUNUCU ÜNİTELERİ

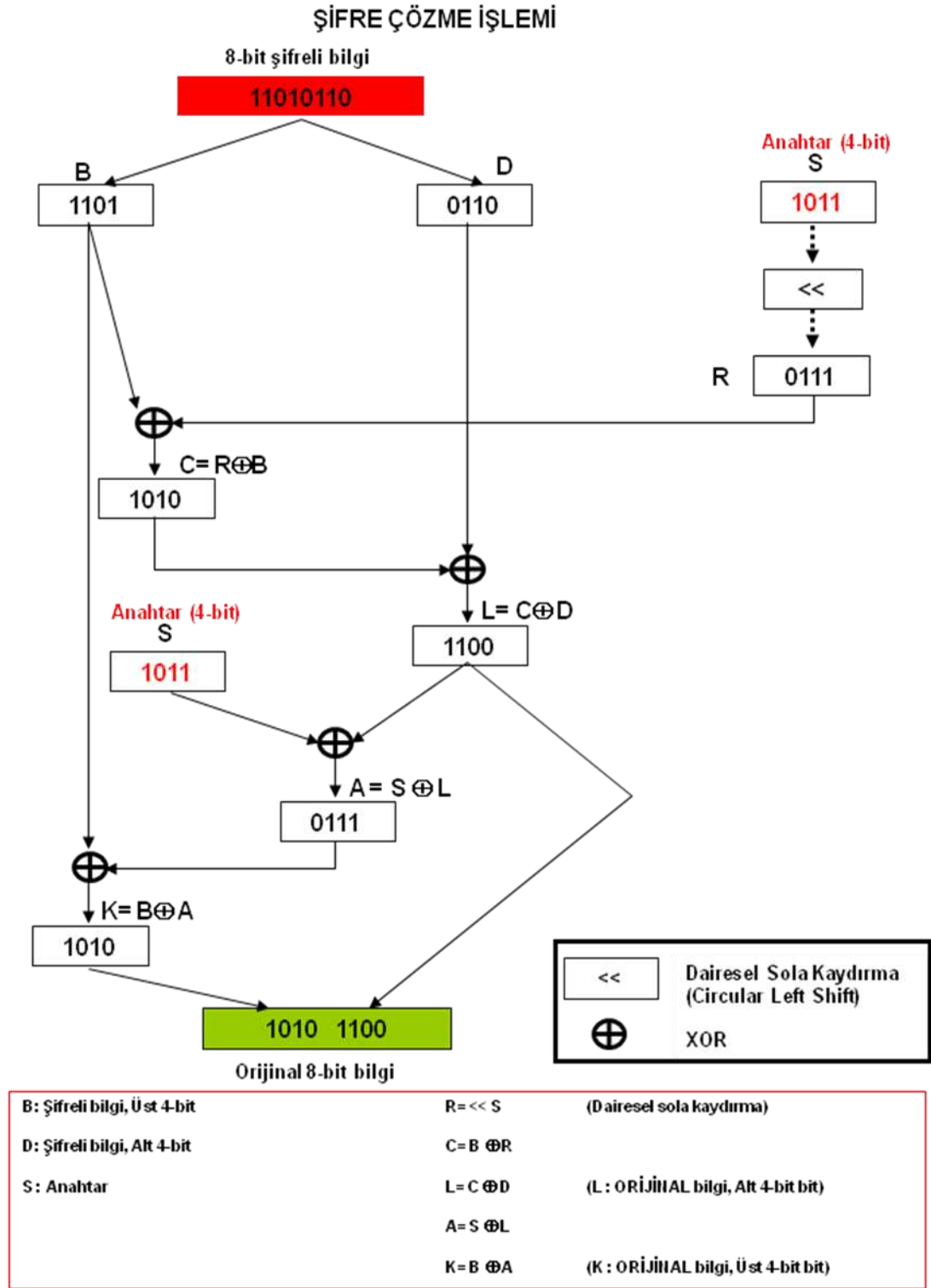
Sisteme giriş yapılmak istendiğinde (yani anahtar üzerindeki butona basıldığında) sunucuya ID kimliği gönderilir. Sunucu gönderilen ID numarasını aldığı anda rastgele olarak bir şifre üretir. Ürettiği bu şifreyi, istemcinin ID numarasına ait şifreleme algoritmasından geçirdikten sonra kriptolanmış bilgiyi istemciye gönderir. Tasarımı yapılan senkron veri iletişim sisteminde kullanılan şifreleme algoritması Şekil 6.1'de gösterilmiştir. Gönderilen bu şifre 8-bitlik 4 adet kaynaktan oluşan 32-bitlik bir şifredir. İstemci kendisine gönderilen kriptolu bilgiyi alarak çözer, bunun için kendi ID numarasına ait şifre çözme algoritmasını çalıştırır. Şifreyi çözerek bulduğu orijinal şifreyi tekrar sunucuya gönderir. Şifre çözme algoritması Şekil 6.2'de gösterilmiştir.

ŞİFRELEME İŞLEMİ



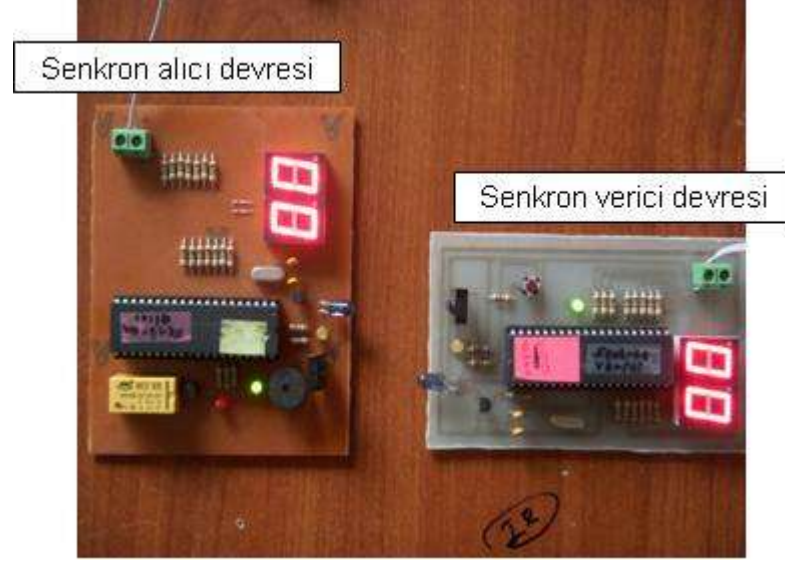
K : ORJİNAL bilgi, Üst 4-bit	R = $\ll$ S (Dairesel sola kaydırma)
L : ORJİNAL bilgi, Alt 4-bit	A = $L \oplus S$
S : Anahtar	B = $K \oplus A$ (B: Şifreli bilgi, Üst 4-bit)
	C = $B \oplus R$
	D = $L \oplus C$ (D: Şifreli bilgi, Alt 4-bit)

Şekil 6.1: Şifreleme Algoritması



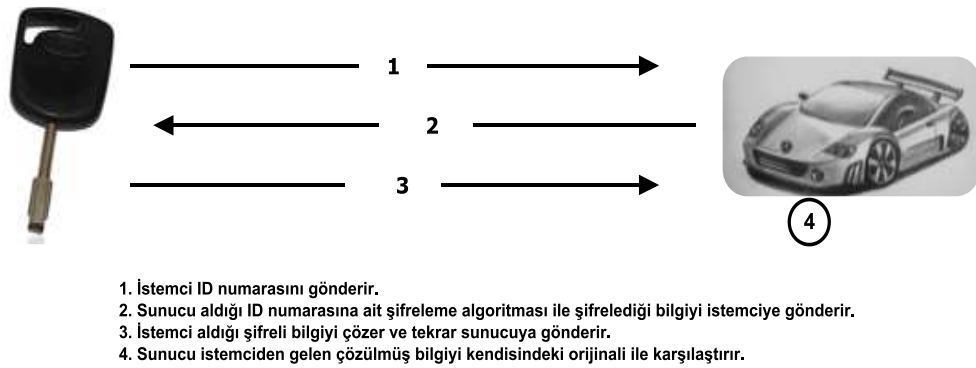
Şekil 6.2: Şifre Çözme Algoritması

İstemci kısmında yapılan işlemlerin akış diyagramı Şekil 6.4'de sunulmuştur.

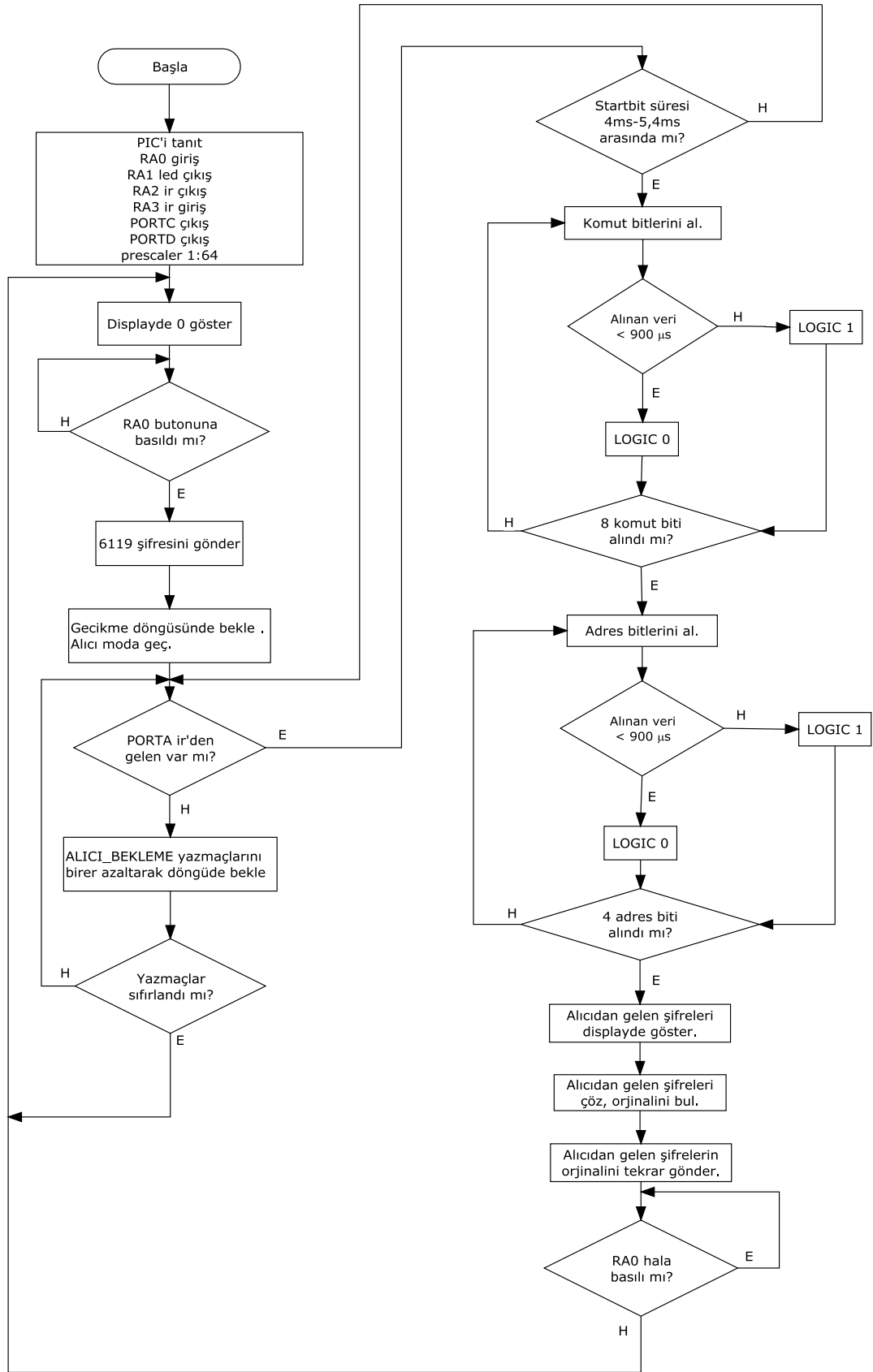


Resim 6.1: Senkron Verici ve Alıcı Devreleri

Sunucu, istemcinin gönderdiği şifreyi kendisindeki şifre ile karşılaştırır, aynı ise sistemi açar. Aynı değilse sisteme girişe izin vermez, tekrar herhangi bir istemciden ID numarasının gelmesini beklemeye başlar. Şekil 6.5'de sunucu kısmında yapılan işlemlerin akış diyagramı sunulmuştur.



Şekil 6.3: Senkron Veri İletişim Sistemi



Şekil 6.4: Senkron Sistem İstemci Akış Şeması

D. SENKRON VE ASENKRON VERİ İLETİŞİM SİSTEMLERİ ARASINDAKİ FARKLAR

Asenkron veri iletişim sisteminde güvenlik tek kullanımlık şifre tekniği ile sağlanmıştır. Kullanıcıdan kaynaklanabilecek hatalara karşı da tedbir amaçlı olarak 10 adet şifrenin kontrol merkezi tarafından üretilerek saklanması tasarlanmıştır. Kullanıcının uzaktan kontrol mekanizmasını alıcıdan bağımsız olarak 10 defadan fazla kullanması durumunda sistemin sıfırlanmasına gerek vardır.

Senkron sistemde asenkronda olduğu gibi 10 adet şifreyi üretip EEPROM'da saklamaya gerek yoktur. Çünkü istemcide herhangi bir şifre üretme söz konusu değildir. Şifreler tamamen sunucu tarafında üretilmekte, istemci sadece sunucunun kriptoladığı şifreyi çözerek orijinalini bulmaktadır. Sunucunun ürettiği şifreler rastgele olup, her defasında farklı bir şifre üretmektedir. Sunucunun şifre üretmeye başlaması için istemciden ID numarasının gelmesi şarttır. Bu şekilde istemci ile sunucu arasındaki senkronizasyon sağlanmaktadır.

VII. SONUÇ

Günümüzde bir çok sistemde ihtiyaç duyulan güvenlik uygulamaları için, verici ve alıcı modülleri arasında güvenli iletişim kurulmasını sağlayan, IR (kızıl ötesi) haberleşme tabanlı senkron ve asenkron olmak üzere iki farklı tasarım önerilmiş ve gerçekleştirilmiştir. İlk tasarımda asenkron iletişim sistemi kullanılmış olup, kullanıcı kimliğine göre özel OTP (one-time password) şifre üretim algoritmaları kullanılarak IR veri iletişimine uyarlanmıştır. Önerilen ikinci tasarımda hem kaynak hem de kullanıcının verici/alıcı (transceiver) modülüne sahip olduğu senkron iletişim sistemi kullanılmıştır. Her kullanıcı için sırasıyla 32-bit ID numarası kontrolü ve ikinci aşama olarak sistemde kayıtlı/yetkili ise rastgele bir soru yöneltilerek cevabı beklenmektedir. Sunucu kendi cevabı ile istemci cevabını karşılaştırır. Soru-cevap sayıları istenildiği kadar artırılabilir. Yetkisiz kişiler tarafından IR kesme/kopyalama yapılsa dahi önerilen her iki sistem tarafından kopyalanan verinin hiçbir önemi bulunmamaktadır.

Önerilen sistemleri mevcut sistemlerden ayıran en belirgin farklar; asenkron tasarım uygulamasında her defasında farklı kullan-at şifresinin üretilmesi iken senkron sistemde sunucu-istemci arasındaki karşılıklı sorgulamalar ile çift-yönlü iletişim/sorgulamanın tesis edilmiş olmasıdır. Önerilen her iki sistem için gerekli ilave güvenlik duvarları oluşturulmuştur. IR tabanlı iletişim için standart dışı özel bir protokol üretilerek ilave bir güvenlik duvarı daha oluşturulmuştur.

Oluşturulmuş olan güvenlik duvarlarının sistemin çalışması esnasında herhangi bir zaman kaybı ya da gecikmeye yol açmadığı görülmüştür. Senkron sistemde 32-bit ID ve daha sonrasında karşılıklı 32-bit soru-cevap gönderimi söz konusudur. 32-bitlik bir bilgi IR iletişim protokolü gereği 4 paket halinde iletilmektedir. İletilen bilginin maksimum gönderim süresi (tüm bitler 1 ise) 26.4 milisaniyedir. Bu durumda ID bilgisi, soru ve cevap olarak toplam 96-bitlik bilginin 12 paket halinde karşılıklı alınıp verilmesi 316.8 ms. sürmektedir. Asenkron sistemde ise sadece 24-bitlik tek kullanımlık şifre gönderildiği için bu süre 79.2 ms. olmaktadır. Alıcı ve verici

ünitelerinde komut işletim süreleri de dahil olmak üzere sistemin çalışması 500 milisaniyenin altında gerçekleşmektedir. Bu süre kullanıcı açısından herhangi bir gecikmeye yol açmadığı gibi sisteme dışarıdan müdahale etmek isteyenler için de oldukça kısa bir süredir.

Önerilen her iki yaklaşım (senkron & asenkron), yazılım ve donanımı ile birlikte prototip olarak üretilmiştir. Sistemler PIC16F877A ve PIC16F628A mikrodenetleyicileri kullanılarak tasarlanmıştır. Maliyet ve boyut olarak efektif hale getirilmiştir.

Senkron veri iletişim sistemi bir ya da birden fazla kullanıcısı olan güvenli giriş sistemlerinde kullanılabilir. Her kullanıcının farklı bir ID numarası olduğundan sisteme dışarıdan müdahale etmek isteyen bir kişinin öncelikle sistemde tanımlı geçerli bir ID numarasını ve bu ID numarasına ait şifreleme algoritmasını ele geçirmiş olması gerekmektedir. Ayrıca kullanıcılardan herhangi birisinin anahtarını kaybetmesi durumunda, kaybolan anahtarın yetkisi pasif duruma getirilebilir. Bu esnada diğer kullanıcılar sistemi sorunsuz olarak kullanmaya devam edebilir. Bu sistemde güvenlik açısından hangi kullanıcının ne zaman giriş yaptığı kayıt altına alınabileceği gibi, farklı kullanıcılara farklı yetkilendirmeler yapabilmek de mümkündür. Örneğin; kullanıcının sistemi açabilmesi için gün ve saat kısıtlaması yapılabilir, ya da birden fazla ofis odasının olduğu bir ortamda kullanıcı sadece yetki verilen odaların kapısını açabilir.

Tasarlanan sistemler günlük hayatta güvenlik gereksinimi olan ev, ofis-büro gibi birimlere güvenli/kayıtlı giriş amacıyla, otomobil immobilisier uygulamaları, PC ve diğer elektronik donanımlara yetkilendirilmemiş kişilerin erişiminin engellenmesi amacıyla kullanılabilir.

KAYNAKÇA

1. G.Jayendra,S.Kumarawadu,L.Meegahapola, "RFID-Based Anti-theft Auto Security System with an Immobilizer", Industrial and Information Systems, ICIIS 2007. pp.441-446, August 2007.
2. S.M.Mahmud, S.Shanker, "In-Vehicle Secure Wireless Personal Area Network (SWPAN)", IEEE Transactions on Vehicular Technology , vol.55, no.3, pp.1051-1061, May 2006.
3. F.Zhang, D.Huang, Z.Dong, Y.Huang , "Design and Implementation of Automatic Clearance Control System Based on RFID" , Proc. of the 7.World Congress on Intelligent Control and Automation, pp.6621-6626, June 2008.
4. B.Davis, R.DeLong, "Combined Remote Key Control and Immobilization System for Vehicle Security", IEEE Power Electronics in Transportation, pp.125-132, October 1996.
5. B.C.M.Fung, K.Al-Hussaeni, M.Cao, "Preserving RFID Data Privacy", IEEE Int.Conf. on RFID, pp.200-207, April 2009.
6. L.Wuming, H.Pingyang, Z.Ruilin, "Study on Design and Application of Wireless Sensor Network Based on Communication of RFID System", WiCom '09. 5th International Conference , pp. 1-6, September 2009.
7. M.Vogt,A.Poschmann,C.Paar, "Cryptography is Feasible on 4-bit Microcontrollers – A Proof of Concept", IEEE International Conference of RFID, pp.241-248, April 2009.
8. H.J.Chae,D.J.Yeager,J.R.Smith,K.Fu, "Maximalist Cryptography and Computation on the WISP UHF RFID Tag", Proc. of the Conference on RFID Security, July 2007.

9. T.Staake, F.Thiesse, E.Fleisch, "Extending the EPC Network-The Potential of RFID in Anti-Counterfeiting", Proceedings of the ACM Symposium on Applied Computing, pp.1607–1612, March 2005.
10. P.Tuylsand,L.Batina,"RFID-Tags for Anti-Counterfeiting," Topics in Cryptology-CT-RSA, vol.3860, pp.115–131, 2006.
11. A.Juels, "Rfid Security and Privacy: A Research Survey", IEEE Journal on Selected Areas in Communications, vol.24, no.2, pp.381-394, February 2006.
12. M.Lehtonen, T.Staake, F.Michahelles, E.Fleisch, "From Identification to Authentication - a Review of RFID Product Authentication Techniques" Printed Handout of Workshop on RFID Security–RFID Sec06, 2006.
13. P.Rotter, "A Framework for Assessing RFID System Security and Privacy Risks", IEEE Pervasive Computing, vol. 7, no. 2, pp. 70-77, April-June 2008.
14. G.Dargan,B.Johnson,M.Panchalingam,C.Stratis, "The Use of Radio Frequency Identification as a Replacement for Traditional Barcoding." 45-877. Final Project Strategic Uses of Information Technology. Carnegie Mellon University, 2004.
15. M.Lampe,M.Strassner, "The Potential of RFID for Moveable Asset Management", Workshop on Ubiquitous Commerce at Ubicomp 2003.
16. J.Collins,. "Can RFID Save the Cattle Industry?" RFID Journal, Vertical Focus, December 23,2003.
17. C.M. Roberts, "Radio Frequency Identification (RFID)", Computers & Security, Volume 25, Issue 1, Pages 18-26, February 2006.

18. D.Avivi, "Automatic Vehicle Identification - AVI - Electronic License Plates: The Public Safety Perspective", Proc. 25th Annual IEEE International Carnahan Conference on Security Technology, pp.96-99, October 1991.
19. H.S.Park, S.C.Yang, D.H.Oh, J.D.Kim, "Design and Implementation of WLAN-based Automatic Vehicle Identification", International Conference on Computational Science and Engineering, pp.310-317, August 2009.
20. X.Fan,Y.Zhang, "A Design of Bi-verification Vehicle Access Intelligent Control System Based on RFID", The Ninth International Conference on Electronic Measurement & Instruments, ICEMI'2009, pp.1-569 – 1-573, August 2009.
21. K.S.Khangura, N.V.Middleton, M.M.Ollivier, "Vehicle Anti-Theft System Uses RFID", IEE Colloquium on Vehicle Security Systems, pp. 4/1-4/7, October 1993.
22. M.Hirano, M.Takeuchi, T.A.Tomoda, K.I.Nakano, "Keyless Entry System With Radio Card Transponder", IEEE Transactions on Industrial Electronics, vol.35, no.2, pp.208-216, May 1988.
23. R.G.Gallager, Information Theory and Reliable Communication, J.Wiley&Sons Inc. , 1968.
24. S.Ertürk, Sayısal Haberleşme, Birsen Yayınevi, 2005.
25. J.L.LoCicero, B.P.Patel, Line Coding – Mobile Communications Handbook, Boca Raton: CRC Press LLC, 1999.
26. D.A.Ramirez, M.R.Ayala, E.A.Gonzalez, J.A.Mendez, "Educational Prototype for Line Coding", Proceedings of the 6th WSEAS International Conference on Engineering Education, pp.232-235, 2009.

27. T. Hämäläinen, M.Kivikoski, "Secure Infrared Control System for Automotive Applications", Proceedings of the 1996 IEEE IECON 22nd International Conference, Vol.2, pp.852-857, August 1996.
28. C.E.Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal, vol.28-4, pp. 656-715, 1949.
29. K.M.Shaheen, "Code Book Cipher System", Proc. IEEE International Carnahan Conference on Security Technology, pp.66-71, 1994.
30. J.H.Beker,F.Piper, Cipher Systems: The protection of Communication, Northwood Publications, 1982.
31. National Bureau of Standards, "Data Encryption Standard (DES)", Federal Information Processing Standards (FIPS), Pub.No.46, 1977.
32. B.Sklar, Digital Communication: Fundamental and Applications, Prentice Hall, 1988.
33. J.Daemen,V.Rijmen, "Rijndael, The Advanced Encryption Standard", Dr.Dobb's Journal, Vol.26, No.3, pp.137-139, 2001.
34. National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)", Federal Information Processing Standards (FIPS), Pub.No.197, 2001.
35. R.Merkle, M.Hellman, "Hiding Information and Signatures in Trapdoor Knapsacks," IEEE Trans. Inform. Theory, vol. IT-24, no.5, pp.525-530, 1978.
36. A.Shamir, "A Polynomial-Time Algorithm for Breaking the Basic Merkle -Hellman Cryptosystem", IEEE Transactions on Information Theory, Vol.30, No.5, pp.699 – 704, September 1984.

37. W.Diffie,M.Hellman, "New Directions in Cryptography." IEEE Trans. Inform. Theory, vol. IT-22, pp. 472-492, 1976.
38. R.Rivest, A.Shamir, L.Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120-126, 1978.
39. T.Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms " IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp.469-472, July 1985.
40. N.Koblitz, "Elliptic Curve Cryptosystems", American Mathematical Society Mathematics of Computation, Vol.48, No.177, pp.203-209, January 1987.
41. F.Akar, M.Tekeli, "IR Tabanlı Senkron ve Asenkron Güvenlik Sistemi Tasarımı", 6th International Advanced Technologies Symposium (IATS'11), pp.257-263, May 2011.
42. D.M.Pozar, Microwave Engineering, 3rd Ed., John Wiley & Sons,2004
43. E.S.Barr, "Historical Survey of the Early Development of the Infrared Spectral Region", American Journal of Physics., vol. 28, No.1, pp.42-54, January 1960.
44. W.N.Arnuist, "Survey of Early Infrared Developments", Proc.Inst.of Radio Engrs., vol. 47, No.9, pp.1420-1430, September 1959.
45. R. Hudson,Jr., Infrared System Engineering, Wiley & Sons Inc.,1969.
46. J.B. Carruthers, "Wireless Infrared Communications", Wiley Encyclopedia of Telecommunications, 2002.

47. M.K.Krolak,M.E.Novak, “An Introduction to Infrared Technology : Applications in the Home, Classroom, Workplace, and Beyond ...”, 1995.
48. S.Williams, “IrDA : Past,Present and Future”, IEEE Pers.Comm., vol. 7, no.1, pp. 11-19, February 2000.
49. V.Vitsas, P.Parker, A.C.Boucouvalas, “IrDA Infrared Wireless Communications: Protocol Throughput Optimization”, IEEE Wireless Communications, pp. 22-29, April 2003.
50. P.Barker, A.C.Boucouvalas, “Performance Modeling of the IrDA Protocol for Infrared Wireless Communications”, IEEE Commun.Mag., vol. 36, no.12, pp.113-117, December 1998.
51. T.Özuğur, J.A.Copeland, “Next-Generation Indoor Infrared LANs: Issues and Approaches”, IEEE Pers.Comm., pp.6-19, December 1999.
52. A.C.Boucouvalas, P.Huang , “Modelling and Optimising TinyTP over IrDA Stacks”, EURASIP Journal on Applied Signal Processing, vol.2005, No.1, pp.45–56, March 2005.
53. F.Akar, M.Yağımlı, PIC16F877A Proje Tasarımı, Beta Basım A.Ş. 2007.
54. F.Akar, M.Yağımlı, PIC Mikrodenetleyiciler 16F84A & 16F628A, Beta Basım A.Ş. 2006.
55. J.Sanchez, M.P.Canton, Microcontroller Programming-The Microchip PIC, CRC Press, 2007.
56. PIC16F84A Data Sheet (DS35007B), Microchip Technology Inc., 2001.

57. PIC16F627A/628A/648A Data Sheet (DS40044A), Microchip Technology Inc., 2002.
58. PICmicro Mid-Range MCU Family Reference Manual (DS33023A), Microchip Technology Inc., 1997.
59. PIC16F87XA Data Sheet (DS39582B), Microchip Technology Inc., 2003.
60. Data Sheet for HCS412 Keeloq Code Hopping Encoder and Transponder (DS41099C), Microchip Technology Inc. 2002.
61. A.I.Alrabady, S.M.Mahmud, "Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs",IEEE Trans. On Vehicular Tech., Vol. 54, No.1, pp.41-50, January 2005.
62. A.I.Alrabady, S.M.Mahmud, "Some attacks against vehicles' passive entry security systems and their solutions",IEEE Trans. On Vehicular Tech., Vol. 52, No.2, pp.431-439, March 2003.
63. J.Al-Jaroodi,J.Aziz,N.Mohamed, "Middleware for RFID Systems An Overview", 33rd Annual IEEE International Computer Software and Applications Conference, Vol 2, pp.154-159, July 2009.
64. J.Landt, "Shrouds of Time: The history of RFID ". AIM, Inc. 2001.
65. J.M.Kahn, J.R.Barry, "Wireless Infrared Communications",Proc. Of IEEE, Vol. 85, No. 2, pp.265-298, February 1997.
66. D.R.Pauluzzi, P.McConnell, R.L.Poulin, "Free-space, Undirected Infrared Voice and Data Communications with a Comparison to RF Systems", IEEE International Conference on Selected Topics in Wireless Communications, Conference Proceedings, pp.279-285, June 1992.

67. J.H.Whu, C.C.Kung, J.H.Rao, P.C.Wang, C.L.Lin, T.W.Hou, "Design of an In-Vehicle Anti-Theft Component", 8.International Conference on Intelligent Systems Design and Applications, 2008, Vol.1, pp.566-569.

EKLER

EK-A : ASENKRON VERİCİ PROGRAM KODLARI

EK-B : ASENKRON ALICI PROGRAM KODLARI

EK-C : SENKRON İSTEMCİ PROGRAM KODLARI

EK-D : SENKRON SUNUCU PROGRAM KODLARI

EK-A: ASENKRON VERİCİ PROGRAM KODLARI

```

;***** ASENKRON VERİCİ *****

LIST    p=16F628
include "P16F628.inc"

__CONFIG __CP_OFF & __WDT_OFF & __PWRTE_ON
& __XT_OSC & __MCLRE_ON & __BODEN_OFF &
__LVP_OFF & __DATA_CP_OFF

count1      EQU 0x20
counta      EQU 0x21
countb      EQU 0x22
count       EQU 0x23
Delay_Count EQU 0x24
Bit_Cntr    EQU 0x25
Data_Byte   EQU 0x26
Dev_Byte    EQU 0x27
Rcv_Byte    EQU 0x28
Pulse       EQU 0x29
Data_Bytel  EQU 0x2A
Dev_Bytel   EQU 0x2B
GECICI_KAYNAK_1 EQU 0x2C
GECICI_KAYNAK_2 EQU 0x2D
GECICI_KAYNAK_3 EQU 0x2E
GECICI_SIFRE_1 EQU 0x2F
GECICI_SIFRE_2 EQU 0x30
GECICI_SIFRE_3 EQU 0x31
GECICI_KAYNAK_A EQU 0x32
GECICI_KAYNAK_B EQU 0x33
GECICI_KAYNAK_C EQU 0x34
GECICI_KAYNAK_D EQU 0x35
GECICI_KAYNAK_K EQU 0x36
GECICI_KAYNAK_L EQU 0x37
DEGISTIRICI EQU 0x38
DEGISTIRICI1 EQU 0x39
DEGISTIRICI2 EQU 0x3A
ANAHTAR     EQU 0x3B
ANAHTAR1    EQU 0x3C
ircounter   EQU 0x3D
KAYNAK_1    EQU 0x3E
KAYNAK_2    EQU 0x3F
KAYNAK_3    EQU 0x40
W_TEMP      EQU 0x41
STATUS_TEMP EQU 0x42
PCLATH_TEMP EQU 0x43
HEX_ORTA    EQU 0x44
HEX_YUKSEK  EQU 0x45
HEX_DUSUK   EQU 0x46
BUTON_KONTROL_REG EQU 0x47

IR_PORT Equ PORTB
IR_TRIS Equ TRISB
IR_Out Equ 0x01

org 0x0000
GOTO Start

org 0x004
GOTO KESME_ALTPROG

KESME_ALTPROG
    MOVWF W_TEMP
    MOVF STATUS,W
    MOVWF STATUS_TEMP
    MOVF PCLATH,W
    MOVWF PCLATH_TEMP
    CLRF PCLATH

TSTF HEX_ORTA
SKPNZ
DECF HEX_YUKSEK,F
DECFSZ HEX_ORTA,F

GOTO CIK

TSTF HEX_YUKSEK
SKPZ
GOTO CIK
MOVLW h'07'
MOVWF HEX_YUKSEK
MOVLW h'A1'
MOVWF HEX_ORTA

MOVLW h'20'
ADDWF HEX_DUSUK,F
SKPNC
INCF HEX_ORTA,F

BTFSS INTCON,T0IF
GOTO CIK

INCF BUTON_KONTROL_REG

CIK
BCF INTCON,T0IF
MOVF PCLATH_TEMP,W
MOVWF PCLATH
MOVF STATUS_TEMP,W
MOVWF STATUS
SWAPF W_TEMP,F
SWAPF W_TEMP,W
RETFIE

Start
MOVLW 0x07
MOVWF CMCON

CLRF IR_PORT
BSF STATUS,RP0
MOVLW b'11111101'
MOVWF IR_TRIS
MOVLW 0xff
MOVWF PORTA

MOVLW b'10000000'
MOVWF OPTION_REG

BCF STATUS,RP0
BANKSEL PIE1
BSF PIE1,EEIE
BANKSEL PORTA

CLRF GECICI_KAYNAK_1
CLRF GECICI_KAYNAK_2
CLRF GECICI_KAYNAK_3
CLRF GECICI_KAYNAK_A
CLRF GECICI_KAYNAK_B
CLRF GECICI_KAYNAK_C
CLRF GECICI_KAYNAK_D
CLRF GECICI_KAYNAK_K
CLRF GECICI_KAYNAK_L
CLRF GECICI_SIFRE_1
CLRF GECICI_SIFRE_2
CLRF GECICI_SIFRE_3
CLRF DEGISTIRICI

```

EK-A'NIN DEVAMI

CLRF	DEGISTIRICI1	CALL	YENI_SIFRE
CLRF	DEGISTIRICI2		
CLRF	ANAHTAR	loop	
CLRF	ANAHTAR1	BTFSC	PORTA,1
CLRF	ircounter	GOTO	Read_Sw
CLRF	BUTON_KONTROL_REG	GOTO	loop
MOVLW	b'10100000'		
MOVWF	INTCON	SIFRE_SIFIRLAYICI	
MOVLW	h'07'	MOVLW	h'04'
MOVWF	HEX_YUKSEK	MOVWF	Dev_Bytel
MOVLW	h'A1'+1	MOVLW	h'06'
MOVWF	HEX_ORTA	MOVWF	Data_Bytel
MOVLW	h'20'		
MOVWF	HEX_DUSUK	CALL	Switch
BASLA		CALL	Switch
CALL	SIFRE_OKU	CALL	Switch
CALL	YENI_SIFRE	CALL	Switch
Read_Sw		CALL	Switch
BTFSC	PORTA,1	CALL	Switch
GOTO	Read_Sw	CALL	Switch
CLRF	BUTON_KONTROL_REG	CALL	Switch
CLRF	TMR0	CALL	Switch
BUTON_KONTROL		CALL	Switch
BCF	STATUS,C	MOVLW	h'05'
MOVLW	d'252'	MOVWF	Dev_Bytel
ADDWF	BUTON_KONTROL_REG,W	MOVLW	h'01'
BTFSC	STATUS,C	MOVWF	Data_Bytel
GOTO	SIFRE_SIFIRLAYICI	CALL	Switch
		CALL	Switch
BTFSS	PORTA,1	CALL	Switch
GOTO	BUTON_KONTROL	CALL	Switch
		CALL	Switch
MOVLW	h'01'	CALL	Switch
MOVWF	Dev_Bytel	CALL	Switch
MOVF	GECICI_SIFRE_1,W	CALL	Switch
MOVWF	Data_Bytel	CALL	Switch
		CALL	Switch
CALL	Switch	CALL	Switch
CALL	Switch	CALL	Switch
CALL	Switch	CALL	Switch
CALL	Switch	CALL	Switch
CALL	Switch	CALL	Switch
CALL	Switch	CALL	Switch
CALL	Switch	CALL	Switch
CALL	Switch	CALL	Switch
MOVLW	h'02'	CALL	Switch
MOVWF	Dev_Bytel	MOVLW	h'07'
MOVF	GECICI_SIFRE_2,W	MOVWF	Dev_Bytel
MOVWF	Data_Bytel	MOVLW	h'09'
		MOVWF	Data_Bytel
CALL	Switch	CALL	Switch
CALL	Switch	CALL	Switch
CALL	Switch	CALL	Switch
CALL	Switch	CALL	Switch
CALL	Switch	CALL	Switch
CALL	Switch	CALL	Switch
CALL	Switch	CALL	Switch
CALL	Switch	CALL	Switch
MOVLW	h'03'	CALL	SIFRE_SIFIRLA
MOVWF	Dev_Bytel	CLRF	GECICI_KAYNAK_1
MOVF	GECICI_SIFRE_3,W	CLRF	GECICI_KAYNAK_2
MOVWF	Data_Bytel	CLRF	GECICI_KAYNAK_3
CALL	Switch	CLRF	GECICI_KAYNAK_A
CALL	Switch	CLRF	GECICI_KAYNAK_B
CALL	Switch	CLRF	GECICI_KAYNAK_C
CALL	Switch	CLRF	GECICI_KAYNAK_D
CALL	Switch	CLRF	GECICI_KAYNAK_K
CALL	Switch	CLRF	GECICI_KAYNAK_L
CALL	Switch	CLRF	GECICI_SIFRE_1

EK-A'NIN DEVAMI

```

        CLRF      GECICI_SIFRE_2
        CLRF      GECICI_SIFRE_3
        CLRF      DEGISTIRICI
        CLRF      DEGISTIRICI1
        CLRF      DEGISTIRICI2
        CLRF      ANAHTAR
        CLRF      ANAHTAR1
        CLRF      ircounter
        CLRF      BUTON_KONTROL_REG
        CALL      YENI_SIFRE

        GOTO      Read_Sw


Switch
        MOVF      Dev_Bytel,w
        MOVWF     Dev_Byte
        MOVF      Data_Bytel,w
        MOVWF     Data_Byte

        CALL      Xmit_RS232
        CALL      Delay20
        RETLW     0x00


TX_Start
        MOVLW     d'184'
        CALL      IR_pulse
        MOVLW     d'23'
        CALL      NO_pulse
        RETLW     0x00


TX_One
        MOVLW     d'46'
        CALL      IR_pulse
        MOVLW     d'23'
        CALL      NO_pulse
        RETLW     0x00


TX_Zero
        MOVLW     d'23'
        CALL      IR_pulse
        MOVLW     d'23'
        CALL      NO_pulse
        RETLW     0x00


IR_pulse
        MOVWF     count


irloop
        BSF       IR_PORT,IR_Out
        NOP       ;
        NOP       ;
        NOP       ;
        NOP       ;
        NOP       ;
        NOP       ;
        NOP       ;
        BCF       IR_PORT,IR_Out
        NOP       ;
        NOP       ;
        NOP       ;
        NOP       ;
        NOP       ;
        NOP       ;
        NOP       ;
        NOP       ;
        NOP       ;
        NOP       ;
        NOP       ;
        NOP       ;
        DECFSZ    count,F
        GOTO      irloop
        RETLW     0

```

```

NO_pulse
MOVWF    count

irloop2
BCF      IR_PORT,IR_Out
NOP      ;
NOP      ;
NOP      ;
NOP      ;
NOP      ;
NOP      ;
NOP      ;
NOP      ;
NOP      ;
NOP      ;
BCF      IR_PORT,IR_Out
NOP      ;
NOP      ;
NOP      ;
NOP      ;
NOP      ;
NOP      ;
NOP      ;
NOP      ;
NOP      ;
NOP      ;
DECFSZ   count,F
GOTO     irloop2
RETLW    0

Xmit_RS232
MOVWF    Data_Byte
MOVLW    0x08
MOVWF    Bit_Cntr
CALL     TX_Start

Ser_Loop
RRF      Data_Byte,f
BTFSK    STATUS,C
CALL     TX_One
BTFSK    STATUS,C
CALL     TX_Zero
DECFSZ   Bit_Cntr,f
GOTO     Ser_Loop

MOVLW    0x04
MOVWF    Bit_Cntr

Ser_Loop2
RRF      Dev_Byte,f
BTFSK    STATUS,C
CALL     TX_One
BTFSK    STATUS,C
CALL     TX_Zero
DECFSZ   Bit_Cntr,f
GOTO     Ser_Loop2
RETLW    0x00

YENI_SIFRE
MOVF     GECICI_KAYNAK_1,W
MOVWF    KAYNAK_1
MOVF     GECICI_KAYNAK_2,W
MOVWF    KAYNAK_2
MOVF     GECICI_KAYNAK_3,W
MOVWF    KAYNAK_3

CALL     SIFRE_YAZ

BCF      STATUS,C
INCF     GECICI_KAYNAK_1,F
BCF      STATUS,Z
MOVF     DEGISTIRICI,W
BTFSK    STATUS,Z
GOTO     DIGER

```

EK-A'NIN DEVAMI

```

RRF      GECICI_KAYNAK_1,F
RRF      GECICI_KAYNAK_1,F
INCF     GECICI_KAYNAK_1,F
MOVLW    h'04'
MOVWF    DEGISTIRICI
GOTO     DEVAM

DIGER
RLF      GECICI_KAYNAK_1,F
DECF     DEGISTIRICI,F

DEVAM
DECF     GECICI_KAYNAK_2,F
BCF      STATUS,Z
MOVF     DEGISTIRICI1,W
BTFS     STATUS,Z
GOTO     Diger1
RLF      GECICI_KAYNAK_2,F
INCF     GECICI_KAYNAK_2,F
MOVLW    h'03'
MOVWF    DEGISTIRICI1
GOTO     DEVAM1

DIGER1
RRF      GECICI_KAYNAK_2,F
RRF      GECICI_KAYNAK_2,F
DECF     DEGISTIRICI1,F

DEVAM1
INCF     GECICI_KAYNAK_3,F
INCF     GECICI_KAYNAK_3,F
BCF      STATUS,Z
MOVF     DEGISTIRICI2,W
BTFS     STATUS,Z
GOTO     Diger2
RRF      GECICI_KAYNAK_3,F
DECF     GECICI_KAYNAK_3,F
MOVLW    h'03'
MOVWF    DEGISTIRICI2
GOTO     DEVAM2

DIGER2
DECF     GECICI_KAYNAK_3,F
RLF      GECICI_KAYNAK_3,F
DECF     DEGISTIRICI2

DEVAM2
BCF      STATUS,C
MOVLW    h'05'

MOVWF    ANAHTAR
MOVLW    h'F0'
ANDWF    GECICI_KAYNAK_3,W
MOVWF    GECICI_KAYNAK_K

MOVLW    h'04'
MOVWF    ircounter

kaydir1
BCF      STATUS,C
RRF      GECICI_KAYNAK_K,1
DECFSZ   ircounter,1
GOTO     kaydir1

BCF      STATUS,C
MOVLW    h'0F'
ANDWF    GECICI_KAYNAK_3,W
MOVWF    GECICI_KAYNAK_L

MOVF     ANAHTAR,W
XORWF    GECICI_KAYNAK_L,W
MOVWF    GECICI_KAYNAK_A
XORWF    GECICI_KAYNAK_K,W
MOVWF    GECICI_KAYNAK_B

RLF      ANAHTAR,W
XORWF    GECICI_KAYNAK_B,W
MOVWF    GECICI_KAYNAK_C
XORWF    GECICI_KAYNAK_L,W
MOVWF    GECICI_KAYNAK_D

MOVLW    h'04'
MOVWF    ircounter

kaydir2
BCF      STATUS,C
RLF      GECICI_KAYNAK_B,1
DECFSZ   ircounter,1
GOTO     kaydir2

BCF      STATUS,C
MOVF     GECICI_KAYNAK_B,W
XORWF    GECICI_KAYNAK_D,W
MOVWF    GECICI_SIFRE_3

MOVWF    ANAHTAR1
XORWF    GECICI_KAYNAK_2,W
MOVWF    GECICI_KAYNAK_A
XORWF    GECICI_KAYNAK_1,W
MOVWF    GECICI_SIFRE_1

RLF      ANAHTAR1,W
XORWF    GECICI_KAYNAK_B,W
MOVWF    GECICI_KAYNAK_C
XORWF    GECICI_KAYNAK_2,W
MOVWF    GECICI_SIFRE_2

BCF      STATUS,C
RETURN

SIFRE_OKU
;EEPROM BELLEKTEKI 3 KAYNAK
;DEGERINI OKUR

BANKSEL  EEADR
MOVLW    h'00'

MOVWF    EEADR
BSF      EECON1,RD

MOVF     EEDATA,W

BANKSEL  GECICI_KAYNAK_1
MOVWF    GECICI_KAYNAK_1

BANKSEL  EEADR
MOVLW    h'01'

MOVWF    EEADR

BSF      EECON1,RD

MOVF     EEDATA,W

BANKSEL  GECICI_KAYNAK_2
MOVWF    GECICI_KAYNAK_2

BANKSEL  EEADR
MOVLW    h'02'

MOVWF    EEADR

BSF      EECON1,RD

MOVF     EEDATA,W

BANKSEL  GECICI_KAYNAK_3
MOVWF    GECICI_KAYNAK_3

RETURN

```

EK-A'NIN DEVAMI

```

;EEPROMA 3 KAYNAK
;DEGERINI YAZAR

SIFRE_SIFIRLA
BANKSEL EEADR
MOVLW h'00'
MOVWF EEADR

MOVLW h'00'
BANKSEL EEDATA
MOVWF EEDATA

;YAZMA ISLEMI İÇİN GEREKLİ
;BAYRAK DÜZENLEMELERİ

BANKSEL PIR1
BCF PIR1,EEIF

BANKSEL EECON1
BSF EECON1,WREN
BCF INTCON,GIE

;YAZMA ISLEMI İÇİN ZORUNLU
;KULLANILMASI GEREKEN KODLAR

MOVLW h'55'
MOVWF EECON2
MOVLW h'AA'
MOVWF EECON2
BSF EECON1,WR

BANKSEL PIR1

DELAY0
BTFSS PIR1,EEIF
GOTO DELAY0

BCF PIR1,EEIF

;h'00' ADRESİ SIFIRLANDI.

BANKSEL EEADR
MOVLW h'01'
MOVWF EEADR

MOVLW h'00'
BANKSEL EEDATA
MOVWF EEDATA

;YAZMA ISLEMI İÇİN GEREKLİ
;BAYRAK DÜZENLEMELERİ

BANKSEL PIR1
BCF PIR1,EEIF

BANKSEL EECON1
BSF EECON1,WREN
BCF INTCON,GIE

;YAZMA ISLEMI İÇİN ZORUNLU
;KULLANILMASI GEREKEN KODLAR

MOVLW h'55'
MOVWF EECON2
MOVLW h'AA'
MOVWF EECON2
BSF EECON1,WR
BANKSEL PIR1

DELAY1
BTFSS PIR1,EEIF
GOTO DELAY1
BCF PIR1,EEIF

;h'01' ADRESİ SIFIRLANDI.

```

```

BANKSEL EEADR
MOVLW h'02'
MOVWF EEADR

MOVLW h'00'
BANKSEL EEDATA
MOVWF EEDATA

;YAZMA ISLEMI İÇİN GEREKLİ
;BAYRAK DÜZENLEMELERİ

BANKSEL PIR1
BCF PIR1,EEIF

BANKSEL EECON1
BSF EECON1,WREN
BCF INTCON,GIE

;YAZMA ISLEMI İÇİN ZORUNLU
;KULLANILMASI GEREKEN KODLAR

MOVLW h'55'
MOVWF EECON2
MOVLW h'AA'
MOVWF EECON2
BSF EECON1,WR

BANKSEL PIR1

DELAY2
BTFSS PIR1,EEIF
GOTO DELAY2

;h'02' ADRESİ SIFIRLANDI.

;YAZMA ISLEMI BITTI, TÜM
;BAYRAKLARI İLK KONUMUNA AL

BCF PIR1,EEIF
BANKSEL EECON1
BCF EECON1,WREN
BSF INTCON,GIE
BANKSEL GECICI_KAYNAK_3
RETURN

;EEPROMA 3 KAYNAK DEGERINI
;YAZAR

```

```

SIFRE_YAZ
BANKSEL EEADR
MOVLW h'00'
MOVWF EEADR

BANKSEL KAYNAK_1
MOVF KAYNAK_1,W
BANKSEL EEDATA
MOVWF EEDATA

;YAZMA ISLEMI İÇİN GEREKLİ
;BAYRAK DÜZENLEMELERİ

BANKSEL PIR1; BANK0'a geç
BCF PIR1,EEIF

BANKSEL EECON1
BSF EECON1,WREN
BCF INTCON,GIE

;YAZMA ISLEMI İÇİN ZORUNLU
;KULLANILMASI GEREKEN KODLAR

MOVLW h'55'
MOVWF EECON2
MOVLW h'AA'
MOVWF EECON2
BSF EECON1,WR

```

EK-A'NIN DEVAMI

```

BANKSEL    PIR1

DELAY3
BTFSS     PIR1,EEIF
GOTO      DELAY3
BCF       PIR1,EEIF

;GECICI_KAYNAK_1 YAZILDI
;GECICI_KAYNAK_2 GEÇİYOR

BANKSEL EEADR
MOVLW     h'01'
MOVWF     EEADR

BANKSEL KAYNAK_2
MOVF      KAYNAK_2,0
BANKSEL EEDATA
MOVWF     EEDATA

;YAZMA ISLEMI İÇİN GEREKLİ
;BAYRAK DÜZENLEMELERİ

BANKSEL    PIR1
BCF       PIR1,EEIF

BANKSEL    EECON1
BSF       EECON1,WREN
BCF       INTCON,GIE

;YAZMA ISLEMI İÇİN ZORUNLU
;KULLANILMASI GEREKEN KODLAR

MOVLW     h'55'
MOVWF     EECON2
MOVLW     h'AA'
MOVWF     EECON2
BSF       EECON1,WR

BANKSEL    PIR1

DELAY4
BTFSS     PIR1,EEIF
GOTO      DELAY4

BCF       PIR1,EEIF

;GECICI_KAYNAK_2 YAZILDI
;GECICI_KAYNAK_3 GEÇİYOR

BANKSEL EEADR
MOVLW     h'02'
MOVWF     EEADR

BANKSEL KAYNAK_3
MOVF      KAYNAK_3,0

BANKSEL EEDATA
MOVWF     EEDATA

;YAZMA ISLEMI İÇİN GEREKLİ
;BAYRAK DÜZENLEMELERİ

BANKSEL    PIR1
BCF       PIR1,EEIF
BANKSEL    EECON1
BSF       EECON1,WREN
BCF       INTCON,GIE

;YAZMA ISLEMI İÇİN ZORUNLU
;KULLANILMASI GEREKEN KODLAR

MOVLW     h'55'
MOVWF     EECON2
MOVLW     h'AA'
MOVWF     EECON2
BSF       EECON1,WR

```

```

BANKSEL    PIR1

DELAY5
BTFSS     PIR1,EEIF
GOTO      DELAY5

;YAZMA ISLEMI BITTI,
;TÜM BAYRAKLARI İLK KONUMUNA AL
BCF       PIR1,EEIF
BANKSEL    EECON1
BCF       EECON1,WREN
BSF       INTCON,GIE
BANKSEL    GECICI_KAYNAK_3
RETURN

;Gecikmeler

Delay255    MOVLW    0xff
              GOTO     d0
Delay100    MOVLW    d'100'
              GOTO     d0
Delay50     MOVLW    d'50'
              GOTO     d0
Delay27     MOVLW    d'27'
              GOTO     d0
Delay20     MOVLW    d'20'
              GOTO     d0
Delay5      MOVLW    0x05
d0          MOVWF     count1
d1          MOVLW     0xC7
              MOVWF     counta
              MOVLW     0x01
              MOVWF     countb
Delay_0     DECFSZ    counta,f
              GOTO     $+2
              DECFSZ    countb,f
              GOTO     Delay_0
              DECFSZ    count1,f
              GOTO     d1
              RETLW     0x00

              END
; 'program sonu'

```

EK-B: ASENKRON ALICI PROGRAM KODLARI

```

;***** ASENKRON ALICI *****
list      p=16f877A
#include <p16f877A.inc>

__CONFIG h'3F31'

w_temp      EQU    0x20
status_temp EQU    0x21

irerror      EQU    0x22

irtimer      EQU    0x23

ircounter    EQU    0x24

ircmd        EQU    0x25

iradr        EQU    0x26

irtemp       EQU    0x27

delay1       EQU    0x28
delay2       EQU    0x29
DEGISTIRICI  EQU    0x2A
DEGISTIRICI1 EQU    0x2B
DEGISTIRICI2 EQU    0x2C
ANAHTAR      EQU    0x2D
ANAHTAR1     EQU    0x2E
delay22      EQU    0x2F
delay11      EQU    0x30
ALINAN_SIFRE_1 EQU    0x31
ALINAN_SIFRE_2 EQU    0x32
ALINAN_SIFRE_3 EQU    0x33
SIFRE_SAYICI EQU    0x34
SIFRE1_1     EQU    0x35
SIFRE1_2     EQU    0x36
SIFRE1_3     EQU    0x37
SIFRE2_1     EQU    0x38
SIFRE2_2     EQU    0x39
SIFRE2_3     EQU    0x3A
SIFRE3_1     EQU    0x3B
SIFRE3_2     EQU    0x3C
SIFRE3_3     EQU    0x3D
SIFRE4_1     EQU    0x3E
SIFRE4_2     EQU    0x3F
SIFRE4_3     EQU    0x40
SIFRE5_1     EQU    0x41
SIFRE5_2     EQU    0x42
SIFRE5_3     EQU    0x43
SIFRE6_1     EQU    0x44
SIFRE6_2     EQU    0x45
SIFRE6_3     EQU    0x46
SIFRE7_1     EQU    0x47
SIFRE7_2     EQU    0x48
SIFRE7_3     EQU    0x49
SIFRE8_1     EQU    0x4A
SIFRE8_2     EQU    0x4B
SIFRE8_3     EQU    0x4C
SIFRE9_1     EQU    0x4D
SIFRE9_2     EQU    0x4E
SIFRE9_3     EQU    0x4F
SIFRE10_1    EQU    0x50
SIFRE10_2    EQU    0x51
SIFRE10_3    EQU    0x52
GECICI_SIFRE_1 EQU    0x53
GECICI_SIFRE_2 EQU    0x54
GECICI_SIFRE_3 EQU    0x55
GECICI_KAYNAK_1 EQU    0x56

GECICI_KAYNAK_2 EQU    0x57
GECICI_KAYNAK_3 EQU    0x58
KAYNAK1_1       EQU    0x59
KAYNAK1_2       EQU    0x5A
KAYNAK1_3       EQU    0x5B
KAYNAK11_1      EQU    0x5C
KAYNAK11_2      EQU    0x5D
KAYNAK11_3      EQU    0x5E
GECICI_KAYNAK_A EQU    0x5F
GECICI_KAYNAK_B EQU    0x61
GECICI_KAYNAK_C EQU    0x62
GECICI_KAYNAK_D EQU    0x63
GECICI_KAYNAK_K EQU    0x64
GECICI_KAYNAK_L EQU    0x65
GOSTERICI       EQU    0x66
GOSTERICI_1     EQU    0x67
GOSTERICI_2     EQU    0x68
hafıza_sıfırla_1 EQU    0x69
hafıza_sıfırla_2 EQU    0x6A
hafıza_sıfırla_3 EQU    0x6B
hafıza_sıfırla_4 EQU    0x6C

KAYNAK2_1       EQU    0xA0
KAYNAK2_2       EQU    0xA1
KAYNAK2_3       EQU    0xA2
KAYNAK3_1       EQU    0xA3
KAYNAK3_2       EQU    0xA4
KAYNAK3_3       EQU    0xA5
KAYNAK4_1       EQU    0xA6
KAYNAK4_2       EQU    0xA7
KAYNAK4_3       EQU    0xA8
KAYNAK5_1       EQU    0xA9
KAYNAK5_2       EQU    0xAA
KAYNAK5_3       EQU    0xAB
KAYNAK6_1       EQU    0xAC
KAYNAK6_2       EQU    0xAD
KAYNAK6_3       EQU    0xAE
KAYNAK7_1       EQU    0xAF
KAYNAK7_2       EQU    0xB0
KAYNAK7_3       EQU    0xB1
KAYNAK8_1       EQU    0xB2
KAYNAK8_2       EQU    0xB3
KAYNAK8_3       EQU    0xB4
KAYNAK9_1       EQU    0xB5
KAYNAK9_2       EQU    0xB6
KAYNAK9_3       EQU    0xB7
KAYNAK10_1      EQU    0xB8
KAYNAK10_2      EQU    0xB9
KAYNAK10_3      EQU    0xBA

led            EQU    0x01

ir             EQU    0x07

;*****

ORG            0x000
GOTO          init

ORG            0x004
MOVWF         w_temp
MOVF          STATUS,w
MOVWF         status_temp

```

EK-B'NİN DEVAMI

;isr kodları bu bölüme yazılarak
;call subroutine olarak çağrılabilir

```

MOVF    status_temp,w
MOVWF   STATUS
SWAPF   w_temp,f
SWAPF   w_temp,w
RETFIE

init
CLRF    PORTD

CLRF    DEGISTIRICI
CLRF    DEGISTIRICI1
CLRF    DEGISTIRICI2
CLRF    ANAHTAR
CLRF    ANAHTAR1
CLRF    DEGISTIRICI
CLRF    DEGISTIRICI1
CLRF    DEGISTIRICI2
CLRF    ANAHTAR
CLRF    ANAHTAR1
CLRF    delay22
CLRF    delay11
CLRF    ALINAN_SIFRE_1
CLRF    ALINAN_SIFRE_2
CLRF    ALINAN_SIFRE_3
CLRF    SIFRE_SAYICI
CLRF    SIFRE1_1
CLRF    SIFRE1_2
CLRF    SIFRE1_3
CLRF    SIFRE2_1
CLRF    SIFRE2_2
CLRF    SIFRE2_3
CLRF    SIFRE3_1
CLRF    SIFRE3_2
CLRF    SIFRE3_3
CLRF    SIFRE4_1
CLRF    SIFRE4_2
CLRF    SIFRE4_3
CLRF    SIFRE5_1
CLRF    SIFRE5_2
CLRF    SIFRE5_3
CLRF    SIFRE6_1
CLRF    SIFRE6_2
CLRF    SIFRE6_3
CLRF    SIFRE7_1
CLRF    SIFRE7_2
CLRF    SIFRE7_3
CLRF    SIFRE8_1
CLRF    SIFRE8_2
CLRF    SIFRE8_3
CLRF    SIFRE9_1
CLRF    SIFRE9_2
CLRF    SIFRE9_3
CLRF    SIFRE10_1
CLRF    SIFRE10_2
CLRF    SIFRE10_3
CLRF    GECICI_SIFRE_1
CLRF    GECICI_SIFRE_2
CLRF    GECICI_SIFRE_3
CLRF    GECICI_KAYNAK_1
CLRF    GECICI_KAYNAK_2
CLRF    GECICI_KAYNAK_3
CLRF    KAYNAK1_1
CLRF    KAYNAK1_2
CLRF    KAYNAK1_3
CLRF    KAYNAK11_1
CLRF    KAYNAK11_2
CLRF    KAYNAK11_3
CLRF    GECICI_KAYNAK_A
CLRF    GECICI_KAYNAK_B
CLRF    GECICI_KAYNAK_C
CLRF    GECICI_KAYNAK_D
CLRF    GECICI_KAYNAK_K
CLRF    GECICI_KAYNAK_L

```

```

BANKSEL KAYNAK2_1
CLRF    KAYNAK2_1
CLRF    KAYNAK2_2
CLRF    KAYNAK2_3
CLRF    KAYNAK3_1
CLRF    KAYNAK3_2
CLRF    KAYNAK3_3
CLRF    KAYNAK4_1
CLRF    KAYNAK4_2
CLRF    KAYNAK4_3
CLRF    KAYNAK5_1
CLRF    KAYNAK5_2
CLRF    KAYNAK5_3
CLRF    KAYNAK6_1
CLRF    KAYNAK6_2
CLRF    KAYNAK6_3
CLRF    KAYNAK7_1
CLRF    KAYNAK7_2
CLRF    KAYNAK7_3
CLRF    KAYNAK8_1
CLRF    KAYNAK8_2
CLRF    KAYNAK8_3
CLRF    KAYNAK9_1
CLRF    KAYNAK9_2
CLRF    KAYNAK9_3
CLRF    KAYNAK10_1
CLRF    KAYNAK10_2
CLRF    KAYNAK10_3
BANKSEL PORTA
CALL    delayrout1
CALL    delayrout1
CALL    delayrout1
CLRF    ircmd
CLRF    iradr
BCF     STATUS, RP1
BSF     STATUS, RP0

MOVLW  0X07
MOVWF   CMCON

MOVLW  b'10000000'
MOVWF   TRISB

MOVLW  b'00000000'
MOVWF   TRISC

MOVLW  b'00000000'
MOVWF   TRISD

BANKSEL PIE2
BSF    PIE2,EEIE

BANKSEL OPTION_REG
MOVLW  b'10000101'
MOVWF  OPTION_REG
BCF    STATUS,RP0

BASLA
CALL    SIFRE_OKU
MOVF    GECICI_KAYNAK_1,W
MOVWF   KAYNAK11_1
MOVF    GECICI_KAYNAK_2,W
MOVWF   KAYNAK11_2
MOVF    GECICI_KAYNAK_3,W
MOVWF   KAYNAK11_3

MOVLW  h'0A'
MOVWF   SIFRE_SAYICI
CALL    SIFRE_URET

MOVLW  h'00'
MOVWF   GOSTERICI
CALL    goster

CLRF    PORTB
BSF     PORTB,1

```

test

```
CALL    read_sony
BTFSC  irerror,0
GOTO   test
CALL    ir_to_outp
CALL    delayrout1
GOTO   test
```

read_sony

```
BSF     irerror,0
BCF     INTCON,GIE
CLRWDI

BTFSC  PORTB,ir

GOTO   end_sony
CLRF   TMR0
```

sony_st1

```
BTFSS  PORTB,ir
GOTO   sony_st1
MOVF    TMR0,0
MOVWF  irtimer
MOVLW  d'64'

SUBWF  irtimer,0
BTFSS  STATUS,C
GOTO   end_sony

MOVLW  d'170'

ADDWF  irtimer,0
BTFSC  STATUS,C
GOTO   end_sony

MOVLW  d'8'
MOVWF  ircounter
```

rd_sony_cmd

```
CLRF   TMR0
```

sony_prt1_c

```
BTFSC  PORTB,ir
GOTO   sony_prt1_c

MOVF    TMR0,0
MOVWF  irtimer

MOVLW  d'5'
SUBWF  irtimer,0
BTFSS  STATUS,C
GOTO   end_sony

MOVLW  d'241'

ADDWF  irtimer,0
BTFSC  STATUS,C
GOTO   end_sony
CLRF   TMR0
CLRWDI
```

sony_prt2_c

```
BTFSS  PORTB,ir
GOTO   sony_prt2_c
MOVF    TMR0,0
MOVWF  irtimer
MOVLW  d'5'
SUBWF  irtimer,0
BTFSS  STATUS,C
GOTO   end_sony
MOVLW  d'230'

ADDWF  irtimer,0
BTFSC  STATUS,C
GOTO   end_sony
MOVLW  d'241'
```

```
ADDWF  irtimer,0
BTFSC  STATUS,C
GOTO   sony_its_1
```

sony_its_0

```
BCF     STATUS,C
RRF     ircmd,1
GOTO   nxt_sony_cmd
```

sony_its_1

```
BSF     STATUS,C
RRF     ircmd,1
```

nxt_sony_cmd

```
DECFSZ  ircounter,1
GOTO   rd_sony_cmd
BCF     STATUS,C
MOVLW  d'4'
MOVWF  ircounter
```

rd_sony_adr

```
CLRF   TMR0
```

sony_prt1_a

```
BTFSC  PORTB,ir
GOTO   sony_prt1_a
MOVF    TMR0,0
MOVWF  irtimer
MOVLW  d'5'
SUBWF  irtimer,0
BTFSS  STATUS,C
GOTO   end_sony
MOVLW  d'241'
ADDWF  irtimer,0
BTFSC  STATUS,C
GOTO   end_sony
CLRF   TMR0
CLRWDI;
```

sony_prt2_a

```
BTFSS  PORTB,ir;
GOTO   sony_prt2_a
MOVF    TMR0,0
MOVWF  irtimer
MOVLW  d'5'
SUBWF  irtimer,0
BTFSS  STATUS,C
GOTO   end_sony
MOVLW  d'230'
ADDWF  irtimer,0
BTFSC  STATUS,C
GOTO   end_sony
MOVLW  d'241'
ADDWF  irtimer,0
BTFSC  STATUS,C
GOTO   sony_its_1_a
```

sony_its_0_a

```
BCF     STATUS,C
RRF     iradr,1
GOTO   nxt_sony_adr
```

sony_its_1_a

```
BSF     STATUS,C
RRF     iradr,1
```

nxt_sony_adr

```
DECFSZ  ircounter,1
GOTO   rd_sony_adr

BCF     STATUS,C

MOVLW  h'04'
MOVWF  ircounter
```

EK-B'NİN DEVAMI

```

kaydır
BCF STATUS,C
RRF iradr,1
DECFSZ ircounter,1
GOTO kaydır
BCF STATUS,C
CLRF irerror

end_sony
BCF INTCON,TMR0IF

BSF STATUS,RP0
MOVLW b'10000101'
MOVWF OPTION_REG
BCF STATUS,RP0
RETURN

ir_to_outp
MOVF ircmd,w
MOVWF irtemp
BCF STATUS,Z
MOVF iradr,w
SUBLW h'01'
BTFSZ STATUS,Z
GOTO sifre_2
MOVF irtemp,w
MOVWF ALINAN_SIFRE_1
MOVWF GOSTERICI
CALL goster
BCF STATUS,Z
RETURN

sifre_2
BCF STATUS,Z
MOVF iradr,w
SUBLW h'02'
BTFSZ STATUS,Z
GOTO sifre_3
MOVF irtemp,w
MOVWF ALINAN_SIFRE_2
MOVWF GOSTERICI
CALL goster
BCF STATUS,Z
RETURN

sifre_3
BCF STATUS,Z
MOVF iradr,w
SUBLW h'03'
BTFSZ STATUS,Z
GOTO sifre_4
MOVF irtemp,w
MOVWF ALINAN_SIFRE_3
MOVWF GOSTERICI
CALL goster
BCF STATUS,Z
GOTO SIFRE_KONTROL_1

sifre_4
BCF STATUS,Z
MOVF iradr,w
SUBLW h'04'
BTFSZ STATUS,Z
GOTO sifre_5
MOVF irtemp,w
MOVWF hafıza_sıfırla_1
MOVWF GOSTERICI
CALL goster
BCF STATUS,Z
RETURN

sifre_5
BCF STATUS,Z
MOVF iradr,w
SUBLW h'05'
BTFSZ STATUS,Z

GOTO sifre_6
MOVF irtemp,w
MOVWF hafıza_sıfırla_2
MOVWF GOSTERICI
CALL goster
BCF STATUS,Z
RETURN

sifre_6
BCF STATUS,Z
MOVF iradr,w
SUBLW h'06'
BTFSZ STATUS,Z
GOTO sifre_7
MOVF irtemp,w
MOVWF hafıza_sıfırla_3
MOVWF GOSTERICI
CALL goster
BCF STATUS,Z
RETURN

sifre_7
BCF STATUS,Z
MOVF iradr,w
SUBLW h'07'
BTFSZ STATUS,Z
RETURN
MOVF irtemp,w
MOVWF hafıza_sıfırla_4
MOVWF GOSTERICI
CALL goster
BCF STATUS,Z
GOTO hafıza_sıfırla

SIFRE_KONTROL_1
BCF STATUS,Z
MOVF SIFRE1_1,W
SUBWF ALINAN_SIFRE_1,W
BTFSZ STATUS,Z
GOTO SIFRE_KONTROL_2
BCF STATUS,Z
MOVF SIFRE1_2,W
SUBWF ALINAN_SIFRE_2,W
BTFSZ STATUS,Z
GOTO SIFRE_KONTROL_2
BCF STATUS,Z
MOVF SIFRE1_3,W
SUBWF ALINAN_SIFRE_3,W
BTFSZ STATUS,Z
GOTO SIFRE_KONTROL_2
;SIFRENİN DOĞRU OLDUĞUNU GÖRDÜ
MOVLW h'01'
MOVWF SIFRE_SAYICI
GOTO SIFRE_DOĞRU

SIFRE_KONTROL_2
BCF STATUS,Z
MOVF SIFRE2_1,W
SUBWF ALINAN_SIFRE_1,W
BTFSZ STATUS,Z
GOTO SIFRE_KONTROL_3
BCF STATUS,Z
MOVF SIFRE2_2,W
SUBWF ALINAN_SIFRE_2,W
BTFSZ STATUS,Z
GOTO SIFRE_KONTROL_3
BCF STATUS,Z
MOVF SIFRE2_3,W
SUBWF ALINAN_SIFRE_3,W
BTFSZ STATUS,Z
GOTO SIFRE_KONTROL_3
;SIFRENİN DOĞRU OLDUĞUNU GÖRDÜ
MOVLW h'02'
MOVWF SIFRE_SAYICI
GOTO SIFRE_DOĞRU

```

EK-B'NİN DEVAMI

SIFRE_KONTROL_3

```
BCF STATUS,Z
MOVF SIFRE3_1,W
SUBWF ALINAN_SIFRE_1,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_4
BCF STATUS,Z
MOVF SIFRE3_2,W
SUBWF ALINAN_SIFRE_2,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_4
BCF STATUS,Z
MOVF SIFRE3_3,W
SUBWF ALINAN_SIFRE_3,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_4
;SIFRENIN DOGRU OLDUGUNU GORDU
MOVLW h'03'
MOVWF SIFRE_SAYICI
GOTO SIFRE_DOGRU
```

SIFRE_KONTROL_4

```
BCF STATUS,Z
MOVF SIFRE4_1,W
SUBWF ALINAN_SIFRE_1,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_5
BCF STATUS,Z
MOVF SIFRE4_2,W
SUBWF ALINAN_SIFRE_2,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_5
BCF STATUS,Z
MOVF SIFRE4_3,W
SUBWF ALINAN_SIFRE_3,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_5
;SIFRENIN DOGRU OLDUGUNU GORDU
MOVLW h'04'
MOVWF SIFRE_SAYICI
GOTO SIFRE_DOGRU
```

SIFRE_KONTROL_5

```
BCF STATUS,Z
MOVF SIFRE5_1,W
SUBWF ALINAN_SIFRE_1,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_6
BCF STATUS,Z
MOVF SIFRE5_2,W
SUBWF ALINAN_SIFRE_2,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_6
BCF STATUS,Z
MOVF SIFRE5_3,W
SUBWF ALINAN_SIFRE_3,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_6
;SIFRENIN DOGRU OLDUGUNU GORDU
MOVLW h'05'
MOVWF SIFRE_SAYICI
GOTO SIFRE_DOGRU
```

SIFRE_KONTROL_6

```
BCF STATUS,Z
MOVF SIFRE6_1,W
SUBWF ALINAN_SIFRE_1,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_7
BCF STATUS,Z
MOVF SIFRE6_2,W
SUBWF ALINAN_SIFRE_2,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_7
BCF STATUS,Z
MOVF SIFRE6_3,W
```

```
SUBWF ALINAN_SIFRE_3,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_7
;SIFRENIN DOGRU OLDUGUNU GORDU
MOVLW h'06'
MOVWF SIFRE_SAYICI
GOTO SIFRE_DOGRU
```

SIFRE_KONTROL_7

```
BCF STATUS,Z
MOVF SIFRE7_1,W
SUBWF ALINAN_SIFRE_1,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_8
BCF STATUS,Z
MOVF SIFRE7_2,W
SUBWF ALINAN_SIFRE_2,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_8
BCF STATUS,Z
MOVF SIFRE7_3,W
SUBWF ALINAN_SIFRE_3,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_8
;SIFRENIN DOGRU OLDUGUNU GORDU
MOVLW h'07'
MOVWF SIFRE_SAYICI
GOTO SIFRE_DOGRU
```

SIFRE_KONTROL_8

```
BCF STATUS,Z
MOVF SIFRE8_1,W
SUBWF ALINAN_SIFRE_1,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_9
BCF STATUS,Z
MOVF SIFRE8_2,W
SUBWF ALINAN_SIFRE_2,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_9
BCF STATUS,Z
MOVF SIFRE8_3,W
SUBWF ALINAN_SIFRE_3,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_9
;SIFRENIN DOGRU OLDUGUNU GORDU
MOVLW h'08'
MOVWF SIFRE_SAYICI
GOTO SIFRE_DOGRU
```

SIFRE_KONTROL_9

```
BCF STATUS,Z
MOVF SIFRE9_1,W
SUBWF ALINAN_SIFRE_1,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_10
BCF STATUS,Z
MOVF SIFRE9_2,W
SUBWF ALINAN_SIFRE_2,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_10
BCF STATUS,Z
MOVF SIFRE9_3,W
SUBWF ALINAN_SIFRE_3,W
BTFSS STATUS,Z
GOTO SIFRE_KONTROL_10
;SIFRENIN DOGRU OLDUGUNU GORDU
MOVLW h'09'
MOVWF SIFRE_SAYICI
GOTO SIFRE_DOGRU
```

SIFRE_KONTROL_10

```
BCF STATUS,Z
MOVF SIFRE10_1,W
SUBWF ALINAN_SIFRE_1,W
BTFSS STATUS,Z
```

EK-B'NİN DEVAMI

```

GOTO    YANLIS_SIFRE
BCF     STATUS,Z
MOVF    SIFRE10_2,W
SUBWF   ALINAN_SIFRE_2,W
BTFSS   STATUS,Z
GOTO    YANLIS_SIFRE
BCF     STATUS,Z
MOVF    SIFRE10_3,W
SUBWF   ALINAN_SIFRE_3,W
BTFSS   STATUS,Z
GOTO    YANLIS_SIFRE
;SIFRENIN DOGRU OLDUGUNU GORDU
MOVLW   h'0A'
MOVWF   SIFRE_SAYICI
GOTO    SIFRE_DOGRU

hafıza_sıfırla
BCF     STATUS,Z
MOVF    hafıza_sıfırla_1,w
XORLW   h'06'

BTFSS   STATUS,Z
GOTO    YANLIS_SIFRE
BCF     STATUS,Z

MOVF    hafıza_sıfırla_2,w
XORLW   h'01'

BTFSS   STATUS,Z
GOTO    YANLIS_SIFRE
BCF     STATUS,Z

MOVF    hafıza_sıfırla_3,w
XORLW   h'01'

BTFSS   STATUS,Z
GOTO    YANLIS_SIFRE
BCF     STATUS,Z

MOVF    hafıza_sıfırla_4,w
XORLW   h'09'

BTFSS   STATUS,Z
GOTO    YANLIS_SIFRE
BCF     STATUS,Z

;BUNDAN SONRA rastgele URETTİĞİ
;ŞİFRELERİ KARŞIYA KRİPTO
;ALGORİTMASINDAN GEÇİREREK GONDERECEK.

CALL    sifre_sıfırla
CLRF    DEGISTIRICI

CLRF    DEGISTIRICI1
CLRF    DEGISTIRICI2
CLRF    ANAHTAR
CLRF    ANAHTAR1
CLRF    DEGISTIRICI
CLRF    DEGISTIRICI1
CLRF    DEGISTIRICI2
CLRF    ANAHTAR
CLRF    ANAHTAR1
CLRF    delay22
CLRF    delay11
CLRF    ALINAN_SIFRE_1
CLRF    ALINAN_SIFRE_2
CLRF    ALINAN_SIFRE_3
CLRF    SIFRE_SAYICI
CLRF    SIFRE1_1
CLRF    SIFRE1_2
CLRF    SIFRE1_3
CLRF    SIFRE2_1
CLRF    SIFRE2_2
CLRF    SIFRE2_3

CLRF    SIFRE3_1
CLRF    SIFRE3_2
CLRF    SIFRE3_3
CLRF    SIFRE4_1
CLRF    SIFRE4_2
CLRF    SIFRE4_3
CLRF    SIFRE5_1
CLRF    SIFRE5_2
CLRF    SIFRE5_3
CLRF    SIFRE6_1
CLRF    SIFRE6_2
CLRF    SIFRE6_3
CLRF    SIFRE7_1
CLRF    SIFRE7_2
CLRF    SIFRE7_3
CLRF    SIFRE8_1
CLRF    SIFRE8_2
CLRF    SIFRE8_3
CLRF    SIFRE9_1
CLRF    SIFRE9_2
CLRF    SIFRE9_3
CLRF    SIFRE10_1
CLRF    SIFRE10_2
CLRF    SIFRE10_3
CLRF    GECICI_SIFRE_1
CLRF    GECICI_SIFRE_2
CLRF    GECICI_SIFRE_3
CLRF    GECICI_KAYNAK_1
CLRF    GECICI_KAYNAK_2
CLRF    GECICI_KAYNAK_3
CLRF    KAYNAK1_1
CLRF    KAYNAK1_2
CLRF    KAYNAK1_3
CLRF    KAYNAK11_1
CLRF    KAYNAK11_2
CLRF    KAYNAK11_3
CLRF    GECICI_KAYNAK_A
CLRF    GECICI_KAYNAK_B
CLRF    GECICI_KAYNAK_C
CLRF    GECICI_KAYNAK_D
CLRF    GECICI_KAYNAK_K
CLRF    GECICI_KAYNAK_L
BANKSEL KAYNAK2_1
CLRF    KAYNAK2_1
CLRF    KAYNAK2_2
CLRF    KAYNAK2_3
CLRF    KAYNAK3_1
CLRF    KAYNAK3_2
CLRF    KAYNAK3_3
CLRF    KAYNAK4_1
CLRF    KAYNAK4_2
CLRF    KAYNAK4_3
CLRF    KAYNAK5_1
CLRF    KAYNAK5_2
CLRF    KAYNAK5_3
CLRF    KAYNAK6_1
CLRF    KAYNAK6_2
CLRF    KAYNAK6_3
CLRF    KAYNAK7_1
CLRF    KAYNAK7_2
CLRF    KAYNAK7_3
CLRF    KAYNAK8_1
CLRF    KAYNAK8_2
CLRF    KAYNAK8_3
CLRF    KAYNAK9_1
CLRF    KAYNAK9_2
CLRF    KAYNAK9_3
CLRF    KAYNAK10_1
CLRF    KAYNAK10_2
CLRF    KAYNAK10_3
BANKSEL PORTA
MOVLW   h'0A'
MOVWF   SIFRE_SAYICI
CALL    SIFRE_URET
BSF     PORTB,2
CALL    delayrout11

```

EK-B'NİN DEVAMI

```

BCF      PORTB,2
CALL     delayrout11
BSF      PORTB,2
CALL     delayrout11
BCF      PORTB,2
CALL     delayrout11
BSF      PORTB,2
CALL     delayrout11
BCF      PORTB,2
MOVLW    h'00'
MOVWF    GOSTERICI
CALL     goster
RETURN

YANLIŞ_SIFRE
BCF      PORTB,0
MOVLW    h'00'
MOVWF    GOSTERICI
CALL     goster
RETURN

SIFRE_DOGRU
BSF      PORTB,0
BCF      PORTB,led

;1-2 SANİYE KADAR SİSTEM AÇIK
;İKAZINI VERİP TEKRAR SİSTEMİ
;KAPATILARAK TÜM GEÇİCİ VERİLERİ SİLSİN!

BSF      PORTB,2 ;BUZZER SES VER!
CALL     delayrout11
BCF      PORTB,2 ;BUZZER KAPAT!
CALL     delayrout11
BSF      PORTB,2 ;BUZZER SES VER!
CALL     delayrout11
BCF      PORTB,2 ;BUZZER KAPAT!
CALL     delayrout11
BSF      PORTB,2 ;BUZZER SES VER!
CALL     delayrout11
BCF      PORTB,2 ;BUZZER KAPAT!
CALL     delayrout11

BSF      PORTB,2 ;BUZZER SES VER!
CALL     delayrout11
CALL     delayrout11

BCF      PORTB,2 ;BUZZER KAPAT!
CALL     delayrout11
BSF      PORTB,2 ;BUZZER SES VER!
CALL     delayrout11
BCF      PORTB,2 ;BUZZER KAPAT!
CALL     delayrout11
BSF      PORTB,2 ;BUZZER SES VER!
CALL     delayrout11
BCF      PORTB,2 ;BUZZER KAPAT!
CALL     delayrout11
BSF      PORTB,2 ;BUZZER SES VER!
CALL     delayrout11
BCF      PORTB,2 ;BUZZER KAPAT!
CALL     delayrout11
BSF      PORTB,2 ;BUZZER SES VER!
CALL     delayrout11
BCF      PORTB,2 ;BUZZER KAPAT!
CALL     delayrout11
BCF      STATUS,Z;
BCF      PORTB,0 ; KİLİDİ KAPAT
BCF      PORTB,2 ; BUZZER KAPAT

MOVLW    h'00'
MOVWF    GOSTERICI
CALL     goster

CALL     SIFRE_URET
BSF      PORTB,led

RETURN

goster
MOVF     GOSTERICI,W
ANDLW    h'0F'
MOVWF    GOSTERICI_1

MOVF     GOSTERICI,W
ANDLW    h'F0'
MOVWF    GOSTERICI

MOVLW    h'04'
MOVWF    ircounter

kaydır_1
BCF      STATUS,C
RRF      GOSTERICI,1
DECFSZ   ircounter,1
GOTO     kaydır_1
BCF      STATUS,C

MOVF     GOSTERICI,W
MOVWF    GOSTERICI_2

MOVF     GOSTERICI_1,W
MOVWF    GOSTERICI
CALL     DISPLAY
MOVF     GOSTERICI,W
MOVWF    PORTC

MOVF     GOSTERICI_2,W
MOVWF    GOSTERICI
CALL     DISPLAY
MOVF     GOSTERICI,W
MOVWF    PORTD

RETURN

DISPLAY
BCF      STATUS,Z
MOVF     GOSTERICI,W
BTFS     STATUS,Z
GOTO     DISPLAY_1
MOVLW    h'3F'
MOVWF    GOSTERICI
BCF      STATUS,Z
RETURN

DISPLAY_1
BCF      STATUS,Z
MOVF     GOSTERICI,W
SUBLW    h'01'
BTFS     STATUS,Z
GOTO     DISPLAY_2
MOVLW    h'06'
MOVWF    GOSTERICI
BCF      STATUS,Z
RETURN

DISPLAY_2
BCF      STATUS,Z
MOVF     GOSTERICI,W
SUBLW    h'02'
BTFS     STATUS,Z
GOTO     DISPLAY_3
MOVLW    h'5B'
MOVWF    GOSTERICI
BCF      STATUS,Z
RETURN

DISPLAY_3
BCF      STATUS,Z
MOVF     GOSTERICI,W
SUBLW    h'03'
BTFS     STATUS,Z
GOTO     DISPLAY_4

```

EK-B'NİN DEVAMI

```

        MOVLW    h'4F'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN
DISPLAY_4
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'04'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_5
        MOVLW    h'66'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN
DISPLAY_5
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'05'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_6
        MOVLW    h'6D'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN
DISPLAY_6
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'06'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_7
        MOVLW    h'7D'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN
DISPLAY_7
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'07'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_8
        MOVLW    h'07'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN
DISPLAY_8
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'08'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_9
        MOVLW    h'7F'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN
DISPLAY_9
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'09'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_10
        MOVLW    h'6F'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN
DISPLAY_10
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'0A'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_11
        MOVLW    h'77'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN
DISPLAY_11
        BCF      STATUS,Z

```

```

        MOVF     GOSTERICI,W
        SUBLW    h'0B'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_12
        MOVLW    h'7C'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN
DISPLAY_12
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'0C'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_13
        MOVLW    h'39'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN
DISPLAY_13
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'0D'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_14
        MOVLW    h'5E'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN
DISPLAY_14
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'0E'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_15
        MOVLW    h'79'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN
DISPLAY_15
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'0F'
        BTFSS    STATUS,Z
        RETURN
        MOVLW    h'71'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN
SIFRE_URET
        CALL     YENI_SIFRE

        MOVF     SIFRE2_1,W
        MOVWF    SIFRE1_1
        MOVF     SIFRE2_2,W
        MOVWF    SIFRE1_2
        MOVF     SIFRE2_3,W
        MOVWF    SIFRE1_3

        MOVF     SIFRE3_1,W
        MOVWF    SIFRE2_1
        MOVF     SIFRE3_2,W
        MOVWF    SIFRE2_2
        MOVF     SIFRE3_3,W
        MOVWF    SIFRE2_3

        MOVF     SIFRE4_1,W
        MOVWF    SIFRE3_1
        MOVF     SIFRE4_2,W
        MOVWF    SIFRE3_2
        MOVF     SIFRE4_3,W
        MOVWF    SIFRE3_3

        MOVF     SIFRE5_1,W
        MOVWF    SIFRE4_1
        MOVF     SIFRE5_2,W

```

EK-B'NİN DEVAMI

```

MOVWF SIFRE4_2
MOVWF SIFRE5_3,W
MOVWF SIFRE4_3

MOVWF SIFRE6_1,W
MOVWF SIFRE5_1
MOVWF SIFRE6_2,W
MOVWF SIFRE5_2
MOVWF SIFRE6_3,W
MOVWF SIFRE5_3

MOVWF SIFRE7_1,W
MOVWF SIFRE6_1
MOVWF SIFRE7_2,W
MOVWF SIFRE6_2
MOVWF SIFRE7_3,W
MOVWF SIFRE6_3

MOVWF SIFRE8_1,W
MOVWF SIFRE7_1
MOVWF SIFRE8_2,W
MOVWF SIFRE7_2
MOVWF SIFRE8_3,W
MOVWF SIFRE7_3

MOVWF SIFRE9_1,W
MOVWF SIFRE8_1
MOVWF SIFRE9_2,W
MOVWF SIFRE8_2
MOVWF SIFRE9_3,W
MOVWF SIFRE8_3

MOVWF SIFRE10_1,W
MOVWF SIFRE9_1
MOVWF SIFRE10_2,W
MOVWF SIFRE9_2
MOVWF SIFRE10_3,W
MOVWF SIFRE9_3

MOVWF GECICI_SIFRE_1,W
MOVWF SIFRE10_1
MOVWF GECICI_SIFRE_2,W
MOVWF SIFRE10_2
MOVWF GECICI_SIFRE_3,W
MOVWF SIFRE10_3

DECFSZ SIFRE_SAYICI
GOTO SIFRE_URET
CALL SIFRE_YAZ

RETURN

YENI_SIFRE
BCF STATUS,C
INCF GECICI_KAYNAK_1,F
BCF STATUS,Z
MOVF DEGISTIRICI,W
BTFSS STATUS,Z
GOTO DIGER
RRF GECICI_KAYNAK_1,F
RRF GECICI_KAYNAK_1,F
INCF GECICI_KAYNAK_1,F
MOVLW h'04'
MOVWF DEGISTIRICI
GOTO DEVAM

DIGER
RLF GECICI_KAYNAK_1,F
DECF DEGISTIRICI,F

DEVAM
DECF GECICI_KAYNAK_2,F
BCF STATUS,Z
MOVF DEGISTIRICI1,W
BTFSS STATUS,Z
GOTO DIGER1
RLF GECICI_KAYNAK_2,F

INCF GECICI_KAYNAK_2,F
MOVLW h'03'
MOVWF DEGISTIRICI1
GOTO DEVAM1

DIGER1
RRF GECICI_KAYNAK_2,F
RRF GECICI_KAYNAK_2,F
DECF DEGISTIRICI1,F

DEVAM1
INCF GECICI_KAYNAK_3,F
INCF GECICI_KAYNAK_3,F
BCF STATUS,Z
MOVF DEGISTIRICI2,W
BTFSS STATUS,Z
GOTO DIGER2
RRF GECICI_KAYNAK_3,F
DECF GECICI_KAYNAK_3,F
MOVLW h'03'
MOVWF DEGISTIRICI2
GOTO DEVAM2

DIGER2
DECF GECICI_KAYNAK_3,F
RLF GECICI_KAYNAK_3,F
DECF DEGISTIRICI2

DEVAM2
BANKSEL KAYNAK2_1
MOVF KAYNAK2_1,W
BANKSEL KAYNAK1_1
MOVWF KAYNAK1_1
BANKSEL KAYNAK2_2
MOVF KAYNAK2_2,W
BANKSEL KAYNAK1_2
MOVWF KAYNAK1_2
BANKSEL KAYNAK2_3
MOVF KAYNAK2_3,W
BANKSEL KAYNAK1_3
MOVWF KAYNAK1_3

BANKSEL KAYNAK3_1
MOVF KAYNAK3_1,W
MOVWF KAYNAK2_1
MOVF KAYNAK3_2,W
MOVWF KAYNAK2_2
MOVF KAYNAK3_3,W
MOVWF KAYNAK2_3

MOVF KAYNAK4_1,W
MOVWF KAYNAK3_1
MOVF KAYNAK4_2,W
MOVWF KAYNAK3_2
MOVF KAYNAK4_3,W
MOVWF KAYNAK3_3

MOVF KAYNAK5_1,W
MOVWF KAYNAK4_1
MOVF KAYNAK5_2,W
MOVWF KAYNAK4_2
MOVF KAYNAK5_3,W
MOVWF KAYNAK4_3

MOVF KAYNAK6_1,W
MOVWF KAYNAK5_1
MOVF KAYNAK6_2,W
MOVWF KAYNAK5_2
MOVF KAYNAK6_3,W
MOVWF KAYNAK5_3

MOVF KAYNAK7_1,W
MOVWF KAYNAK6_1
MOVF KAYNAK7_2,W
MOVWF KAYNAK6_2
MOVF KAYNAK7_3,W
MOVWF KAYNAK6_3

```

EK-B'NİN DEVAMI

```

MOVF    KAYNAK8_1,W
MOVWF   KAYNAK7_1
MOVF    KAYNAK8_2,W
MOVWF   KAYNAK7_2
MOVF    KAYNAK8_3,W
MOVWF   KAYNAK7_3

```

```

MOVF    KAYNAK9_1,W
MOVWF   KAYNAK8_1
MOVF    KAYNAK9_2,W
MOVWF   KAYNAK8_2
MOVF    KAYNAK9_3,W
MOVWF   KAYNAK8_3

```

```

MOVF    KAYNAK10_1,W
MOVWF   KAYNAK9_1
MOVF    KAYNAK10_2,W
MOVWF   KAYNAK9_2
MOVF    KAYNAK10_3,W
MOVWF   KAYNAK9_3

```

```

BANKSEL KAYNAK11_1
MOVF    KAYNAK11_1,W
BANKSEL KAYNAK10_1
MOVWF   KAYNAK10_1
BANKSEL KAYNAK11_2
MOVF    KAYNAK11_2,W
BANKSEL KAYNAK10_2
MOVWF   KAYNAK10_2
BANKSEL KAYNAK11_3
MOVF    KAYNAK11_3,W
BANKSEL KAYNAK10_3
MOVWF   KAYNAK10_3

```

```

BANKSEL GECICI_KAYNAK_1
MOVF    GECICI_KAYNAK_1,W
MOVWF   KAYNAK11_1
MOVF    GECICI_KAYNAK_2,W
MOVWF   KAYNAK11_2
MOVF    GECICI_KAYNAK_3,W
MOVWF   KAYNAK11_3

```

```

BCF     STATUS,C
MOVLW  h'05'

```

```

MOVWF   ANAHTAR
MOVLW  h'F0'
ANDWF   GECICI_KAYNAK_3,W
MOVWF   GECICI_KAYNAK_K

```

```

MOVLW  h'04'
MOVWF   ircounter

```

kaydır1

```

BCF     STATUS,C
RRF     GECICI_KAYNAK_K,1
DECFSZ  ircounter,1
GOTO    kaydır1
BCF     STATUS,C

```

```

MOVLW  h'0F'
ANDWF   GECICI_KAYNAK_3,W
MOVWF   GECICI_KAYNAK_L

```

```

MOVF    ANAHTAR,W
XORWF   GECICI_KAYNAK_L,W
MOVWF   GECICI_KAYNAK_A
XORWF   GECICI_KAYNAK_K,W
MOVWF   GECICI_KAYNAK_B

```

```

RLF     ANAHTAR,W
XORWF   GECICI_KAYNAK_B,W
MOVWF   GECICI_KAYNAK_C
XORWF   GECICI_KAYNAK_L,W
MOVWF   GECICI_KAYNAK_D

```

```

MOVLW  h'04'
MOVWF   ircounter

```

kaydır2

```

BCF     STATUS,C
RLF     GECICI_KAYNAK_B,1
DECFSZ  ircounter,1
GOTO    kaydır2
BCF     STATUS,C
MOVF    GECICI_KAYNAK_B,W
XORWF   GECICI_KAYNAK_D,W
MOVWF   GECICI_SIFRE_3

```

```

MOVWF   ANAHTAR1
XORWF   GECICI_KAYNAK_2,W
MOVWF   GECICI_KAYNAK_A
XORWF   GECICI_KAYNAK_1,W
MOVWF   GECICI_SIFRE_1

```

```

RLF     ANAHTAR1,W
XORWF   GECICI_KAYNAK_B,W
MOVWF   GECICI_KAYNAK_C
XORWF   GECICI_KAYNAK_2,W
MOVWF   GECICI_SIFRE_2
BCF     STATUS,C
RETURN

```

SIFRE_OKU

```

;EEPROM BELLEKTEKİ 3 KAYNAK
;DEGERİNİ OKUR

```

```

BANKSEL EEADR
MOVLW  h'00'

```

```

MOVWF   EEADR

```

```

BANKSEL EECON1
BCF     EECON1,EEPGD
BSF     EECON1, RD

```

```

BANKSEL EEDATA
MOVF    EEDATA,W

```

```

BANKSEL GECICI_KAYNAK_1
MOVWF   GECICI_KAYNAK_1

```

```

BANKSEL EEADR
MOVLW  h'01'

```

```

MOVWF   EEADR

```

```

BANKSEL EECON1
BCF     EECON1,EEPGD
BSF     EECON1, RD

```

```

BANKSEL EEDATA
MOVF    EEDATA,W

```

```

BANKSEL GECICI_KAYNAK_2
MOVWF   GECICI_KAYNAK_2

```

```

BANKSEL EEADR
MOVLW  h'02'

```

```

MOVWF   EEADR

```

```

BANKSEL EECON1
BCF     EECON1,EEPGD
BSF     EECON1, RD

```

```

BANKSEL EEDATA
MOVF    EEDATA,W

```

```

BANKSEL GECICI_KAYNAK_3

```

EK-B'NİN DEVAMI

```

MOVWF GECICI_KAYNAK_3

RETURN

SIFRE_YAZ
;EEPROMA 3 KAYNAK DEGERINI YAZAR

BANKSEL EEADR
MOVLW h'00'
MOVWF EEADR
BANKSEL KAYNAK1_1
MOVF KAYNAK1_1,W
BANKSEL EEDATA
MOVWF EEDATA

;YAZMA ISLEMI İÇİN GEREKLİ
;BAYRAK DÜZENLEMELERİ

BANKSEL PIR2
BCF PIR2, EEIF
BANKSEL EECON1
BCF EECON1,EEPGD
BSF EECON1,WREN
BCF INTCON,GIE

;YAZMA ISLEMI İÇİN ZORUNLU
;KULLANILMASI GEREKEN KODLAR

MOVLW h'55'
MOVWF EECON2
MOVLW h'AA'
MOVWF EECON2
BSF EECON1,WR
BANKSEL PIR2

DELAY0
BTFSS PIR2,EEIF
GOTO DELAY0
BCF PIR2,EEIF

;KAYNAK1_1 YAZILDI KAYNAK1_2 GEÇİYOR

BANKSEL EEADR
MOVLW h'01'
MOVWF EEADR
BANKSEL KAYNAK1_2
MOVF KAYNAK1_2,0
BANKSEL EEDATA
MOVWF EEDATA

;YAZMA ISLEMI İÇİN GEREKLİ
;BAYRAK DÜZENLEMELERİ

BANKSEL PIR2
BCF PIR2, EEIF
BANKSEL EECON1
BCF EECON1,EEPGD
BSF EECON1,WREN
BCF INTCON,GIE

;YAZMA ISLEMI İÇİN ZORUNLU
;KULLANILMASI GEREKEN KODLAR

MOVLW h'55'
MOVWF EECON2
MOVLW h'AA'
MOVWF EECON2
BSF EECON1,WR
BANKSEL PIR2

DELAY1
BTFSS PIR2,EEIF
GOTO DELAY1
BCF PIR2,EEIF

;KAYNAK1_2 YAZILDI KAYNAK1_3 GEÇİYOR

```

```

BANKSEL EEADR
MOVLW h'02'
MOVWF EEADR
BANKSEL KAYNAK1_3
MOVF KAYNAK1_3,0
BANKSEL EEDATA
MOVWF EEDATA

;YAZMA ISLEMI İÇİN GEREKLİ
;BAYRAK DÜZENLEMELERİ

BANKSEL PIR2
BCF PIR2, EEIF
BANKSEL EECON1
BCF EECON1,EEPGD
BSF EECON1,WREN
BCF INTCON,GIE

;YAZMA ISLEMI İÇİN ZORUNLU
;KULLANILMASI GEREKEN KODLAR

MOVLW h'55'
MOVWF EECON2
MOVLW h'AA'
MOVWF EECON2
BSF EECON1,WR
BANKSEL PIR2

DELAY2
BTFSS PIR2,EEIF
GOTO DELAY2

;YAZMA ISLEMI BITTI,
;TÜM BAYRAKLARI İLK KONUMUNA AL

BCF PIR2,EEIF
BANKSEL EECON1
BCF EECON1,WREN
BSF INTCON,GIE
BANKSEL KAYNAK1_3
RETURN

sifre_sifirla
BANKSEL EEADR
MOVLW h'00'
MOVWF EEADR
MOVLW h'00'
BANKSEL EEDATA
MOVWF EEDATA

;YAZMA ISLEMI İÇİN GEREKLİ
;BAYRAK DÜZENLEMELERİ

BANKSEL PIR2
BCF PIR2, EEIF
BANKSEL EECON1
BCF EECON1,EEPGD
BSF EECON1,WREN
BCF INTCON,GIE

;YAZMA ISLEMI İÇİN ZORUNLU
;KULLANILMASI GEREKEN KODLAR

MOVLW h'55'
MOVWF EECON2
MOVLW h'AA'
MOVWF EECON2
BSF EECON1,WR
BANKSEL PIR2

DELAY3
BTFSS PIR2,EEIF
GOTO DELAY3
BCF PIR2,EEIF

;KAYNAK1_1 YAZILDI KAYNAK1_2 GEÇİYOR

```

EK-B'NİN DEVAMI

```

BANKSEL EEADR
MOVLW  h'01'
MOVWF  EEADR

MOVLW  h'00'
BANKSEL EEDATA
MOVWF  EEDATA

;YAZMA ISLEMI İÇİN GEREKLİ
;BAYRAK DÜZENLEMELERİ

BANKSEL PIR2
BCF     PIR2, EEIF
BANKSEL EECON1
BCF     EECON1, EEPGD
BSF     EECON1, WREN
BCF     INTCON, GIE

;YAZMA ISLEMI İÇİN ZORUNLU
;KULLANILMASI GEREKEN KODLAR

MOVLW  h'55'
MOVWF  EECON2
MOVLW  h'AA'
MOVWF  EECON2
BSF     EECON1, WR
BANKSEL PIR2

DELAY4
BTFSS  PIR2, EEIF
GOTO   DELAY4
BCF     PIR2, EEIF

;KAYNAK1_2 YAZILDI KAYNAK1_3 GEÇİYOR

BANKSEL EEADR
MOVLW  h'02'
MOVWF  EEADR
MOVLW  h'00'
BANKSEL EEDATA
MOVWF  EEDATA

;YAZMA ISLEMI İÇİN GEREKLİ
;BAYRAK DÜZENLEMELERİ

BANKSEL PIR2
BCF     PIR2, EEIF
BANKSEL EECON1
BCF     EECON1, EEPGD
BSF     EECON1, WREN
BCF     INTCON, GIE

;YAZMA ISLEMI İÇİN ZORUNLU
;KULLANILMASI GEREKEN KODLAR

MOVLW  h'55'
MOVWF  EECON2
MOVLW  h'AA'
MOVWF  EECON2
BSF     EECON1, WR
BANKSEL PIR2

DELAY5
BTFSS  PIR2, EEIF
GOTO   DELAY5

;YAZMA ISLEMI BITTI,
;TÜM BAYRAKLARI ILK KONUMUNA AL

BCF     PIR2, EEIF
BANKSEL EECON1

```

```

BCF     EECON1, WREN
BSF     INTCON, GIE
BANKSEL KAYNAK1_3
RETURN

delayrout1
MOVLW  d'255'
MOVWF  delay2

looping2
MOVLW  d'255'
MOVWF  delay1

looping1
NOP
NOP
DECFSZ delay1,1
GOTO   looping1
DECFSZ delay2,1
GOTO   looping2
RETURN

delayrout11
MOVLW  d'40'
MOVWF  delay22

looping22
MOVLW  d'255'
MOVWF  delay11

looping11
NOP
NOP
DECFSZ delay11,1
GOTO   looping11
DECFSZ delay22,1
GOTO   looping22

RETURN

END
; 'program sonu'

```

EK-C: SENKRON İSTEMCİ PROGRAM KODLARI

```

;***** SENKRON İSTEMCİ *****
LIST    p=16F877A

#include <p16f877A.inc>
__CONFIG h'3F31'

        CBLOCK    0x20
            count1
            counta
            countb
            count
            Delay_Count
            Bit_Cntr
            Data_Byte
            Dev_Byte
            Rcv_Byte
            Pulse
            Dev_Byte1
            Data_Byte1
            irerror
            irtimer
            ircounter
            ircmd
            iradr
            ALICI_BEKLEME_1
            ALICI_BEKLEME_2
            ALICI_BEKLEME_3
            SIFRELER_ALINDI_MI
            irtemp1_1
            irtemp2_1
            irtemp3_1
            irtemp4_1
            irtemp
            irtemp1
            irtemp2
            irtemp3
            irtemp4
            ALINAN_SIFRE
            ORJINAL_SIFRE
            ANAHTAR
            ANAHTAR1
            ALINAN_SIFRE_A
            ALINAN_SIFRE_B
            ALINAN_SIFRE_C
            ALINAN_SIFRE_D
            ALINAN_SIFRE_K
            ALINAN_SIFRE_L
            delay1
            delay2
            delay11
            delay22
            GOSTERICI
            GOSTERICI_1
            GOSTERICI_2
            w_temp
            status_temp

        ENDC

IR_PORT Equ    PORTA
IR_Out  Equ    0x02
ir      Equ     0x03

ORG     0x000
GOTO    Start
ORG     0x004
GOTO    KESME_PROG

;***** KESME_PROG;*****
        MOVWF    w_temp
        MOVF     STATUS,w
        MOVWF    status_temp
        MOVF     status_temp,w
        MOVWF    STATUS
        SWAPF    w_temp,f
        SWAPF    w_temp,w
        RETFIE

;*****
Start
        CLRF     IR_PORT
        BCF      STATUS, RP1
        BSF      STATUS, RP0
        MOVLW    0X07
        MOVWF    CMCON

        MOVLW    h'06'
        MOVWF    ADCON1

        MOVLW    b'00001001'
        MOVWF    TRISA

        MOVLW    b'00000000'
        MOVWF    TRISC

        MOVLW    b'00000000'
        MOVWF    TRISD
        BCF      STATUS, RP0

        BANKSEL OPTION_REG
        MOVLW    b'10000101'
        MOVWF    OPTION_REG
        BANKSEL PORTA

        MOVLW    h'00'
        MOVWF    GOSTERICI
        CALL     goster
        CLRF     PORTA

Read_Sw
        MOVLW    h'00'
        MOVWF    GOSTERICI
        CALL     goster
        CLRF     SIFRELER_ALINDI_MI
        BSF      PORTA, 1

Read_Sw1
        BTFSC    PORTA, 0
        GOTO     Read_Sw1

        MOVLW    h'01'
        MOVWF    Dev_Byte1
        MOVLW    h'06'
        MOVWF    Data_Byte1

        CALL     Switch
        CALL     Switch
        CALL     Switch
        CALL     Switch
        CALL     Switch
        CALL     Switch
        CALL     Switch
        CALL     Switch
        CALL     Switch
        CALL     Switch

```

EK-C'NİN DEVAMI

```

MOVWL    h'02'
MOVWF    Dev_Bytel
MOVWL    h'01'
MOVWF    Data_Bytel

CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch

MOVWL    h'03'
MOVWF    Dev_Bytel
MOVWL    h'01'
MOVWF    Data_Bytel

CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch

MOVWL    h'04'
MOVWF    Dev_Bytel
MOVWL    h'09'
MOVWF    Data_Bytel

CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch
CALL     Switch

BCF      PORTA,1

;İLK ŞİFRE GONDERİLDİ
;ALICI BUNU DOĞRULARSA BİZE RANDOM
;BİR SAYIYI KRİPTO ALGORİTMASINDAN
;GEÇİREREK TEKRAR GONDERECEK BURADA
;BUNUN İÇİN ALICI MODA GEÇİYOR
;ANCAK VERİNİN GELMEMESİ DURUMUNDA
;TAKILMAMAK İÇİN BUNU BİR
;GECİKME ALGORİTMASI İLE YAPACAK.

MOVWL    h'04'
MOVWF    ALICI_BEKLEME_1

DONGU3
MOVWL    h'CF'
MOVWF    ALICI_BEKLEME_2

DONGU2
MOVWL    h'FF'
MOVWF    ALICI_BEKLEME_3

DONGU1
CALL     read_sony
BTFSC    irerror,0
GOTO     DONGU1_DEVAM

CALL     ir_to_outp
BCF      STATUS,Z
MOVF     SIFRELER_ALINDI_MI,W
BTFSS    STATUS,Z
GOTO     DEVAM

```

[illegible]

EK-C'NİN DEVAMI

```

CALL    Switch
CALL    Switch
CALL    Switch

MOVLW   h'04'
MOVWF   Dev_Bytel
MOVF     irtemp4_1,W
MOVWF   Data_Bytel

CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch

loop
    BTFSC  PORTA,0
    GOTO   Read_Sw
    GOTO   loop

;=====

ir_to_outp
    MOVF   ircmd,w
    MOVWF  irtemp
    BCF    STATUS,Z
    MOVF   iradr,w
    SUBLW  h'01'
    BTFSS  STATUS,Z
    GOTO   sifre_2
    MOVF   irtemp,w
    MOVWF  irtemp1
    BCF    STATUS,Z
    MOVF   irtemp1,w
    MOVWF  GOSTERICI
    CALL   goster
    RETURN

sifre_2
    BCF    STATUS,Z
    MOVF   iradr,w
    SUBLW  h'02'
    BTFSS  STATUS,Z
    GOTO   sifre_3
    MOVF   irtemp,w
    MOVWF  irtemp2
    BCF    STATUS,Z
    MOVF   irtemp2,w
    MOVWF  GOSTERICI
    CALL   goster
    RETURN

sifre_3
    BCF    STATUS,Z
    MOVF   iradr,w
    SUBLW  h'03'
    BTFSS  STATUS,Z
    GOTO   sifre_4
    MOVF   irtemp,w
    MOVWF  irtemp3
    BCF    STATUS,Z
    MOVF   irtemp3,w
    MOVWF  GOSTERICI
    CALL   goster
    RETURN

sifre_4
    BCF    STATUS,Z
    MOVF   iradr,w
    SUBLW  h'04'

    BTFSS  STATUS,Z
    RETURN

    MOVF   irtemp,w
    MOVWF  irtemp1
    CALL   ALINAN_SIFRE
    MOVF   irtemp1,w
    MOVWF  ORJINAL_SIFRE,W

    MOVF   irtemp2,w
    MOVWF  irtemp2_1
    CALL   ALINAN_SIFRE
    MOVF   irtemp2_1,w
    MOVWF  ORJINAL_SIFRE,W

    MOVF   irtemp3,w
    MOVWF  irtemp3_1
    CALL   ALINAN_SIFRE
    MOVF   irtemp3_1,w
    MOVWF  ORJINAL_SIFRE,W

    MOVF   irtemp4,w
    MOVWF  irtemp4_1
    CALL   ALINAN_SIFRE
    MOVF   irtemp4_1,w
    MOVWF  ORJINAL_SIFRE,W

    INCF   SIFRELER_ALINDI_MI
    RETURN

;=====

Switch
    MOVF   Dev_Bytel,w
    MOVWF  Dev_Byte
    MOVF   Data_Bytel,w
    MOVWF  Data_Byte

    CALL   Xmit_RS232
    CALL   Delay20
    RETLW  0x00

TX_Start
    MOVLW  d'184'
    CALL   IR_pulse
    MOVLW  d'23'
    CALL   NO_pulse
    RETLW  0x00

TX_One
    MOVLW  d'46'
    CALL   IR_pulse
    MOVLW  d'23'
    CALL   NO_pulse
    RETLW  0x00

TX_Zero
    MOVLW  d'23'
    CALL   IR_pulse
    MOVLW  d'23'
    CALL   NO_pulse
    RETLW  0x00

IR_pulse
    MOVWF  count

```

EK-C'NİN DEVAMI

```

irloop
    BSF      IR_PORT,IR_Out
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    BCF      IR_PORT,IR_Out
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    DECFSZ   count,F
    GOTO     irloop
    RETLW    0

```

```

NO_pulse
    MOVWF    count

```

```

irloop2
    BCF      IR_PORT,IR_Out
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    BCF      IR_PORT,IR_Out
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    DECFSZ   count,F
    GOTO     irloop2
    RETLW    0

```

```

Xmit_RS232
    MOVWF    Data_Byte
    MOVLW    0x08
    MOVWF    Bit_Cntr
    CALL     TX_Start

```

```

Ser_Loop
    RRF      Data_Byte,f
    BTFSC    STATUS,C
    CALL     TX_One
    BTFSS    STATUS,C
    CALL     TX_Zero
    DECFSZ   Bit_Cntr,f
    GOTO     Ser_Loop

    MOVLW    0x04
    MOVWF    Bit_Cntr

```

```

Ser_Loop2
    RRF      Dev_Byte,f
    BTFSC    STATUS,C
    CALL     TX_One
    BTFSS    STATUS,C
    CALL     TX_Zero
    DECFSZ   Bit_Cntr,f
    GOTO     Ser_Loop2
    RETLW    0x00
;=====

```

```

read_sony
    BSF      irerror,0

    BCF      INTCON,GIE
    CLRWDI
    BTFSC    PORTB,ir
    GOTO     end_sony
    CLRF     TMR0

```

```

sony_st1
    BTFSS    PORTA,ir
    GOTO     sony_st1
    MOVF     TMR0,0
    MOVWF    irtimer
    MOVLW    d'64'

    SUBWF    irtimer,0
    BTFSS    STATUS,C
    GOTO     end_sony

```

```

    MOVLW    d'170'
    ADDWF    irtimer,0

    BTFSC    STATUS,C
    GOTO     end_sony

    MOVLW    d'8'
    MOVWF    ircounter

```

```

rd_sony_cmd
    CLRF     TMR0

```

```

sony_prt1_c
    BTFSC    PORTA,ir

    GOTO     sony_prt1_c

    MOVF     TMR0,0
    MOVWF    irtimer

    MOVLW    d'5'
    SUBWF    irtimer,0
    BTFSS    STATUS,C
    GOTO     end_sony

    MOVLW    d'241'

```

```

    ADDWF    irtimer,0
    BTFSC    STATUS,C
    GOTO     end_sony
    CLRF     TMR0

    CLRWDI

```

```

sony_prt2_c
    BTFSS    PORTA,ir

    GOTO     sony_prt2_c
    MOVF     TMR0,0
    MOVWF    irtimer
    MOVLW    d'5'
    SUBWF    irtimer,0
    BTFSS    STATUS,C
    GOTO     end_sony

```

EK-C'NİN DEVAMI

```

        MOVLW    d'230'
        ADDWF    irtimer,0
        BTFSC    STATUS,C
        GOTO     end_sony
        MOVLW    d'241'

        ADDWF    irtimer,0
        BTFSC    STATUS,C
        GOTO     sony_its_1

sony_its_0
        BCF      STATUS,C
        RRF      ircmd,1
        GOTO     nxt_sony_cmd

sony_its_1
        BSF      STATUS,C
        RRF      ircmd,1

nxt_sony_cmd
        DECFSZ   ircounter,1
        GOTO     rd_sony_cmd
        BCF      STATUS,C

        MOVLW    d'4'
        MOVWF    ircounter

rd_sony_adr
        CLRF     TMR0

sony_prt1_a

        BTFSC    PORTA,ir

        GOTO     sony_prt1_a
        MOVF     TMR0,0
        MOVWF    irtimer
        MOVLW    d'5'
        SUBWF    irtimer,0
        BTFSS    STATUS,C
        GOTO     end_sony
        MOVLW    d'241'
        ADDWF    irtimer,0
        BTFSC    STATUS,C
        GOTO     end_sony
        CLRF     TMR0
        CLRWDI;

sony_prt2_a
        BTFSS    PORTA,ir;
        GOTO     sony_prt2_a
        MOVF     TMR0,0
        MOVWF    irtimer
        MOVLW    d'5'
        SUBWF    irtimer,0
        BTFSS    STATUS,C
        GOTO     end_sony
        MOVLW    d'230'
        ADDWF    irtimer,0
        BTFSC    STATUS,C
        GOTO     end_sony
        MOVLW    d'241'
        ADDWF    irtimer,0
        BTFSC    STATUS,C
        GOTO     sony_its_1_a

sony_its_0_a
        BCF      STATUS,C
        RRF      iradr,1
        GOTO     nxt_sony_adr

sony_its_1_a
        BSF      STATUS,C
        RRF      iradr,1

nxt_sony_adr

        DECFSZ   ircounter,1
        GOTO     rd_sony_adr

        BCF      STATUS,C

        MOVLW    h'04'
        MOVWF    ircounter

kaydır
        BCF      STATUS,C
        RRF      iradr,1
        DECFSZ   ircounter,1
        GOTO     kaydır
        BCF      STATUS,C

        CLRF     irerror

end_sony
        BCF      INTCON,TMR0IF

        BSF      STATUS,RP0
        MOVLW    b'10000101'
        MOVWF    OPTION_REG
        BCF      STATUS,RP0
        RETURN
;=====

goster
        MOVF     GOSTERICI,W
        ANDLW    h'0F'
        MOVWF    GOSTERICI_1

        MOVF     GOSTERICI,W
        ANDLW    h'F0'
        MOVWF    GOSTERICI

        MOVLW    h'04'
        MOVWF    ircounter

kaydır_1
        BCF      STATUS,C
        RRF      GOSTERICI,1
        DECFSZ   ircounter,1
        GOTO     kaydır_1
        BCF      STATUS,C

        MOVF     GOSTERICI,W
        MOVWF    GOSTERICI_2

        MOVF     GOSTERICI_1,W
        MOVWF    GOSTERICI
        CALL     DISPLAY
        MOVF     GOSTERICI,W
        MOVWF    PORTC

        MOVF     GOSTERICI_2,W
        MOVWF    GOSTERICI
        CALL     DISPLAY
        MOVF     GOSTERICI,W
        MOVWF    PORTD

        RETURN
;=====

SIFRE_COZ

        BCF      STATUS,C
        MOVLW    h'0B'

        MOVWF    ANAHTAR

        RLF      ANAHTAR,W
        MOVWF    ANAHTAR1
        MOVLW    h'F0'
        ANDWF    ALINAN_SIFRE,W
        MOVWF    ALINAN_SIFRE_B

```

EK-C'NİN DEVAMI

```

        MOVLW    h'04'
        MOVWF    Bit_Cntr
kaydır3
        BCF      STATUS,C
        RRF      ALINAN_SIFRE_B,1
        DECFSZ   Bit_Cntr,1
        GOTO     kaydır3
        BCF      STATUS,C

        MOVLW    h'0F'
        ANDWF    ALINAN_SIFRE,W
        MOVWF    ALINAN_SIFRE_D

        MOVF     ANAHTAR1,W
        XORWF    ALINAN_SIFRE_B,W
        MOVWF    ALINAN_SIFRE_C
        XORWF    ALINAN_SIFRE_D,W
        MOVWF    ALINAN_SIFRE_L
        XORWF    ANAHTAR,W
        MOVWF    ALINAN_SIFRE_A
        XORWF    ALINAN_SIFRE_B,W
        MOVWF    ALINAN_SIFRE_K

        MOVLW    h'04'
        MOVWF    Bit_Cntr
kaydır4
        BCF      STATUS,C
        RLF      ALINAN_SIFRE_K,1
        DECFSZ   Bit_Cntr,1
        GOTO     kaydır4
        BCF      STATUS,C

        MOVF     ALINAN_SIFRE_K,W
        XORWF    ALINAN_SIFRE_L,W
        MOVWF    ORJINAL_SIFRE

        RETURN
;=====
delayrout1
        MOVLW    d'255'
        MOVWF    delay2

looping2
        MOVLW    d'255'
        MOVWF    delay1

looping1
        NOP
        NOP
        DECFSZ   delay1,1
        GOTO     looping1
        DECFSZ   delay2,1
        GOTO     looping2

        RETURN
;=====

DISPLAY

        BCF      STATUS,Z

        MOVF     GOSTERICI,W

        BTFSS    STATUS,Z
        GOTO     DISPLAY_1
        MOVLW    h'3F'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN

DISPLAY_1
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'01'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_2
        MOVLW    h'06'
        MOVWF    GOSTERICI

```

```

        BCF      STATUS,Z
        RETURN

DISPLAY_2
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'02'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_3
        MOVLW    h'5B'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN

DISPLAY_3
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'03'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_4
        MOVLW    h'4F'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN

DISPLAY_4
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'04'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_5
        MOVLW    h'66'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN

DISPLAY_5
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'05'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_6
        MOVLW    h'6D'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN

DISPLAY_6
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'06'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_7
        MOVLW    h'7D'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN

DISPLAY_7
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'07'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_8
        MOVLW    h'07'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN

DISPLAY_8
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'08'
        BTFSS    STATUS,Z
        GOTO     DISPLAY_9
        MOVLW    h'7F'
        MOVWF    GOSTERICI
        BCF      STATUS,Z
        RETURN

DISPLAY_9
        BCF      STATUS,Z
        MOVF     GOSTERICI,W
        SUBLW    h'09'

```

EK-C'NİN DEVAMI

```

    BTFSS    STATUS,Z
    GOTO     DISPLAY_10
    MOVLW    h'6F'
    MOVWF    GOSTERICI
    BCF      STATUS,Z
    RETURN

DISPLAY_10
    BCF      STATUS,Z
    MOVF     GOSTERICI,W
    SUBLW    h'0A'
    BTFSS    STATUS,Z
    GOTO     DISPLAY_11
    MOVLW    h'77'
    MOVWF    GOSTERICI
    BCF      STATUS,Z
    RETURN

DISPLAY_11
    BCF      STATUS,Z
    MOVF     GOSTERICI,W
    SUBLW    h'0B'
    BTFSS    STATUS,Z
    GOTO     DISPLAY_12
    MOVLW    h'7C'
    MOVWF    GOSTERICI
    BCF      STATUS,Z
    RETURN

DISPLAY_12
    BCF      STATUS,Z
    MOVF     GOSTERICI,W
    SUBLW    h'0C'
    BTFSS    STATUS,Z
    GOTO     DISPLAY_13
    MOVLW    h'39'
    MOVWF    GOSTERICI
    BCF      STATUS,Z
    RETURN

DISPLAY_13
    BCF      STATUS,Z
    MOVF     GOSTERICI,W
    SUBLW    h'0D'
    BTFSS    STATUS,Z
    GOTO     DISPLAY_14
    MOVLW    h'5E'
    MOVWF    GOSTERICI
    BCF      STATUS,Z
    RETURN

DISPLAY_14
    BCF      STATUS,Z
    MOVF     GOSTERICI,W
    SUBLW    h'0E'
    BTFSS    STATUS,Z
    GOTO     DISPLAY_15
    MOVLW    h'79'
    MOVWF    GOSTERICI
    BCF      STATUS,Z
    RETURN

DISPLAY_15
    BCF      STATUS,Z
    MOVF     GOSTERICI,W
    SUBLW    h'0F'
    BTFSS    STATUS,Z
    RETURN
    MOVLW    h'71'
    MOVWF    GOSTERICI
    BCF      STATUS,Z
    RETURN
;=====

delayrout11
    MOVLW    d'40'
    MOVWF    delay22

looping22
    MOVLW    d'255'
    MOVWF    delay11

looping11
    NOP
    NOP
    DECFSZ   delay11,1
    GOTO     looping11
    DECFSZ   delay22,1
    GOTO     looping22

    RETURN
;=====
;Gecikmeler

Delay255    MOVLW    0xff
            GOTO     d0
Delay100    MOVLW    d'100'
            GOTO     d0
Delay50     MOVLW    d'50'
            GOTO     d0
Delay27     MOVLW    d'27'
            GOTO     d0
Delay20     MOVLW    d'20'
            GOTO     d0
Delay5      MOVLW    0x05
d0          MOVWF    count1
d1          MOVLW    0xC7
            MOVWF    counta
            MOVLW    0x01
            MOVWF    countb
Delay_0     DECFSZ   counta,f
            GOTO     $+2
            DECFSZ   countb,f
            GOTO     Delay_0
            DECFSZ   count1,f
            GOTO     d1
            RETLW    0x00

            END

; 'program sonu'

```

EK-D: SENKRON SUNUCU PROGRAM KODLARI

```

;***** SENKRON SUNUCU *****

list      p=16f877A
#include <p16f877A.inc>

__CONFIG h'3F31'

w_temp          EQU    0x30

status_temp     EQU    0x31

irerror         EQU    0x32

irtimer         EQU    0x33

ircounter       EQU    0x34

ircmd           EQU    0x35

iradr           EQU    0x36

irtemp         EQU    0x37

delay1          EQU    0x38
delay2          EQU    0x39
irtemp1         EQU    0x3A
irtemp2         EQU    0x3B
irtemp3         EQU    0x3C
irtemp4         EQU    0x3D
irtemp5         EQU    0x3E
irtemp6         EQU    0x3F
irtemp7         EQU    0x40
irtemp8         EQU    0x41
delay22         EQU    0x42
delay11         EQU    0x43
rastgele1       EQU    0x44
rastgele2       EQU    0x45
rastgele3       EQU    0x46
rastgele4       EQU    0x47
DEGISTIRICI     EQU    0x48
DEGISTIRICI1    EQU    0x49
DEGISTIRICI2    EQU    0x4A
DEGISTIRICI3    EQU    0x4B
SIFRE1          EQU    0x4C
SIFRE2          EQU    0x4D
SIFRE3          EQU    0x4E
SIFRE4          EQU    0x4F
Dev_Byte1       EQU    0x50
Data_Byte1      EQU    0x51
KAYNAK1         EQU    0x52
KAYNAK2         EQU    0x53
KAYNAK3         EQU    0x54
KAYNAK4         EQU    0x55
Dev_Byte        EQU    0x56
Data_Byte       EQU    0x57
KRIPTO_KAYNAK   EQU    0x58
KRIPTOLANMIS_KAYNAK EQU    0x59
KRIPTO_KAYNAK_A EQU    0x5A
KRIPTO_KAYNAK_B EQU    0x5B
KRIPTO_KAYNAK_C EQU    0x5C
KRIPTO_KAYNAK_D EQU    0x5D
KRIPTO_KAYNAK_UST EQU    0x5E
KRIPTO_KAYNAK_ALT EQU    0x5F
Bit_Cntr        EQU    0x60
count           EQU    0x61
count1          EQU    0x62
counta          EQU    0x63

countb          EQU    0x64
ANAHTAR         EQU    0x65
BEKLEME_1       EQU    0x66
BEKLEME_2       EQU    0x67
BEKLEME_3       EQU    0x68
SIFRELER_ALINDI_MI EQU    0x69
SIFRELER_GONDERILDI_MI EQU    0x6A
irtemp_1        EQU    0x6B
GOSTERICI       EQU    0x6C
GOSTERICI_1     EQU    0x6D
GOSTERICI_2     EQU    0x6E

led             EQU    0x01
ir              EQU    0x07
IR_PORT EQU     PORTB
IR_Out EQU      0x06

;*****

ORG    0x000
GOTO  init

ORG    0x004
GOTO  KESME_PROG

KESME_PROG      ;=====

MOVWF w_temp
MOVF  STATUS,w
MOVWF status_temp
MOVF  status_temp,w
MOVWF STATUS
SWAPF w_temp,f
SWAPF w_temp,w
RETFIE

;=====

init
BSF   PORTB,led

CLRF  irtemp
CLRF  irtemp_1
CLRF  irtemp1
CLRF  irtemp2
CLRF  irtemp3
CLRF  irtemp4
CLRF  irtemp5
CLRF  irtemp6
CLRF  irtemp7
CLRF  irtemp8
CALL  delayrout1
CALL  delayrout1
CALL  delayrout1
CLRF  ircmd
CLRF  iradr

BCF   STATUS,RP1
BSF   STATUS,RP0

MOVLW 0x07
MOVWF CMCON

MOVLW h'06'
MOVWF ADCON1

```

EK-D'NİN DEVAMI

MOVLW	b'10000000'	BTFSS	STATUS,Z
MOVWF	TRISB	GOTO	DIGER2
MOVLW	b'00000000'	RRF	rastgele3,F
MOVWF	TRISC	MOVLW	h'03'
MOVLW	b'00000000'	MOVWF	DEGISTIRICI2
MOVWF	TRISD	GOTO	DEVAM2
MOVLW	b'10000101'	DIGER2	
MOVWF	OPTION_REG	RLF	rastgele3,F
BCF	STATUS,RP0	DECF	DEGISTIRICI2
		BCF	STATUS,C
CLRF	SIFRELER_ALINDI_MI	DEVAM2	
CLRF	SIFRELER_GONDERILDI_MI	DECF	rastgele4,F
MOVLW	h'00'	RLF	rastgele4,F
MOVWF	GOSTERICI	BCF	STATUS,Z
CALL	goster	MOVF	DEGISTIRICI3,W
		BTFSS	STATUS,Z
MOVLW	h'81'	GOTO	DIGER3
MOVWF	rastgele1	INCF	rastgele4,F
MOVLW	h'16'	MOVLW	h'03'
MOVWF	rastgele2	MOVWF	DEGISTIRICI3
MOVLW	h'8C'	GOTO	DEVAM3
MOVWF	rastgele3	DIGER3	
MOVLW	h'1A'	DECF	rastgele4,F
MOVWF	rastgele4	DECF	DEGISTIRICI3
		BCF	STATUS,C
test		DEVAM3	
BCF	STATUS,Z	BSF	PORTB,1
MOVF	SIFRELER_GONDERILDI_MI,W	CALL	read_sony
BTFSS	STATUS,Z	BTFSC	irerror,0
GOTO	SIFRE_KONTROL	GOTO	test
BCF	STATUS,C	CALL	ir_to_outp
INCF	rastgele1,F	CALL	delayrout1
BCF	STATUS,Z	GOTO	test
MOVF	DEGISTIRICI,W	SIFRE_KONTROL	
BTFSS	STATUS,Z	BCF	STATUS,Z
GOTO	DIGER	MOVLW	h'02'
NOP		MOVWF	BEKLEME_1
MOVLW	h'04'	DONGU3	
MOVWF	DEGISTIRICI	MOVLW	h'FF'
GOTO	DEVAM	MOVWF	BEKLEME_2
DIGER		DONGU2	
RLF	rastgele1,F	MOVLW	h'FF'
DECF	DEGISTIRICI,F	MOVWF	BEKLEME_3
DEVAM		DONGU1	
DECF	rastgele2,F	CALL	read_sony
BCF	STATUS,Z	BTFSC	irerror,0
MOVF	DEGISTIRICI1,W	GOTO	DONGU1_DEVAM
BTFSS	STATUS,Z	CALL	ir_output_1
GOTO	DIGER1	BCF	STATUS,Z
RRF	rastgele2,F	MOVF	SIFRELER_ALINDI_MI,W
MOVLW	h'03'	BTFSS	STATUS,Z
MOVWF	DEGISTIRICI1	GOTO	DEVAM4
GOTO	DEVAM1	GOTO	DONGU1_DEVAM
DIGER1		DONGU1_DEVAM	
NOP		DECFSZ	BEKLEME_3
DECF	DEGISTIRICI1,F	GOTO	DONGU1
DEVAM1		DECFSZ	BEKLEME_2
INCF	rastgele3,F	GOTO	DONGU2
INCF	rastgele3,F	DECFSZ	BEKLEME_1
BCF	STATUS,Z	GOTO	DONGU3
MOVF	DEGISTIRICI2,W	MOVLW	h'00'
		MOVWF	GOSTERICI

EK-D'NİN DEVAMI

```

CALL    goster
CLRF    SIFRELER_GONDERILDI_MI
CLRF    SIFRELER_ALINDI_MI
GOTO    test

DEVAM4
MOVLW   h'00'
MOVWF   GOSTERICI
CALL    goster

CLRF    SIFRELER_GONDERILDI_MI
CLRF    SIFRELER_ALINDI_MI
GOTO    test

ir_to_outp
MOVF    ircmd,w
MOVWF   irtemp
BCF     STATUS,Z
MOVF    iradr,w
SUBLW   h'01'
BTFSS   STATUS,Z
GOTO    sifre_2
MOVF    irtemp,w
MOVWF   irtemp1
BCF     STATUS,Z
MOVF    irtemp1,w
MOVWF   GOSTERICI
CALL    goster
RETURN

sifre_2
BCF     STATUS,Z
MOVF    iradr,w
SUBLW   h'02'
BTFSS   STATUS,Z
GOTO    sifre_3
MOVF    irtemp,w
MOVWF   irtemp2
BCF     STATUS,Z
MOVF    irtemp2,w
MOVWF   GOSTERICI
CALL    goster
RETURN

sifre_3
BCF     STATUS,Z
MOVF    iradr,w
SUBLW   h'03'
BTFSS   STATUS,Z
GOTO    sifre_4
MOVF    irtemp,w
MOVWF   irtemp3
BCF     STATUS,Z
MOVF    irtemp3,w
MOVWF   GOSTERICI
CALL    goster
RETURN

sifre_4
BCF     STATUS,Z
MOVF    iradr,w
SUBLW   h'04'
BTFSS   STATUS,Z
RETURN
MOVF    irtemp,w
MOVWF   irtemp4
BCF     STATUS,Z
MOVF    irtemp4,w
MOVWF   GOSTERICI
CALL    goster

;BU KISIMA GELDİĞİNDE İLK SABİT ŞİFRE
;SAĞLIKLI BİR ŞEKİLDE ALINMIŞ OLDUĞUNU
;GORDU ŞİMDİ BUNUN DOĞRU OLUP
;OLMADIĞINA BAKACAK

BCF     STATUS,Z
MOVF    irtemp1,w
XORLW   h'06'
BTFSS   STATUS,Z
GOTO    YANLIS_SIFRE

BCF     STATUS,Z
MOVF    irtemp2,w
XORLW   h'01'
BTFSS   STATUS,Z
GOTO    YANLIS_SIFRE

BCF     STATUS,Z
MOVF    irtemp3,w
XORLW   h'01'
BTFSS   STATUS,Z
GOTO    YANLIS_SIFRE
BCF     STATUS,Z
MOVF    irtemp4,w
XORLW   h'09'
BTFSS   STATUS,Z
GOTO    YANLIS_SIFRE
BCF     STATUS,Z

;BUNDAN SONRA rastgele URETTİĞİ
;ŞİFRELERİ KARŞIYA KRİPTO
;ALGORİTMASINDAN GEÇİREREK GONDERECEK.

CLRF    irtemp1
CLRF    irtemp2
CLRF    irtemp3
CLRF    irtemp4

MOVF    rastgele1,W
MOVWF   SIFRE1
MOVF    rastgele2,W
MOVWF   SIFRE2
MOVF    rastgele3,W
MOVWF   SIFRE3
MOVF    rastgele4,W
MOVWF   SIFRE4

MOVF    SIFRE1,W
MOVWF   KRİPTO_KAYNAK

CALL    Sifrele

MOVF    KRİPTOLANMIS_KAYNAK,W
MOVWF   KAYNAK1

MOVF    SIFRE2,W
MOVWF   KRİPTO_KAYNAK
CALL    Sifrele
MOVF    KRİPTOLANMIS_KAYNAK,W
MOVWF   KAYNAK2

MOVF    SIFRE3,W
MOVWF   KRİPTO_KAYNAK
CALL    Sifrele
MOVF    KRİPTOLANMIS_KAYNAK,W
MOVWF   KAYNAK3

MOVF    SIFRE4,W
MOVWF   KRİPTO_KAYNAK
CALL    Sifrele
MOVF    KRİPTOLANMIS_KAYNAK,W
MOVWF   KAYNAK4

BCF     PORTB,1
MOVLW   h'01'
MOVWF   Dev_Bytel
MOVF    KAYNAK1,W
MOVWF   Data_Bytel

CALL    Switch
CALL    Switch

```

EK-D'NİN DEVAMI

```

CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch

BSF      PORTB,1
MOVLW   h'02'
MOVWF   Dev_Bytel
MOVF    KAYNAK2,W
MOVWF   Data_Bytel

CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch

BCF      PORTB,1

MOVLW   h'03'
MOVWF   Dev_Bytel
MOVF    KAYNAK3,W
MOVWF   Data_Bytel

CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch

BSF      PORTB,1

MOVLW   h'04'
MOVWF   Dev_Bytel
MOVF    KAYNAK4,W
MOVWF   Data_Bytel

CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch
CALL    Switch

BCF      PORTB,1
INCF    SIFRELER_GONDERILDI_MI
RETURN

;=====

ir_output_1
MOVF    ircmd,w
MOVWF   irtemp_1
BCF     STATUS,Z
MOVF    iradr,w
SUBLW   h'01'

BTFSS   STATUS,Z
GOTO    sifre_6

sifre_6
BCF     STATUS,Z
MOVF    iradr,w
SUBLW   h'02'
BTFSS   STATUS,Z
GOTO    sifre_7
MOVF    irtemp_1,w
MOVWF   irtemp_6
BCF     STATUS,Z
MOVF    irtemp_6,w
MOVWF   GOSTERICI
CALL    goster
RETURN

sifre_7
BCF     STATUS,Z
MOVF    iradr,w
SUBLW   h'03'
BTFSS   STATUS,Z
GOTO    sifre_8
MOVF    irtemp_1,w
MOVWF   irtemp_7
BCF     STATUS,Z
MOVF    irtemp_7,w
MOVWF   GOSTERICI
CALL    goster
RETURN

sifre_8
BCF     STATUS,Z
MOVF    iradr,w
SUBLW   h'04'
BTFSS   STATUS,Z
RETURN
MOVF    irtemp_1,w
MOVWF   irtemp_8
BCF     STATUS,Z
MOVF    irtemp_8,w
Movwf   GOSTERICI
CALL    goster

BCF     STATUS,Z

MOVF    SIFRE1,W

SUBWF   irtemp_5,W
BTFSS   STATUS,Z
GOTO    YANLIŞ_SIFRE

BCF     STATUS,Z
MOVF    SIFRE2,W
SUBWF   irtemp_6,W
BTFSS   STATUS,Z
GOTO    YANLIŞ_SIFRE

BCF     STATUS,Z
MOVF    SIFRE3,W
SUBWF   irtemp_7,W
BTFSS   STATUS,Z
GOTO    YANLIŞ_SIFRE

BCF     STATUS,Z
MOVF    SIFRE4,W
SUBWF   irtemp_8,W
BTFSS   STATUS,Z
GOTO    YANLIŞ_SIFRE

```

EK-D'NİN DEVAMI

```
;ŞİFRE DOĞRULANDI

        BCF      STATUS,Z
        BSF      PORTB,0
        BSF      PORTB,led

;1-2 SANİYE KADAR SİSTEM AÇIK
;İKAZINI VERİP TEKRAR SİSTEMİ
;KAPATARAK TÜM GEÇİCİ VERİLERİ SİLSİN!
```

```
BSF      PORTB,2  
CALL     delayrout11  
BCF      PORTB,2  
CALL     delayrout11  
BSF      PORTB,2  
CALL     delayrout11  
BCF      PORTB,2  
CALL     delayrout11  
BSF      PORTB,2  
CALL     delayrout11  
BSF      PORTB,2  
CALL     delayrout1  
CALL     delayrout1  
  
BCF      PORTB,2  
CALL     delayrout11  
BSF      PORTB,2  
CALL     delayrout11  
BCF      PORTB,2  
CALL     delayrout11  
BSF      PORTB,2  
CALL     delayrout11  
BCF      PORTB,2  
CALL     delayrout11  
BSF      PORTB,2  
CALL     delayrout11  
BCF      PORTB,2  
CALL     delayrout11  
BSF      PORTB,2  
CALL     delayrout11  
BCF      PORTB,2  
CALL     delayrout11  
BSF      PORTB,2  
CALL     delayrout11  
BCF      PORTB,2  
CALL     delayrout11  
  
BCF      STATUS,Z  
BCF      PORTB,0  
BCF      PORTB,2  
BCF      PORTB,led  
CLRF     irtemp1  
CLRF     irtemp2  
CLRF     irtemp3  
CLRF     irtemp4  
CLRF     irtemp5  
CLRF     irtemp6  
CLRF     irtemp7  
CLRF     irtemp8  
  
MOVLW    h'00'  
MOVWF    GOSTERICI  
CALL     goster  
  
INCF     SIFRELER_ALINDI_MI  
RETURN
```

```
goster
    MOVF    GOSTERICI,W
    ANDLW   h'0F'
    MOVWF   GOSTERICI_1

    MOVF    GOSTERICI,W
    ANDLW   h'F0'
```

```
MOVWF    GOSTERICI
MOVLW    h'04'
MOVWF    ircounter
```

```

kaydır_1
BCF      STATUS,C
RRF      GOSTERICI,1
DECFSZ   ircounter,1
GOTO     kaydır_1
BCF      STATUS,C

MOVF     GOSTERICI,W
MOVWFF   GOSTERICI_2
MOVF     GOSTERICI_1,W
MOVWFF   GOSTERICI
CALL     DISPLAY
MOVF     GOSTERICI,W
MOVWFF   PORTC

MOVF     GOSTERICI_2,W
MOVWFF   GOSTERICI
CALL     DISPLAY
MOVF     GOSTERICI,W
MOVWFF   PORTD

RETURN

```

```

YANLIS_SIFRE
    CLRF    irtemp1
    CLRF    irtemp2
    CLRF    irtemp3
    CLRF    irtemp4
    CLRF    irtemp5
    CLRF    irtemp6
    CLRF    irtemp7
    CLRF    irtemp8
    MOVLW   h'00'
    MOVWF   GOSTERICI
    CALL    goster
    BCF     PORTB,0
    BSF     PORTB,1
    RETURN

```

```
Sifrele      BCF      STATUS,C
              MOVLW    h'F0'
              ANDWF    KRIPTO_KAYNAK,0
              MOVWF    KRIPTO_KAYNAK_UST
              MOVLW    h'04'
              MOVWF    ircounter
```

```

kaydırıl
BCF      STATUS,C
RRF      KRIPTO_KAYNAK_UST,1
DECFSZ   icounter,1
GOTO     kaydırıl
BCF      STATUS,C
MOVWF    KRIPTO_KAYNAK_UST,w

MOVWLW   h'0F'
ANDWF    KRIPTO_KAYNAK,W
MOVWF    KRIPTO_KAYNAK_ALT

MOVWLW   h'0B'
MOVWF    ANAHTAR
MOVF     ANAHTAR,W
XORWF    KRIPTO_KAYNAK_ALT,W
MOVWF    KRIPTO_KAYNAK_A

MOVF     KRIPTO_KAYNAK_A,W
XORWF    KRIPTO_KAYNAK_UST,W
MOVWF    KRIPTO_KAYNAK_B

RLF      ANAHTAR,W
XORWF    KRIPTO_KAYNAK_B,W
MOVWF    KRIPTO_KAYNAK_C

```

EK-D'NİN DEVAMI

```

XORWF   KRIPTO_KAYNAK_ALT,W
MOVWF   KRIPTO_KAYNAK_D

MOVLW   h'04'
MOVWF   ircounter

```

kaydır2

```

BCF      STATUS,C
RLF      KRIPTO_KAYNAK_B,1
DECFSZ   ircounter,1
GOTO     kaydır2
BCF      STATUS,C
MOVF     KRIPTO_KAYNAK_B,W

XORWF    KRIPTO_KAYNAK_D,W
MOVWF    KRIPTOLANMIS_KAYNAK

BCF      STATUS,C
RETLW    0x00

```

read_sony

```

BSF      irerror,0
BCF      INTCON,GIE
CLRWDI
BTFSC    PORTB,ir
GOTO     end_sony
CLRF     TMR0

```

sony_st1

```

BTFSS    PORTB,ir
GOTO     sony_st1
MOVF     TMR0,0
MOVWF    irtimer
MOVLW    d'64'
SUBWF    irtimer,0
BTFSS    STATUS,C
GOTO     end_sony

MOVLW    d'170'
ADDWF    irtimer,0
BTFSC    STATUS,C
GOTO     end_sony

MOVLW    0x08
MOVWF    ircounter

```

rd_sony_cmd

```

CLRF     TMR0

```

sony_prt1_c

```

BTFSC    PORTB,ir
GOTO     sony_prt1_c

MOVF     TMR0,0
MOVWF    irtimer

MOVLW    d'5'
SUBWF    irtimer,0
BTFSS    STATUS,C
GOTO     end_sony

MOVLW    d'241'

ADDWF    irtimer,0
BTFSC    STATUS,C
GOTO     end_sony
CLRF     TMR0

CLRWDI

```

sony_prt2_c

```

BTFSS    PORTB,ir

GOTO     sony_prt2_c
MOVF     TMR0,0

```

```

MOVWF    irtimer
MOVLW    d'5'
SUBWF    irtimer,0
BTFSS    STATUS,C
GOTO     end_sony
MOVLW    d'230'

```

```

ADDWF    irtimer,0
BTFSC    STATUS,C
GOTO     end_sony
MOVLW    d'241'
ADDWF    irtimer,0
BTFSC    STATUS,C
GOTO     sony_its_1

```

sony_its_0

```

BCF      STATUS,C
RRF      ircmd,1
GOTO     nxt_sony_cmd

```

sony_its_1

```

BSF      STATUS,C
RRF      ircmd,1

```

nxt_sony_cmd

```

DECFSZ   ircounter,1
GOTO     rd_sony_cmd
BCF      STATUS,C
MOVLW    0x04
MOVWF    ircounter

```

rd_sony_adr

```

CLRF     TMR0

```

sony_prt1_a

```

BTFSC    PORTB,ir
GOTO     sony_prt1_a
MOVF     TMR0,0
MOVWF    irtimer
MOVLW    d'5'
SUBWF    irtimer,0
BTFSS    STATUS,C
GOTO     end_sony
MOVLW    d'241'
ADDWF    irtimer,0
BTFSC    STATUS,C
GOTO     end_sony
CLRF     TMR0
CLRWDI;

```

sony_prt2_a

```

BTFSS    PORTB,ir;
GOTO     sony_prt2_a
MOVF     TMR0,0
MOVWF    irtimer
MOVLW    d'5'
SUBWF    irtimer,0
BTFSS    STATUS,C
GOTO     end_sony
MOVLW    d'230'
ADDWF    irtimer,0
BTFSC    STATUS,C
GOTO     end_sony
MOVLW    d'241'
ADDWF    irtimer,0
BTFSC    STATUS,C
GOTO     sony_its_1_a

```

sony_its_0_a

```

BCF      STATUS,C
RRF      iradr,1
GOTO     nxt_sony_adr

```

sony_its_1_a

```

BSF      STATUS,C
RRF      iradr,1

```

EK-D'NİN DEVAMI

```

nxt_sony_adr
    DECFSZ   ircounter,1
    GOTO     rd_sony_adr
    BCF      STATUS,C
    MOVLW    0x04
    MOVWF    ircounter

kaydır
    BCF      STATUS,C
    RRF      iradr,1
    DECFSZ   ircounter,1
    GOTO     kaydır
    BCF      STATUS,C
    CLRF     irerror

end_sony
    BCF      INTCON,TMR0IF
    BSF      STATUS,RP0
    MOVLW    b'10000101'
    MOVWF    OPTION_REG
    BCF      STATUS,RP0
    RETURN

Switch
    MOVF     Dev_Byte1,w
    MOVWF    Dev_Byte
    MOVF     Data_Byte1,w
    MOVWF    Data_Byte
    CALL     Xmit_RS232
    CALL     Delay20
    RETLW    0x00

TX_Start
    MOVLW    d'184'
    CALL     IR_pulse
    MOVLW    d'23'
    CALL     NO_pulse
    RETLW    0x00

TX_One
    MOVLW    d'46'
    CALL     IR_pulse
    MOVLW    d'23'
    CALL     NO_pulse
    RETLW    0x00

TX_Zero
    MOVLW    d'23'
    CALL     IR_pulse
    MOVLW    d'23'
    CALL     NO_pulse
    RETLW    0x00

IR_pulse
    MOVWF    count

irloop
    BSF      IR_PORT,IR_Out
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    BCF      IR_PORT,IR_Out
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP

NO_pulse
    MOVWF    count

irloop2
    BCF      IR_PORT,IR_Out
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    BCF      IR_PORT,IR_Out
    NOP
    NOP
    NOP
    NOP
    NOP
    NOP
    DECFSZ   count,F
    GOTO     irloop2
    RETLW    0

Xmit_RS232
    MOVWF    Data_Byte
    MOVLW    0x08
    MOVWF    Bit_Cntr
    CALL     TX_Start

Ser_Loop
    RRF      Data_Byte,f
    BTFSC    STATUS,C
    CALL     TX_One
    BTFSS    STATUS,C
    CALL     TX_Zero
    DECFSZ   Bit_Cntr,f
    GOTO     Ser_Loop
    MOVLW    0x04
    MOVWF    Bit_Cntr

Ser_Loop2
    RRF      Dev_Byte,f
    BTFSC    STATUS,C
    CALL     TX_One
    BTFSS    STATUS,C
    CALL     TX_Zero
    DECFSZ   Bit_Cntr,f
    GOTO     Ser_Loop2
    RETLW    0x00

DISPLAY
    BCF      STATUS,Z
    MOVF     GOSTERICI,W
    BTFSS    STATUS,Z
    GOTO     DISPLAY_1
    MOVLW    h'3F'
    MOVWF    GOSTERICI
    BCF      STATUS,Z
    RETURN

```

EK-D'NİN DEVAMI

```

DISPLAY_1      BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'01'
                BTFSS    STATUS,Z
                GOTO     DISPLAY_2
                MOVLW    h'06'
                MOVWF     GOSTERICI
                BCF      STATUS,Z
                RETURN

DISPLAY_2      BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'02'
                BTFSS    STATUS,Z
                GOTO     DISPLAY_3
                MOVLW    h'5B'
                MOVWF     GOSTERICI
                BCF      STATUS,Z
                RETURN

DISPLAY_3      BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'03'
                BTFSS    STATUS,Z
                GOTO     DISPLAY_4
                MOVLW    h'4F'
                MOVWF     GOSTERICI
                BCF      STATUS,Z
                RETURN

DISPLAY_4      BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'04'
                BTFSS    STATUS,Z
                GOTO     DISPLAY_5
                MOVLW    h'66'
                MOVWF     GOSTERICI
                BCF      STATUS,Z
                RETURN

DISPLAY_5      BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'05'
                BTFSS    STATUS,Z
                GOTO     DISPLAY_6
                MOVLW    h'6D'
                MOVWF     GOSTERICI
                BCF      STATUS,Z
                RETURN

DISPLAY_6      BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'06'
                BTFSS    STATUS,Z
                GOTO     DISPLAY_7
                MOVLW    h'7D'
                MOVWF     GOSTERICI
                BCF      STATUS,Z
                RETURN

DISPLAY_7      BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'07'
                BTFSS    STATUS,Z
                GOTO     DISPLAY_8
                MOVLW    h'07'
                MOVWF     GOSTERICI
                BCF      STATUS,Z
                RETURN

DISPLAY_8      BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'08'
                BTFSS    STATUS,Z

GOTO          DISPLAY_9
MOVLW         h'7F'
MOVWF         GOSTERICI
BCF          STATUS,Z
RETURN

DISPLAY_9      BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'09'
                BTFSS    STATUS,Z
                GOTO     DISPLAY_10
                MOVLW    h'6F'
                MOVWF     GOSTERICI
                BCF      STATUS,Z
                RETURN

DISPLAY_10     BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'0A'
                BTFSS    STATUS,Z
                GOTO     DISPLAY_11
                MOVLW    h'77'
                MOVWF     GOSTERICI
                BCF      STATUS,Z
                RETURN

DISPLAY_11     BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'0B'
                BTFSS    STATUS,Z
                GOTO     DISPLAY_12
                MOVLW    h'7C'
                MOVWF     GOSTERICI
                BCF      STATUS,Z
                RETURN

DISPLAY_12     BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'0C'
                BTFSS    STATUS,Z
                GOTO     DISPLAY_13
                MOVLW    h'39'
                MOVWF     GOSTERICI
                BCF      STATUS,Z
                RETURN

DISPLAY_13     BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'0D'
                BTFSS    STATUS,Z
                GOTO     DISPLAY_14
                MOVLW    h'5E'
                MOVWF     GOSTERICI
                BCF      STATUS,Z
                RETURN

DISPLAY_14     BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'0E'
                BTFSS    STATUS,Z
                GOTO     DISPLAY_15
                MOVLW    h'79'
                MOVWF     GOSTERICI
                BCF      STATUS,Z
                RETURN

DISPLAY_15     BCF      STATUS,Z
                MOVF     GOSTERICI,W
                SUBLW    h'0F'
                BTFSS    STATUS,Z
                RETURN
                MOVLW    h'71'
                MOVWF     GOSTERICI
                BCF      STATUS,Z
                RETURN
;=====

```

```

delayrout1      MOVLW    d'255'
                  MOVWF    delay2

looping2        MOVLW    d'255'
                  MOVWF    delay1

looping1        NOP
                  NOP
                  DECFSZ   delay1,1
                  GOTO     looping1
                  DECFSZ   delay2,1
                  GOTO     looping2
                  RETURN

delayrout11     MOVLW    d'40'
                  MOVWF    delay22

looping22       MOVLW    d'255'
                  MOVWF    delay11

looping11       NOP
                  NOP
                  DECFSZ   delay11,1
                  GOTO     looping11
                  DECFSZ   delay22,1
                  GOTO     looping22
                  RETURN

;=====
;Gecikmeler

Delay255        MOVLW    0xff
                  GOTO     d0
Delay100        MOVLW    d'100'
                  GOTO     d0
Delay50 MOVLW    d'50'
                  GOTO     d0
Delay27 MOVLW    d'27'
                  GOTO     d0
Delay20 MOVLW    d'20'
                  GOTO     d0
Delay5  MOVLW    0x05
d0          MOVWF    count1
d1          MOVLW    0xC7
                  MOVWF    counta
                  MOVLW    0x01
                  MOVWF    countb
Delay_0 DECFSZ   counta,f
                  GOTO     $+2
                  DECFSZ   countb,f
                  GOTO     Delay_0
                  DECFSZ   count1,f
                  GOTO     d1
                  RETLW    0x00

                  END

; 'program sonu'

```