T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK GÜVENLİKLİ KIZILÖTESİ İLETİŞİM UYGULAMASI

YÜKSEK LİSANS TEZİ

Akif AKGÜL

Enstitü Anabilim Dalı : ELEKTRONİK VE BİLG. EĞT.

Tez Danışmanı : Yrd. Doç. Dr. Özdemir ÇETİN

Ocak 2011

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK GÜVENLİKLİ KIZILÖTESİ İLETİŞİM UYGULAMASI

YÜKSEK LİSANS TEZİ

Akif AKGÜL

Enstitü Anabilim Dalı : ELEKTRONİK VE BİLG. EĞT.

Bu tez 17/ 01/ 2011 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Yrd.Doç.Dr. Özdemir ÇETİN Jüri Başkanı	Yrd.Doç.Dr.Öğ.Yb. Feyzi AKAR Üye	Yrd.Doç.Dr. Cüneyt BAYILMIŞ Üye

TEŞEKKÜR

Yüksek lisans eğitimim süresince değerli birikimlerini bana aktaran, tezimin başlangıcından bitimine kadar her aşamasında sorunlarımı dinleyen, çalışmalarıma yön veren ve değerli zamanını sorunlarımın çözümüne ayıran tez danışmanım Sayın Yrd. Doç. Dr. Özdemir ÇETİN'e, tez ile ilgili çalışmam da bilgi ve birikimlerinden yararlandığım değerli hocalarım Yrd. Doç. Dr. Öğ. Yb. Feyzi AKAR ve Yrd. Doç. Dr. Cüneyt BAYILMIŞ'a, araştırma ve çalışmalarımda katkıda bulunan, donanım ve yazılım geliştirmede yardımlarını esirgemeyen Arş. Gör. Sezgin KAÇAR ve Uzman Ahmet KARACA'ya teşekkürlerimi sunarım.

Bugünlere gelmeme katkıda bulunan annem Ayşe ve babam Mehmet AKGÜL'e, ben okurken maddi ve manevi desteklerini esirgemeyen kardeşim Yunus'a ve üzerimde emeği olan herkese sonsuz teşekkürlerimi sunarım.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

TEA	: Tiny Encryption Algorithm
C	: Şifrelenmiş Bilgi
CE	: Chip Enable
D	: Şifre Çözme Bloğu
DES	: Data Encryption Standard (Veri Şifreleme Standardı)
E	: Şifreleme Bloğu, Şifreleme Tekniği
IDEA	: International Data Encryption Algorithm
IR	: Infrared (Kızılötesi)
IrDA	: Infrared Data Association
K	: Anahtar (Key)
UV	: Ultraviyole Işınlar (Morötesi ışınlar)
LSB	: Least Significant Bit (Düşük Değerlikli Bit)
M	: Açık Metin Kodları
ms	: Milisaniye
MSB	: Most Significant Bit (Yüksek Değerlikli Bit)
NIST	: National Institute of Standards and Technology
P	: Şifrelenmemiş bilgi
A	: Alıcı
RSA	: Rivest/Shamir/Adelman
RTC	: Real Time Clock (Gerçek Zaman Saati)
SCLK	: Serial Clock
SEA	: Scalable Encryption Algorithm (Ölçeklenebilir Şifreleme Alg.)
SIRC	: Sony IR Protocol
SPN	: Substitution-Permutation Network
V	: Verici
AES	: Advanced Encryption Standard

CRC32	: Checksum (Bir Çeşit Özet)
RC4	: Ron’s Cipher 4
RC5	: Ron’s Cipher 5
MD5	: Message-Digest Algorithm 5
ECC	: Elliptic Curve
DSA	: Digital Signature Algoritm
AGC	: Otomatik Kazanç Kontrolü
SATE	: Sakarya Tiny Encryption Protocol
µs	: Mikrosaniye
<<	: 1 bit sola kaydırma
>>	: 1 bit sağa kaydırma
^	: XOR İşlemi

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar Kelimeler: Kablosuz Haberleşme, Kriptoloji, Bilgi Güvenliği, Kızılötesi İletişim, Simetrik Şifreleme, Tiny Encryption Algorithm (TEA)

Haberleşmede güvenlik her zaman ön plandadır. İletişim sırasında veriler kötü niyetli kişiler tarafından ele geçirilebilir. Güvenli bir haberleşme için günümüze kadar birçok çalışma yapılmıştır. Fakat teknolojinin her alanında olduğu gibi güvenlik alanında yapılan çalışmalarda da en iyi sonuç elde edilememiştir. Son yıllarda hızla ilerleme kaydeden sayısal elektronik teknolojisi sayesinde mikroişlemcili ve bilgisayar tabanlı birçok elektronik sistemin tasarımı ve uygulaması haberleşmeyi daha kolay ve güvenilir hale getirmiştir.

Bu tez çalışmasında, kablosuz ortamda yüksek hızla çalışan ve diğer kablosuz haberleşme yöntemlerine göre maliyeti düşük olan IR tabanlı sistemlerin güvenliğini arttırmaya yönelik bir çalışma yapılmıştır. İlk olarak standart protokollerden farklı olarak SATE isimli yeni bir protokol tasarlanmıştır. Ardından güvenliği daha da artırmak için sisteme bir simetrik anahtar şifreleme yöntemi olan TEA blok şifreleme algoritması eklenmiştir. Son olarak ise, sistemin yetkisiz kişiler tarafından kullanılmasını önlemek ve kullanımı kolaylaştırmak amacıyla kullanıcı arayüzü eklenmiştir. Arayüz sayesinde sistemi sadece tanımlı kullanıcılar kullanabilecek ve yönetici tarafından kullanıcıların sistemi hangi sıklıkla ve ne zaman kullandıkları kontrol edilebilecektir. SATE protokolünün başarımı bellek boyutu ve çalışma performansı kriterlerine göre incelenerek var olan protokoller ile karşılaştırılmıştır.

HIGH SECURE INFRARED COMMUNICATION APPLICATION

SUMMARY

Key Words: Wireless Communication, Cryptology, Information Security, Infrared Communication, Symmetric Encryption, Tiny Encryption Algorithm (TEA)

Security is always an important issue in communication. Communication data may be got by malicious people during communication. Many studies have been focused for safety communication until today. However, any studies in the field of security haven't been reach perfection like all fields of technology. In recent years due to advancing digital electronic technology, communication has become easier and reliable.

In this thesis, design and applications are performed to increase security in IR based systems, which can work at high speeds in wireless environment with low costs. Firstly, a new protocol is called SATE is designed instead of standard protocol. After TEA algorithm, which is a block encryption algorithm in symmetric key systems, is added to the system. Finally, a user interface implemented in the system to prevent unauthorized entries from transmitting circuit. This interface will accept users who are authorized to use system. With this interface administrator can check the user statistics such as usage rates and access times of users, and interfere the system if necessary. Success of SATE protocol is performed according to memory size and performance of work measures and then compared with existing protocols.

BÖLÜM 1. GİRİŞ

Geliştirilen elektronik güvenlik sistemlerinde kablosuz iletişim gereksinimi hızla artmaktadır. Buradaki en büyük sıkıntı iletişim sırasında bilginin güvensiz ortamlarda alıcıya gönderilmesidir. İletişim protokolünün veya sisteminin güvenliği yetersizse ya da sistem bir güvenlik duvarına sahip değil ise iletişim kötü niyetli kişiler tarafından engellenebilir.

Günümüzde birçok kablosuz haberleşme türü bulunmaktadır, bunlardan birisi de kızılötesi ışınım ile haberleşmedir. Birçok alanda kızılötesi ışınım ile kablosuz haberleşme yapılmaktadır. Her alanda olduğu gibi kızılötesi haberleşmenin de güvenilirliği sorgulanabilir. Güvenli haberleşmenin ön planda olduğu günümüzde özellikle kablosuz haberleşme sistemlerinin güvenliği için birçok çalışma yapılmaktadır. Fakat kızılötesi haberleşme güvenliğini arttırmaya yönelik yapılmış çalışma oldukça azdır.

Bu tez çalışmasında kızılötesi haberleşmede güvenliği arttırmaya yönelik çalışmalar yapılmıştır. İlk olarak kızılötesi iletişim için piyasada varolan standart protokollerden farklı olarak SATE isimli özel bir protokol geliştirilmiştir. SATE protokolü standart protokollerden farklı bir protokol olduğu için geliştirilen sistem başka verici devreleri ile çalıştırılamayacaktır. Doğru iletişimin sağlanabilmesi için gerekli olan ilk adımlardan birisi protokolün anlaşılabilmesidir. Bilinmeyen bir iletişim protokolüne sahip bir sistemde haberleşmeyi sağlamak olanaksızdır.

SATE protokolüne ek güvenlik önlemi olarak verilerin daha güvenli gönderilebilmesi için simetrik anahtarlı sistemlerindeki blok şifreleme algoritmalarından TEA (Tiny Encryption Algorithm) ile şifreleme yapılmıştır. Veriler gönderilmeden önce şifrelendiği için iletişim esnasında herhangi dinleyici veya istenmeyen kişi gerçek verileri elde edemeyecektir. Son olarak ise geliştirilen

sistemin kullanımını kolaylaştırmak ve verici devresinin istenmeyen kişiler tarafından aktif edilmesini engellemek için kullanıcı arayüzü eklenmiştir. Bu sayede sistemi sadece kullanıcı şifresi olan kişiler aktif edebileceklerdir. Ayrıca kullanıcı arayüzündeki tüm kullanıcıları kontrol eden birde yönetici bulunmaktadır. Yönetici şifresine sahip olan kişi tüm kullanıcıların sistemi ne zaman hangi sıklıkla kullandığını kontrol edebilmektedir. Bahsedilen tüm bu güvenlik önlemlerinin herhangi bir aşamasındaki problem durumunda kızılötesi iletişim gerçekleştirilemeyip, istenen sistem aktif edilemeyecektir.

Çalışmanın mikrodenetleyicili sistemlerde uygulanabilması sistemin birçok yerde kullanılmasına olanak sağlamaktadır. Ayrıca günümüze kadar kızılötesi haberleşme güvenliğine yönelik yapılan çalışmalara nazaran sistemde birçok güvenlik duvarının var olması kızılötesi iletişimi daha güvenilir hale getirmiştir.

Genel olarak her türlü bilgi iletiminde güvenli bir haberleşmenin sağlanabilmesi için gerekli minimum bazı gereksinimler bulunmaktadır. Bunlar; gizlilik, bütünlük, doğrulama ve inkar edememedir. Gizlilik, mesajın sadece yetkili kişiler tarafından görülebilmesidir. Bütünlük, mesajın gönderici dışında hiç kimse tarafından değiştirilememesidir. Doğrulama, mesajı gönderen kişinin kimliğinin doğrulanması ve böylece yetkili kişiler dışında hiç kimsenin mesaja erişimine izin verilmemesidir. İnkar edememe ise, mesajı gönderen kişinin mesajı gönderdiğini kabul etmesidir (Yıldırım, 2006).

Güvenli bir haberleşmeden bahsetmek için yukarıda sayılan minimum gereksinimler yerine getirilmelidir. Bunun için kriptolojiden diğer bir deyişle şifreleme biliminden yararlanılır. Kriptoloji, insanlığın yaratılışından günümüze kadar çeşitli evrelerden geçmiştir. Kısacası insanlık ne zaman var olmuşsa kriptoloji de o zaman var olmuştur.

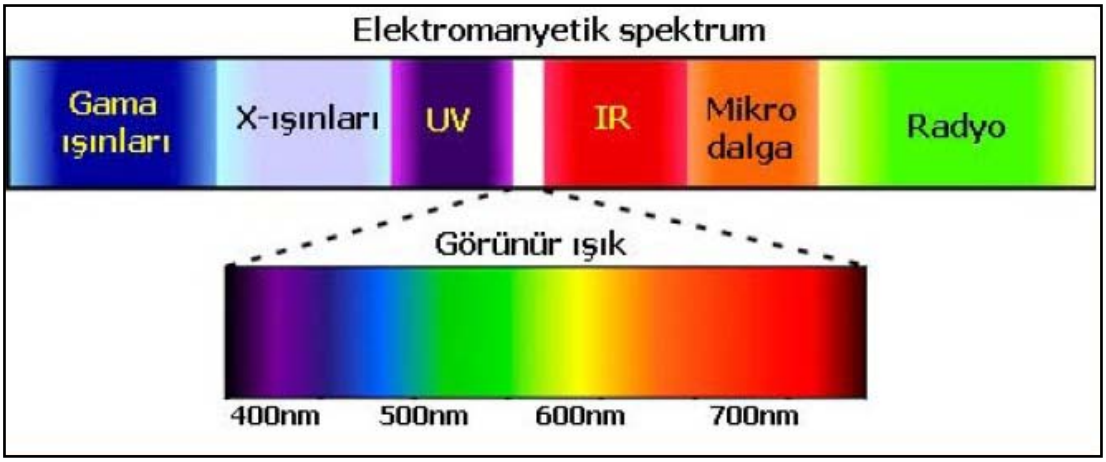
BÖLÜM 2. KIZILÖTESİ IŞINIM VE İLETİŞİM

Birçok alanda kızılötesi ışınım ile kablosuz haberleşme yapılmaktadır. Görülebilir mesafeden bir cihazı uzaktan kumanda etmenin en ekonomik yolu kızılötesi ışık ile kontrol etmektir. Günümüzde IR kontrol tekniği görüntü, ses gibi cihazların yanında sürekli veri transferi işlemlerinde de kullanılmaktadır (Güneş ve Yılmaz, 2007). Kızılötesi iletişimde en önemli unsur iletişim esnasında arada saydam olmayan bir cismin olmamasıdır. Saydam olmayan cisimlerin iletişimi engellemesi dezavantaj gibi gözüksede bazı durumlarda avantaj olmaktadır (Kapalı ortam haberleşmelerinde bilgi güvenliğini sağlaması, vb..). Her alanda olduğu gibi kızılötesi haberleşmenin de güvenilirliği sorgulanabilir. Güvenli haberleşmenin ön planda olduğu günümüzde özellikle kablosuz haberleşme sistemlerinin güvenliği için birçok çalışma yapılmaktadır. Fakat kızılötesi haberleşme güvenliğini arttırmaya yönelik yapılmış çalışma oldukça azdır. Bu tez çalışmasında kızılötesi iletişimde güvenliği arttırmaya yönelik çalışmalar yapılmıştır. Bölüm 2'de kızılötesi iletişim ile ilgili teorik olan bilgiler, Bölüm 4'de ise güvenliği arttırmaya yönelik uygulamalardan bahsedilmiştir.

2.1. Kızılötesi Işınım ve Diğer Işınım Türleri

Elektromanyetik spektrum, ışık hızı ile hareket ederek boşluk boyunca yayılan dalga boyu, nanometrelerden metrelere kadar değişen sürekli enerjidir (Kaçmaz ve Kabdaşlı, 2007). Elektronlar hareket ettiğinde boşlukta yayılabilen elektromanyetik dalgalar oluştururlar. Bu dalgalar 1865'te İngiliz fizikçi James Clerk Maxwell tarafından belirtilmiştir (Sengupta ve Sarka, 2003).

Görünür ışık spektrumu, en uzun radyo dalgalarından en kısa dalga boylu gama ışınlarına kadar uzanan elektromanyetik tayfın bütünü içinde çok küçük bir aralığı kapsar.



Şekil 2.1. Elektromanyetik tayf

Spektrumun dalga boylarına göre dizilen bileşenleri Şekil 2.1 (Erol, 2004) ve Şekil 2.2'de (Genç, 2006) gösterildiği gibidir. Bunlar:

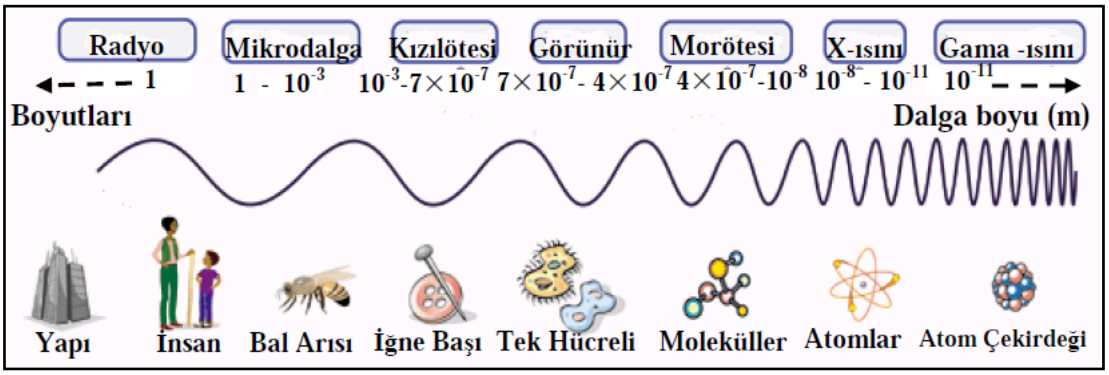
Gama Işınları: 0,01 nanometreden daha küçük dalga boylu ışınlardır. Bir atom çekirdeğinin çapından daha küçük dalga boylu dalgalar içerirler. Bu elektromanyetik tayfın en yüksek enerjili ve frekanslı bölgesidir. Pulsarlar, kara delikler ve kuazarlar gibi cisimlerde meydana gelen şiddetli nükleer tepkimeler sonucu oluşurlar. Ayrıca süpernova patlamalarında ve karadeliklerin etrafını çevreleyen madde diskinden karadeliğin olay ufkundan içine düşen maddenin aşırı ısınması sonucu da oluşurlar. Gama ışını ve X ışını gibi yüksek enerjili ışıma ortaya çıkarmak için son derece sıcak nesneler veya çok yüksek hızlarda parçacık hareketi gerekmektedir (Riz vd., 2006).

X Işınları: 0.01 ile 10 nanometre arasında dalga boyuna sahip ışınlardır (bir atomun boyu kadar). Alman fizikçi Wilhelm Conrad Roentgen tarafından keşfedilmişlerdir. Sınıflandırmada nereye ait olduklarını bilmediği için onlara X-Işınları adını vermiştir. X ışınları yumuşak maddelerin içine nüfuz ederler (Chandra, 2010).

Morötesi (Ultraviole-UV) Işınlar: 10 ile 310 nanometre arasında dalga boyuna sahip ışınlardır (yaklaşık olarak bir virüs boyutunda). Genç, sıcak yıldızlar bol miktarda morötesi ışık üretirler ve yıldızlararası uzayı bu yüksek enerjili ışınlarla yıkarlar. Dünya atmosferindeki ozon tabakası morötesi ve bu gibi kısa dalga boylu ışınların insan, hayvan ve bitkiler üzerindeki zararlı etkilerinin pek çoğundan korumaya

yardım etmektedir. Güneşin morötesi ışınlarından yalnızca bir kısmı yeryüzüne ulaşmaktadır ve bu ışınlar güneş yanıkları gibi cilt hastalıklarının yanı sıra cilt kanserine neden olmaktadır (Cope vd., 2006).

Görünür Işık: Görünür ışık , elektromanyetik tayfın insan gözü tarafından saptanabilen aralığıdır. Bu dalgaboyu aralığına kısaca görünür ışık veya sadece ışık da denmektedir. Aralığın sınırları tam olarak belirlenmemiş olmakla birlikte, ortalama bir insan, 400 ile 700 nm arasındaki dalgaboylarını saptayabilir. Titreşim sayısı olarak, bu aralık 450-750 teraherze eşdeğerdir (Anonim, 2010a).



Şekil 2.2. Elektromanyetik spektrum

Kızılötesi Işınlar: Kızılaltı veya Infrared (IR) olarak da isimlendirilen kızılötesi, görünür ışıktan uzun ve mikrodalgalardan daha kısa olan elektromanyetik bir ışınımdır. Infrared Latince'de aşağı anlamına gelen infra ve ingilizce kırmızı anlamına gelen red kelimelerinden oluşmaktadır ve kırmızıaltı anlamına gelir. Bu dalga türüne kızılötesi denmesinin sebebi ise görülebilir ışık türlerinin içinde en uzun dalgaboyuna sahip olan kırmızı ışıktan da uzun bir dalgaboyuna sahip olmasındandır. Doğrudan alınan güneşışığı %47 kızılötesi, %46 görünür ışık ve %7 morötesi ışınımdan oluşur (Anonim, 2010b). 710 nanometre ile 1 milimetre arası dalga boylarına sahip ışınları kapsar. Sıcak ve soğuk maddeler tarafından oluşturulurlar. Atomlar tarafından emildiklerinde maddeyi ısıtırlar bu yüzden ısı radyasyonu olarak da isimlendirilirler. 37^0C sıcaklığa sahip olan vücudumuz 900 nanometrelik kızılötesi ışıma yapar. Kızılötesi ışığın dalga boyu birkaç mikrometre uzunluğa kadar çıkmaktadır (Yücel, 2005).

Mikrodalga Işınları: 1 mm ile 1 metre arası dalga boylarına sahip ışınları kapsar. Radarlarda kullanılan çok kısa dalga boyuna sahip radyo dalgalarıdır. Mikrodalga fırınlarda ve kablo gerektirmeyen uzak mesafe iletişimlerde kullanılır. Aynı zamanda telefon uyduları da sesimizi iletmek için bu dalga boylarını kullanır. Sesimiz mikrodalga koduna dönüştürülür ve telefonumuz bu kodun şifresini çözer (Fisher, 1968).

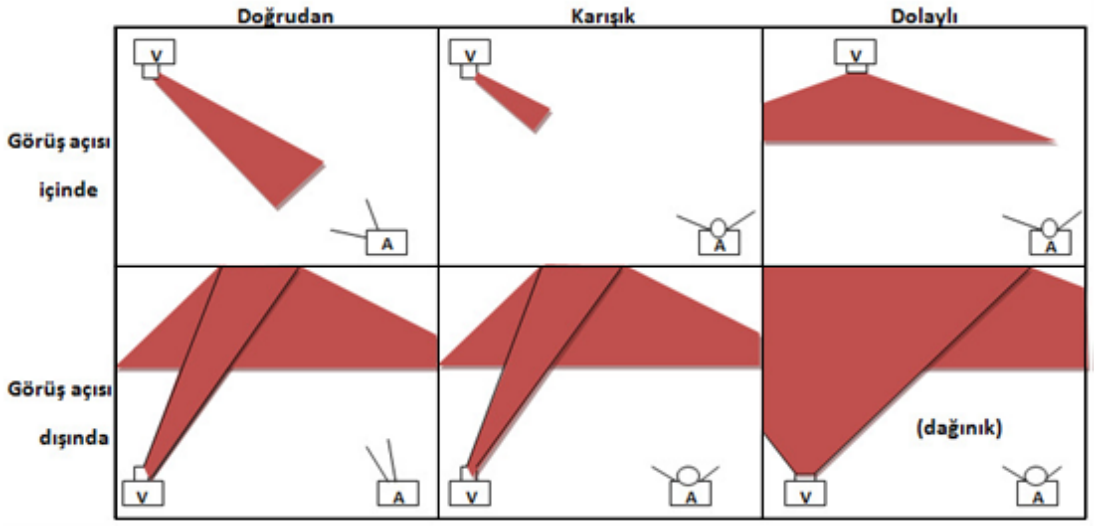
Radyo Dalgaları: Bir kaç santimetreden altı futbol sahasına kadar uzunluğu değişen aralıktaki dalga boylarına sahip olması nedeniyle görünmezdir. Radyolarımız bu dalgaları radyo istasyonlarından alır. Radyo istasyonu, sesi radyo ışığı şeklinde kodlar. Radyomuz düzensiz kodlanmış ışığı işleyerek sese dönüştürür. Radyo dalgaları aynı zamanda yıldızlar ve uzaydaki gazlar tarafından da yayılır, bu yayınımlar sayesinde yıldızların ve bu gazların nelerden meydana geldiği konusunda bilgi sahibi olunur (Genç, 2006).

2.2. Kızılötesi İletişim ve Bağlantı Yöntemleri

Kablosuz kızılötesi iletişim, haberleşme ortamı olarak kızılötesi banda yakın ışınların yayılımını sağlar (Heatley vd., 1998). Kızılötesi ışınımın dalgaboyu 750 nanometre ile 1 mikrometre arasındadır. Normal sıcaklığındaki insan vücudu 10 mikrometre civarında ışıma yapar (Crisp, 2010).

IR veri iletişimi bilgisayar cihazları arasında kısa mesafe iletişimde kullanılmaktadır. IR veri iletişiminde aygıtlar arasındaki standart IrDA (Infrared Data Association) kurumu tarafından sağlanmıştır. IrDA cihazlar, plastik bir mercek tarafından odaklanarak dar bir ışın haline getirilen kızılötesi ışığı kullanmaktadır. Bu ışık kaynağı kapatıp açılarak (modüle ederek) bilgi kodlanır ve karşı tarafa aktarılır. Alıcı tarafta bulunan silikon fotodiyot kızılötesi ışığı yeniden elektrik sinyaline çevirir. Fotodiyot sadece vericiden gelen yüksek frekanstaki sinyali algıladığından haberleşme ortamındaki düşük frekanslı sinyaller filtrelenmiş olur. Kızılötesi cihazlar arasındaki bağlantılar Şekil 2.3'de (Akgül vd., 2010) gösterilen iki farklı şekilde gerçekleştirilebilir; birincisi alıcı ve vericinin karşılıklı yerleştirilmesi (Görüş Açısı

İçinde), diğeri ise alıcı ve vericinin karşılıklı yerleştirilmemesidir (Görüş Açısı Dışında) (Kahn ve Barry, 1997).



Şekil 2.3. IR bağlantı yöntemleri

Görüş açısı içindeki bağlantılarda alıcı vericiden gelen sinyali doğrudan veya dolaylı olarak alırken, görüş açısı dışındaki bağlantılarda ise alıcı vericiden gelen sinyali bir yansıtıcı üzerinden almaktadır. Görüş açısı içindeki bağlantı güç verimliliğini maksimize ederken çoklu yollarda oluşan bozulmaları ise minimize eder. Görüş açısı dışındaki bağlantı, bağlantı kuvvetliliğini artırır ve kullanımı kolaydır. Alıcı ve verici arasında sinyalin geçmesini engelleyen bir cisim olsa bile sistemin çalışmasını etkilemez. En kuvvetli ve kullanımı kolay olan bağlantı dağınık bağlantı olarak da bilinen dolaylı görüş açısı dışındaki bağlantı türüdür (Green, 2007).

2.3. Kızılötesi İletişimin Avantaj ve Dezavantajları

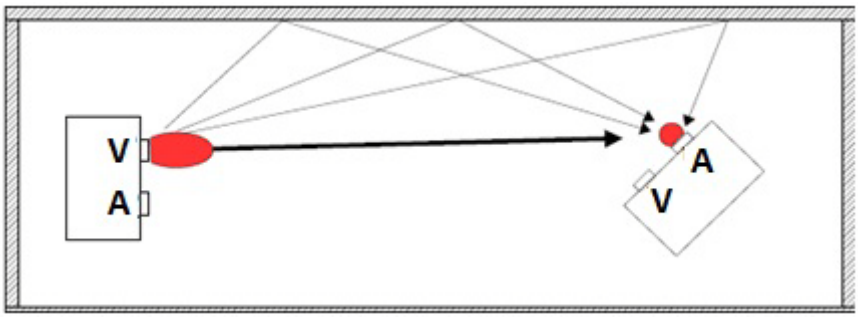
IR tekniği özellikle kapalı alan uygulamalarında kısa mesafe haberleşmesinde diğer kablosuz haberleşme tekniklerine göre önemli avantajlara sahiptir. En önemli avantajları, IR verici ve alıcıları yüksek hızlarda çalışabilirler ve maliyetleri düşüktür. IR ışınım cam gibi saydam nesnelerden geçebilirken duvar gibi saydam olmayan cisimlerden geçemez. Bu durum kapalı alanlarda iletişimi sınırlarken, saldırılara karşı da bir avantaj olmaktadır. İletişimin farklı ortamlar arasında olması

gerektiği durumlarda IR haberleşme tercih edilmemektedir. IR haberleşmede kapalı ortamlardaki iletişimin güvenlik seviyesi her ne kadar yüksek olsa da, dış ortamlardaki iletişimde etkin bir güvenlik duvarının sistemde bulunması önemli bir gereksinimdir.

Kızılötesi dalgaların duvar gibi saydam olmayan cisimlerden geçememeleri, iki farklı odadaki benzer sistemlerin birbirinden etkilenmeden çalışmaları anlamına gelir. Buradan şu sonuç çıkarılabilir, kızılötesi sistemlerin kötü niyetli kişilerce izlenmesi radyo sistemlerine göre daha zordur. Aynı zamanda kızılötesi sistemin kullanılabilmesi için radyo sistemlerinde olduğu gibi bir lisansa gerek yoktur. Bu özellikler kızılötesi sistemleri kapalı mekan kablosuz haberleşmede avantajlı yapmaktadır.

2.4. Kızılötesi İletişimin Çalışması

İki donanım arasındaki kızılötesi iletişimde kilit unsurlardan birisi Şekil 2.4'de (Carruthers, 2002) gösterildiği gibi bağlantının akıcı olması yani alıcı ve verici arasına herhangi bir engelin girmemesi ve aradaki uzaklığın olabilecek minumum seviyede olmasıdır.

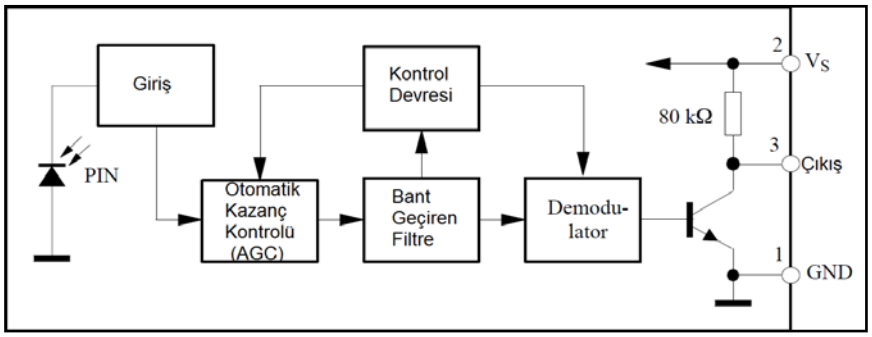


Şekil 2.4. Tipik bir kablosuz kızılötesi haberleşme sistemi

Şekil 2.4'de de gösterilen uzaktan kontrol sistemini gerçekleştirmek için öncelikle kızılötesi ışık yayan bir verici devresine ve kızılötesi ışık algılayan bir alıcı devresine ihtiyaç vardır. Uygun tasarlanmş bir alıcı-verici devresi ile herhangi bir cihazı açıp kapatmak mümkündür.

Şekil 2.5. IR LED ve TSOP12XX alıcı entegresi

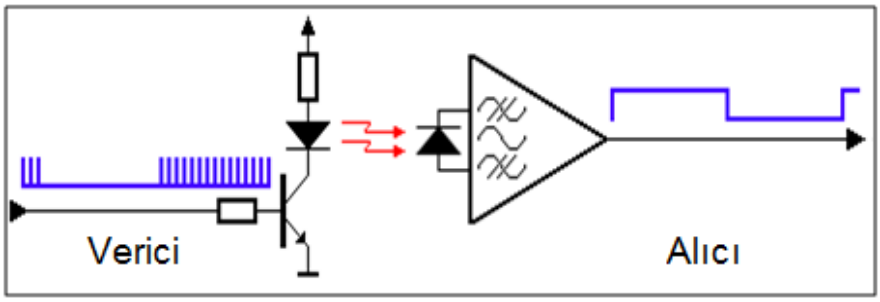
Kızılötesi iletişim için gerekli olan ana elemanlar Şekil 2.5'de gösterilen verici devresindeki IR LED ve alıcı devresindeki TSOP 12XX entegresidir. Frekanslarına göre farklı türlerde alıcı entegreleri bulunmaktadır ve çalıştıkları frekans aralıklarına göre isimlendirilmektedirler. Entegre isminin son iki hanesi frekans aralığını ifade etmektedir (TSOP 1236 - 36 kHZ, TSOP 1238 - 38 kHZ **)**.



Şekil 2.6. TSOP 1236 alıcı entegresi blok diyagramı

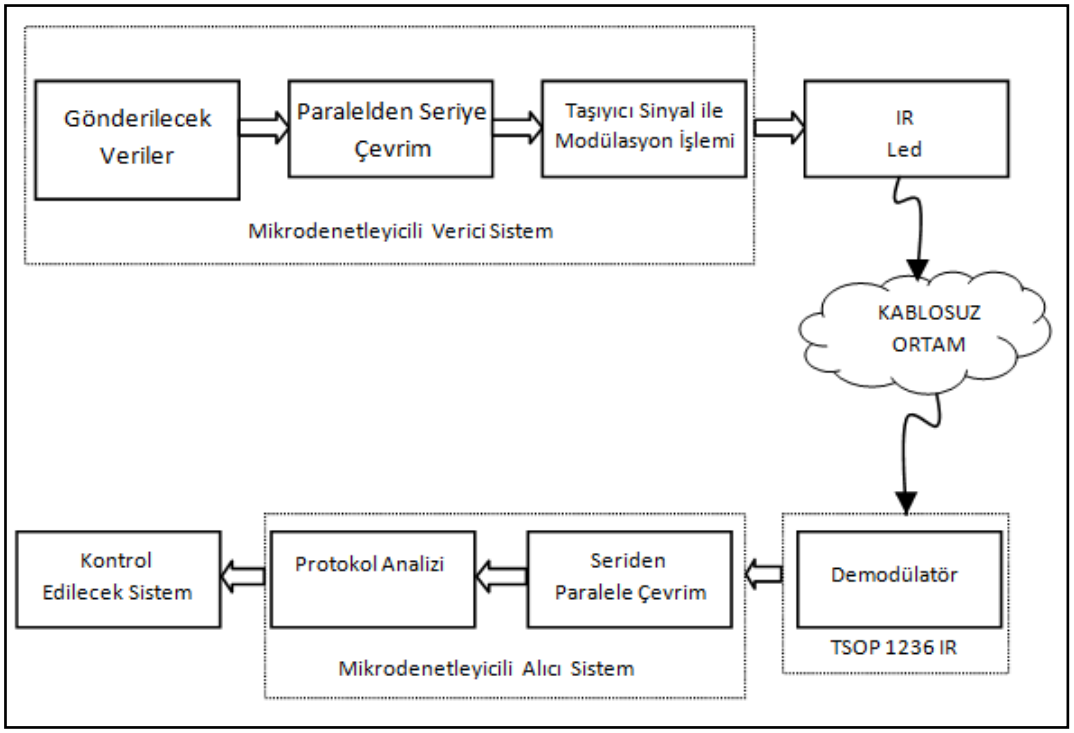
Alıcı entegresinin çalışma mantığı yukarıdaki alıcı entegresi blok diyagramında (Vishay Telefunken, 2001) gösterildiği gibidir. Gelen kızılötesi ışın sinyali öncelikle elektrik sinyaline çevrilir. Farklı genliklerde olabilen sinyaller, en iyi şekilde alınabilmesi ve gereken alıcı duyarlılığının ayarlanması için otomatik kazanç kontrol kısmından geçirilir. Daha sonra bant geçiren filtre kısmında modülasyon frekansı seçilir. Son olarak ise demodulatör kısmında aşağıdaki Şekil 2.7'de (Güneş ve Yılmaz, 2007) gösterilen verici kısmındaki modüle edilmiş sinyaldeki taşıyıcı sinyaller çıkarılarak alıcı kısmında olduğu gibi modüle edilmemiş sinyaller elde edilir. Çıkışın '0' olduğu durumda sinyal var, '1' durumunda ise sinyal yoktur. Sinyal olup olmadığını kontrol etmek için alıcı entegresinin çıkış ucuna bir adet led bağlanabilir. Normalde led her zaman yanık durumdadır, sinyal geldiğinde sönük

durumuna geçmektedir. Alıcı entegresindeki bütün blok diyagram tek bir entegrede toplanabilmekte ve birçok üretici firma bu tür entegreleri farklı özelliklerde üretebilmektedirler.



Şekil 2.7. Kızılötesi çalışma prensibi

IR LED ile verici devresinden kızılötesi sinyaller çevrede başka kızılötesi sinyallerde olabileceği için modüle edilerek belirli bir frekansta alıcı devresine yollanır. Alıcı devresinde TSOP 12XX entegresi ile gelen sinyaller bir önceki sayfada anlatılan çalışma mantığına göre mikrodenetleyiciye aktarılır. Mikrodenetleyicide protokol analizi yapılır. Eğer vericiden gelen sinyaller alıcıda tanımlandığı gibi ise doğru bir iletişim sağlanmış olur. Mikrodenetleyici de doğruluk kontrolü yapılırken başlangıç bit uzunluğu, toplam bit sayısı, lojik ‘1’ ve ‘0’ olduğu durumlardaki bit uzunlukları kontrol edilir. Gelen sinyaller mikrodenetleyicide anlamlı hale getirilerek vericiden gelen sinyaller elde edilmiş olur.



Şekil 2.8. IR haberleşme blok diyagramı

Şekil 2.8'de (Akgül vd., 2010) görülen blok diyagramında; verici devresinden gönderilen bilgiler alıcı devrede protokol çözümü yapılarak sistemin çalışması sağlanır. Haberleşme verileri verici devre üzerinde bulunan IR LED ile seri olarak alıcıya gönderilir. Bilgiler devre üzerinde bulunan butona basıldığında ard arda gönderilir. Veri iletimi seri olarak geçekleştiğinden haberleşme verileri paralelden seriye dönüştürülür. Seri hale dönüşen haberleşme verileri 38 KHzlik taşıyıcı bir sinyal ile modüle edildikten sonra IR LED üzerinden alıcıya aktarılır.

Alıcı devre tarafında TSOP1236 IR dedektörü ile algılanan kızıl ötesi ışık, demodülatörden geçirilerek haberleşme verisi geri elde edilir. Geri elde edilen haberleşme verisi mikrodenetleyici tarafından paralele çevrilerek hafıza alanına kaydedilir ve protokol doğruysa sistem çalıştırılır.

2.5. Kızılötesi İletişimin Kullanıldığı Yerler

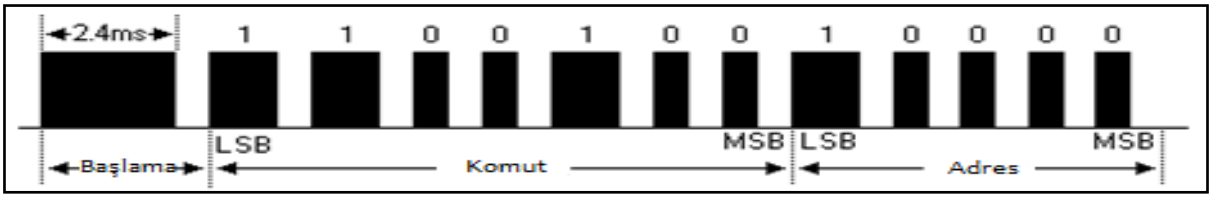
Kızılötesi iletişim hem sivil hem de askeri kullanım alanları bulmuştur. Hedef tesbiti, gözlemleme, gece görüşü, güdüm ve takip sistemleri gibi askeri kullanım alanlarının yanında, ısıl verimlilik analizi, uzaktan sıcaklık ölçme, kısa mesafeli kablosuz

iletişim, spektroskopi ve hava tahmini gibi alanlarda da kullanılmaktadır. Kızılötesi sistemlerin kullanım alanlarından olan gece görüşü genelde askeri amaçla kullanılmakta olup, bu yöntem kızılötesinin insanlar tarafından direkt olarak görülememesi özelliğinden yararlanır. Kızılötesinin yaygın olarak kullanıldığı bir başka alan ise belli bir mesafedeki objelerin ya da canlıların ısısının belirlenmesidir. Bu alanda, kızılötesi ışınlarının maddenin sıcaklığı arttıkça daha fazla emileceği bilgisi kullanılır. Normalde önemsiz bir bilgi gibi gözükse de bu bilginin kullanım alanı çok geniştir. Uydular bu yöntemle dünyanın belli bölgelerindeki sıcaklık dağılımlarını gözlemleyebilirler ve bu sayede meteorolojiye bilgi sağlayabilirler. Askeri alanda füzelerin kendi hedefini otomatik olarak takip etmesini sağlayan ısıya kilitlenen roketler de kızılötesi ısı ölçüm yöntemini kullanırlar (Bezen, 2010).

2.6. Kızılötesi İletişim Protokolleri

Günümüzde birçok firmanın geliştirdiği çeşitli standartlara sahip IR protokolleri vardır. Bunlardan yaygın olarak kullanılanları Sony, Sharp, Nec ve Nokia firmalarının geliştirdiği protokollerdir. Bu protokolleri birbirlerinden ayıran temel farklar ve protokollerin özellikleri başlangıç bit uzunlukları, toplam bit sayıları, lojik ‘1’ ve lojik ‘0’ konumundaki bit uzunluklarıdır. Bu bölümde ilk olarak Sony (SIRC) protokolü anlatılmaktadır.

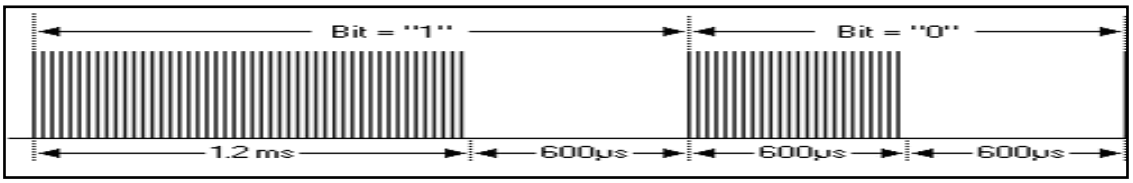
2.6.1. Sony protokolü



Şekil 2.9. Sony protokolünün yapısı

Sony Infrared Control (SIRC) protokolü Sony firması tarafından geliştirilmiş ve zamanla çeşitli alt prosedürlere ayrılmıştır. Toplam 12 bit uzunluğa sahip protokolde adres bilgisi 5 bit komut bilgisi ise 7 bit uzunluğundadır. SIRC protokolünün sinyal şekilleri Şekil 2.9’da (SB-Projects, 2001a) görülmektedir. Burada veri sinyallerinin

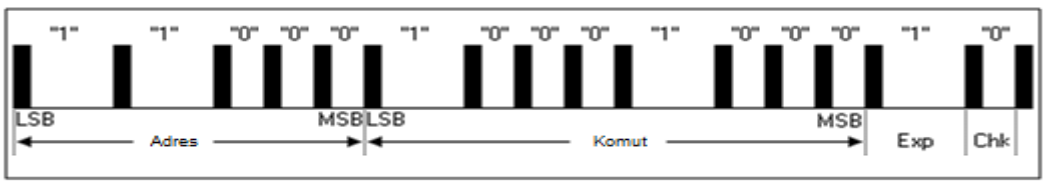
40 kHz'lik bir taşıyıcı sinyal ile modüle edildiği görülmektedir. Böylece yapılan modülasyon işlemi ile iletişim mesafesi artırılmaktadır.



Şekil 2.10. Sony protokolünde veri iletişimi modülasyon

Şekil 2.10'da (SB-Projects, 2001a) tipik bir SIRC protokolünün yapısı görülmektedir. SIRC protokolünde gönderilecek verinin önce düşük değerlikli biti gönderilmektedir. SIRC protokolündeki iletişim için; başlangıç biti olarak 2.4 ms Yüksek (High) ve 0.6 ms Düşük (Low) sinyal gönderilir, ardından 7 bit komut bilgisi gönderilir ve komutun hangi cihaz tarafından (TV, müzik seti vs) algılanacağını gösteren adres bilgisi gönderilir. Sony protokolünde 12 bitlik veri gönderilmeden önce alıcının 2.4 ms High (Header Time) ve 0.6 ms Low pozisyonunda olup olmadığı kontrol edilir. Bu koşullar sağlandıktan sonra gelecek olan bilginin veri bilgisi olduğu alıcı tarafından anlaşılır ve iletişim başlar. Veri bilgisinin ilk biti '0' ise gelen sinyal 0.6ms High seviyesine, 0.6 ms Low seviyesine sahip olur. Eğer ilk bit '1' ise gelen sinyal 1.2 ms high seviyesine, 0.6 ms low seviyesine sahip olur. Bu duruma göre gelen sinyaldeki '0' olan bitlerin periyotları 1.2 ms iken '1' olan bitlerin periyotları ise 1.8ms dir (SB-Projects, 2001a).

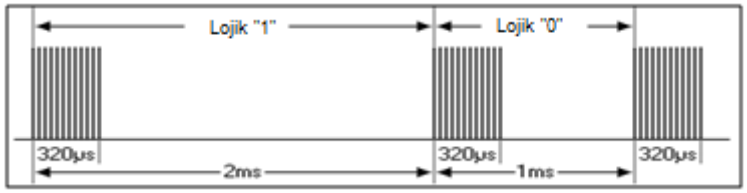
2.6.2. Sharp protokolü



Şekil 2.11. Sharp protokolünün yapısı

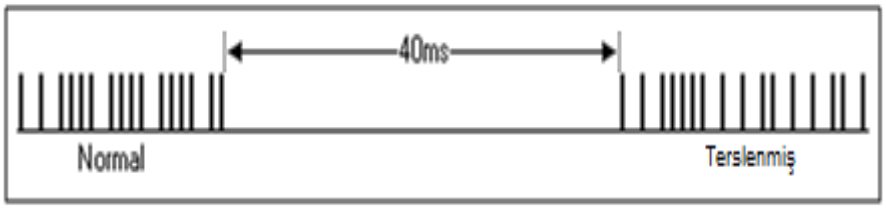
Sharp protokolü Şekil 2.11'de (SB-Projects, 2001b) gösterildiği gibi 5 bitlik cihaz kodu ve 8 bitlik tuş kodundan oluşan 13 bitlik paket data bilgisi kullanır. Diğer

protokollerden farklı olarak start biti yoktur ve paket sonunda iki kontrol biti bulunmaktadır. Sharp protokolünün frekansı 38 kHz'dir. Protokoldeki bit süreleri diğer bitlerinin durumuna göre değişkenlik gösterir.



Şekil 2.12. Sharp protokolünde veri iletişimi

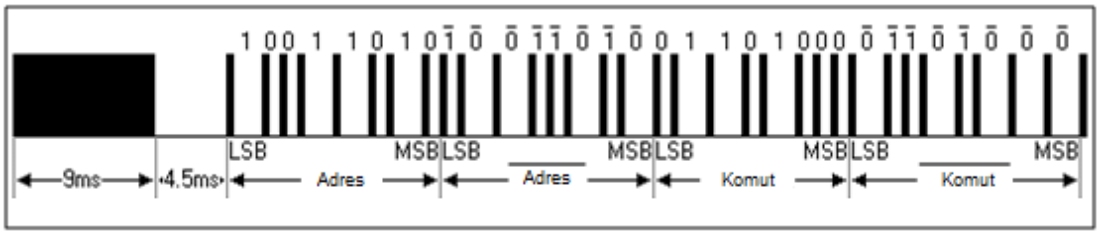
Şekil 2.12'de görüldüğü (SB-Projects, 2001b) gibi Lojik 0 olan bitlerde bit uzunluğu 1 ms, lojik 1 olan bitlerde 2 ms'dir. Lojik '1' ve lojik '0' daki sürelerin ilk 320 µs'si high, kalan süre ise low dur. Lojik '0' olan bitlerde 320 µs high, 680 µs low, Lojik '1' olan bitlerde 320 µs high, 1680 µs low şeklinde data gönderimi yapılmalıdır. Data gönderme mantığı diğer protokoller ile aynıdır ve yollanacak olan bir sonraki bit ara vermeden yollanır. İlk gönderilmesi gereken bit Şekil 2.11'de görüldüğü gibi en soldaki bittir (LSB).



Şekil 2.13. Sharp protokolünde bekleme süresi

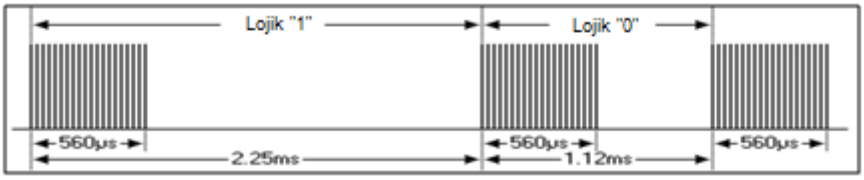
Her paket data gönderimi arasındaki süre Şekil 2.13'de (SB-Projects, 2001b) de gösterildiği gibi 40 ms dir.

2.6.3. Nec protokolü



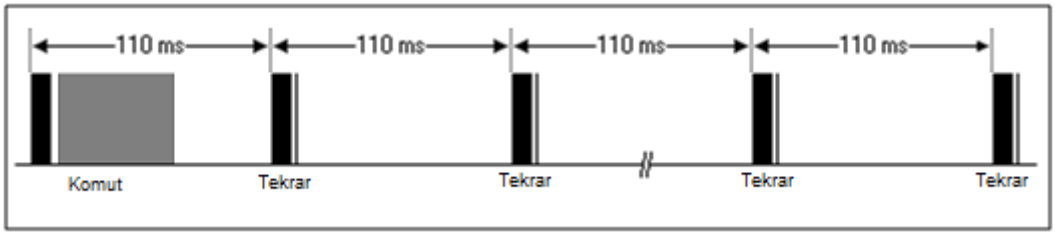
Şekil 2.14. Nec protokolünün yapısı

Nec Protokolünün çalışma frekansı 38 kHz'dir. Bu protokolde 8+8 cihaz kodu ve 8+8 tuş kodu olmak üzere toplam 32 bitlik paket data bilgisi kullanılır. Start biti Sony protokolünde olduğu gibidir ancak Şekil 2.14'de (SB-Projects, 2001c) olduğu gibi başlık zamanı (Header time) 9 ms, header time end ise 4.5 ms'dir. Start bitinden sonra kodlar 2 defa tekrarlanarak yollanır.



Şekil 2.15. Nec protokolünde veri iletişimi

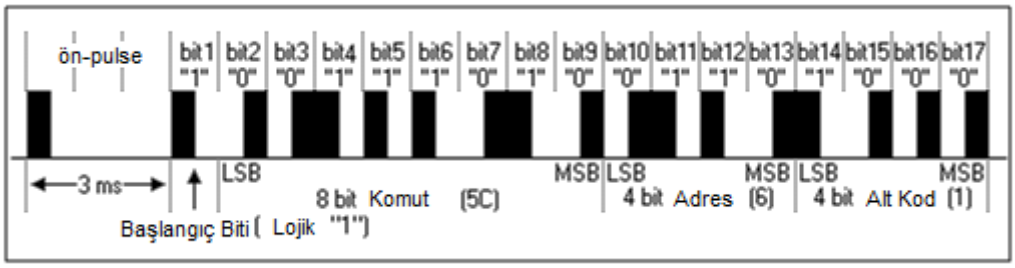
Protokoldeki bit kullanımı Sharp protokolü ile benzerlik göstermektedir. Ancak bir bit süresi Şekil 2.15'de (SB-Projects, 2001c) olduğu gibi lojik '0' olan bitlerde 1.12 ms, lojik '1' olan bitlerde 2.25 ms dir. Her iki durumda da sürenin ilk 560 µs'si high kalan süre low dur. Nec protokolünde data gönderimi; lojik '0' olan bitlerde 560 µs high, 560 µs low, lojik '1' olan bitlerde ise 560 µs high, 1690 µs low şeklinde yapılır. Diğer protokollerden farkı ise "Repeat Start" özelliğidir. İlk starttan sonraki 110 ms bitiminde 9 ms high ve 2.25 ms low yollamamız durumunda Repeat Start durumu oluşur. Bu durumda alıcı data kontrolü yapmadan vericinin bir önceki komutu tekrarladığını anlar ve bir önce aldığı komutu tekrar işler.



Şekil 2.16. Nec protokolünde bekleme süresi

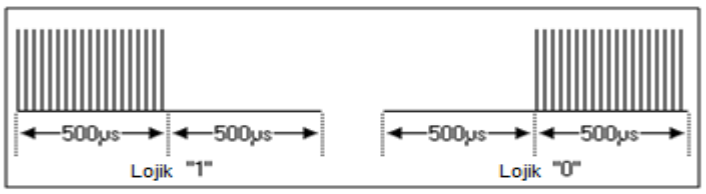
Bu protokolde ilk gidecek en sağdaki bittir (LSB). Şekil 2.16'da da (SB-Projects, 2001c) görüldüğü gibi her paket data gönderimi arasında 110 ms bekleme süresi vardır.

2.6.4. Nokia protokolü



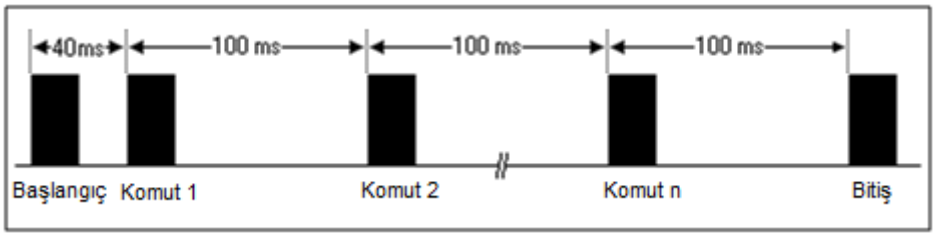
Şekil 2.17. Nokia protokolünün yapısı

Nokia protokolü; Şekil 2.17'de gösterildiği gibi (SB-Projects, 2001d) gibi 4 bitlik cihaz kodu, 8 bitlik tuş ve 4 bitlik alt cihaz kodundan oluşan 16 bitlik paket data bilgisi kullanır. Start için ilk olarak lojik '0' biti yollanır. Daha sonra 2500 µs boyunca low da beklenir ve lojik '1' biti yollanır. Toplam start süresi 4 ms'dir. Start bitinden sonra sırasıyla 8 bit tuş kodu, 4 bit cihaz kodu ve 4 bitlik alt cihaz kodu yollanır.



Şekil 2.18. Nokia protokolünde veri iletişimi

Protokolün frekansı birçok protokolde olduğu gibi 38 kHz'dir. Bu protokol RC5 protokolünü andırır bir bit süresi 1 ms dir. Şekil 2.18'den (SB-Projects, 2001d) bitin 1 olması, bu 1000 µs luk zamanın ilk 500 µs luk kısmında datanın high, kalan 500 µs luk zaman diliminde ise low olmasından anlaşılır. Bitin 0 olması ise, bu 1000 µs luk zamanın ilk 500 µs luk kısmında datanın low, kalan 500 µs luk zaman diliminde ise high olmasından anlaşılır.



Şekil 2.19. Nokia protokolünde bekleme süresi

Bu protokolde de ilk gidecek her protokolde olduğu gibi en sağdaki bittir (LSB). Şekil 2.19'da da (SB-Projects, 2001d) görüldüğü gibi her paket data gönderimi arasında 100 ms bekleme süresi vardır.

BÖLÜM 3. ŞİFRELEME BİLİMİ VE TEKNİKLERİ

Şifreleme, bir bilginin özel bir yöntemle değiştirilerek farklı bir şekle sokulması olarak tanımlanabilir. Şifreleme işlemi sonucunda ortaya çıkan yeni biçimdeki bilgi, şifre çözme işlemine tabi tutularak ilk haline dönüştürülebilir (Gülaçtı, 2010). Şifreleme işlemleri için birçok algoritma geliştirilmiştir. Şifrelenecek veriye göre veya bilginin önemine göre bu algoritmalardan birisi tercih edilebilir. Genel olarak şifreleme algoritmaları açık metin, şifreli metin ve anahtardan oluşmaktadır. Şifreleme algoritmaları kripto sistemin en önemli parçasıdır. Temel olarak şifreleme algoritmalarını simetrik ve asimetrik olarak iki gruba ayırabiliriz. Simetrik algoritmalar şifreleme ve şifre çözme işlemlerinde aynı anahtarı, asimetrik algoritmalar ise farklı anahtarları kullanır. Simetrik şifreleme algoritmaları blok şifreleme ve akış (stream) şifreleme olmak üzere iki gruba ayrılırlar. Blok şifreleme, orijinal metni veya şifreli metni bloklara bölerek şifreleme/şifre çözme işlemini yapar. Akış şifrelemede ise bir bit veya bayt üzerinde şifreleme ve şifre çözme işlemleri yapılır (Şahin vd., 2005).

Günümüzde blok şifreleme algoritmaları, şifreleme işlemlerinde / uygulamalarında yaygın bir şekilde kullanılmaktadırlar. Blok şifreleme algoritmalarının gücü söz konusu olduğunda algoritmada kullanılan S kutuları, döngü sayısı, anahtarların XOR işlemine sokulması, blok uzunluğu, anahtarın uzunluğu ve özelliği büyük önem taşımaktadır. Ayrıca kullanılacak anahtarın rastlantısal olması da gerekir. Diğer yandan algoritmaya yapılan saldırılara karşı dayanıklılıkta, günümüz algoritmalarının gücünün ölçülmesinde önemli bir kıstas olmuştur. Bu saldırılara doğrusal kripto analiz ve diferansiyel kripto analiz saldırılarını örnek olarak verebiliriz (Şahin vd., 2005).

Şifreleme algoritmalarının başarımı; kırılabilme süresinin uzunluğuna, şifreleme ve şifre çözme işlemlerine harcanan zamana, şifreleme ve çözme işleminde ihtiyaç

duyulan bellek miktarına, algoritmaya dayalı şifreleme uygulamalarının esnekliğine, uygulamaların dağıtımındaki kolaylık ya da algoritmaların standart hale getirilebilmesine ve algoritmanın kurulacak sisteme uygunluğuna bağlıdır (Bandırmalı vd., 2008).

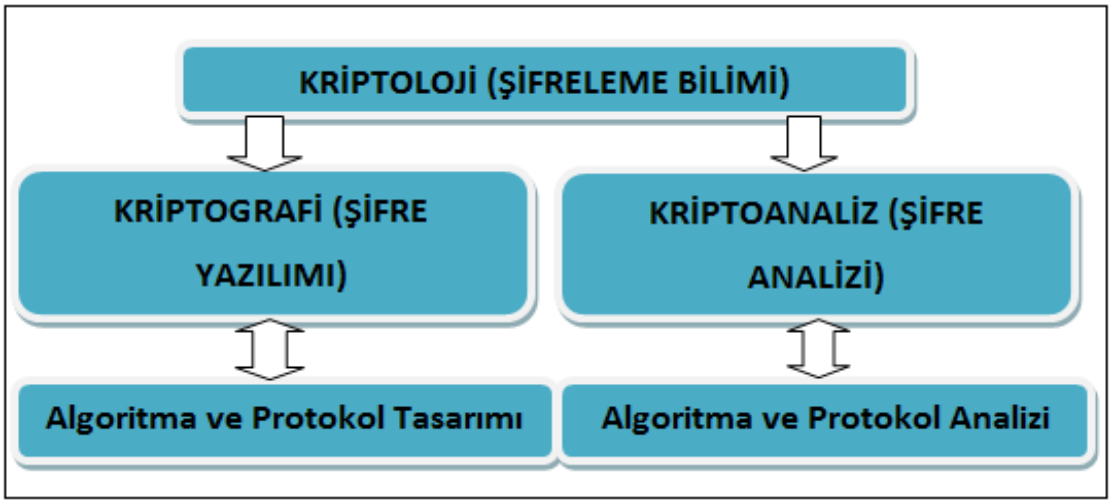
3.1. Şifreleme Bilimi (Kriptoloji)

Şifreleme, yalnızca geçerli geçiş anahtarına sahip olan kişi tarafından düzenlenip okunabilmesini sağlamak için bilgiyi karıştırarak bir ileti veya dosyanın güvenliğini artırma yoludur. Böylece hassas bilgilerin saklanması ya da güvensiz ağlar üzerinden karşı tarafa güvenli bir şekilde gönderilmesi sağlanır. Kriptoloji bilimi bilgi güvenliğinin sağlanması ile uğraşmaktadır. Kriptoloji sayısal verinin korunmasında ya da güvenli bir şekilde iletilmesinde kullanılan şifreleme algoritmalarının tasarımı ve bu algoritmaların güvenlikleri ile ilişkilidir. Bu açıdan bakıldığında bilgi güvenliği, günümüzde sayısal verinin güvenli bir şekilde iletilmesinde çok önemli yer tuttuğu için giderek dikkat çekmektedir (Sakallı, 2006).

Şifreleme ve şifre çözme işleminin zorluğu ihtiyaç duyulan güvenlik seviyesi ile doğru orantılıdır. Çok önemli olmayan bir bilginin şifrelenmesi, bilginin öneminden daha fazla işgücü ve zaman harcanmasından dolayı verimli olmayacaktır. Anahtar seçimi ve şifreleme algoritması özel koşullara bağlı olmamalı ve şifreleme yöntemi her türlü bilgi için aynı şekilde çalışmalıdır. Çok karışık bir sistemin gerçeklenmesi hem hatalara sebep olabilir hem de performans açısından tatmin edici olmayabilir. Şifrelemede yapılan hatalar sonraki adımlara yansımamalı ve mesajın tamamını bozmamalıdır. Şifreleme de kullanılan algoritmanın karıştırma ve dağıtma özelliklerinin olabildiğince iyi olmalıdır. Karıştırma ve dağıtma özelliği ne kadar iyi olursa mesajın şifrelenmiş hali ile açık hali arasında ilişki kurulması oldukça zor olacaktır (Gülaçtı, 2010).

Şekil 3.1'de de gösterilen kriptoloji bilimi; gizlilik, veri bütünlüğü, kimlik doğrulama gibi bilgi güvenliği problemlerine matematiksel teknikler kullanarak çözüm sunan kriptografi ile bu çözümleri çürütme işlemini hedefleyen kriptoanaliz branşlarından oluşan bir bilim dalıdır. Bir bilginin şifrelenmesini amaçlayan kriptografinin

güçlülüğü, şifrelenmiş verinin orjinal metine dönüştürülebilmesi için geçen süre ve kaynak miktarı ile ölçülebilir. Güçlü kriptografi anlayışında şifrelenmiş metnin uygun şifreleme anahtarı olmadan şifrenin çözülmesi zordur. Fakat günümüzde bilgisayarların yüksek işlem gücü şifrelerin kırılmasını mümkün hale getirmektedir. Kriptoanaliz ise; bir şifreleme sistemini veya sadece şifreli mesajı inceleyerek, şifreli mesajın açık halini elde etmeye çalışan bir kriptoloji disiplini olarak tanımlanabilir (Yıldırım, 2006).



Şekil 3.1. Kriptoloji, kriptografi, kriptoanaliz

Şifreleme algoritmaları sayısal veriyi şifreli hale bir anahtar yardımıyla dönüştürmektedir. Şifreleme işlemi sonucunda meydana gelen şifreli metin, saldırgan tarafından anahtar olmadan çözülemez. Bu olayı çok kullanılan bir örnek ile açıklarsak; Sezgin ve Abdullah güvenli olmayan bir hat üzerinden haberleşmek isteyen yetkili kullanıcılar, Musa'da yetkisiz / kötü niyetli kişi olsun. Bu kanal bir telefon hattı ya da bilgisayar ağı olabilir. Sezgin'in Abdullah'a yolladığı bilgi, açık metin olarak isimlendirilir ve herhangi bir metin, nümerik veri ya da herhangi bir şey olabilir. Sezgin, açık metni önceden kararlaştırılan bir anahtar kullanarak şifreler ve kanal üzerinden gönderir. Musa, kanaldaki şifreli metni dinleyerek görebilir fakat anahtar olmadığından açık metni elde edemez. Diğer yandan Abdullah, anahtarı bilmektedir ve şifreli metni değiştirilebilir ve açık metni tekrar oluşturabilir (Stinson, 2002).

3.2. Bilgi Güvenliği

Bilgi güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür. Bunun sağlanması için, uygun güvenlik politikasının belirlenmeli ve uygulanmalıdır. Bu politikalar, faaliyetlerin sorgulanması, erişimlerin izlenmesi, değişikliklerin kayıtlarının tutulup değerlendirilmesi, silme işlemlerinin sınırlandırılması gibi bazı kullanım şekillerine indirgenebilmektedir (Canbek ve Sağıroğlu, 2006).

Bilgi güvenliğinin sağlanmasında uyulması ve uygulanması gereken birçok güvenlik bileşeni vardır. Öncelikle üç ana ilke olan gizlilik, bütünlük ve erişilebilirlik gereksinimlerinin yerine getirilmesi gerekmektedir. Sonrasında ise bunlara ek olarak değerlendirilebilecek giriş kontrolü, emniyet, inkâr edememe, güvenirlik, kayıt tutma, kimlik tespiti gibi diğer şartların sağlanması da güvenliği arttırmaktadır. Bilgi güvenliğinin üst düzeyde sağlanabilmesi için bu bileşenler oldukça önemlidir (Sharp, 2004).

Yukarıda belirtilen bileşenlerin ana unsurlarından kısaca bahsedecek olursak; bilginin gizliliği ile kastedilen, bir bilgiye yetkili kişi ya da kişilerin erişmesinin sağlanmasıdır. Bunu sağlamak için bilgiyi şifreleyip göndermek, kilitli bir kutuya koyarak göndermek gibidir. Kutuyu açmak için o kutunun anahtarına sahip olmak gerekeceği için, kutunun içindeki bilgiye erişim bu şekilde kısıtlanmış olacaktır. Bilginin bütünlüğü ile kastedilen şey bilginin tahrip edilmemesinin garanti altına alınmasıdır. Tahrip edilmiş bir bilginin hiçbir anlamı olmayacaktır. Bilginin erişebilirliği ise, istenildiği zaman bilgiye erişilebilmesi veya talep edilen bilgiye kullanıcıların yetkisi dâhilinde zamanında erişim yapabilmesi için gerekli olan önlemlerin alınmasıdır (Karadere, 2010).

Bilgi güvenliğinin sağlanması için tarih boyunca çeşitli yöntemler kullanılmıştır. Geçmişten günümüze bilgi güvenliğinin sağlanması için sırasıyla fiziksel güvenlik, haberleşme güvenliği, yayılım güvenliği, bilgisayar güvenliği ve ağ güvenliği konularında çalışmalar yapılmıştır (Maiwald, 2003).

Maiwald tarafından ortaya atılan güvenlik önlemlerini sırasıyla açıklanacak olursa ilk konu olan fiziksel güvenlik ile anlatılmak istenen durum şu şekildedir: Tarihte insanlar önemli bilgileri önceleri taşlara kazıyarak daha sonraları da kağıtlara yazarak fiziksel güvenliği sağlanan ortamlarda saklamışlardır. Fiziksel güvenliğin sağlanabilmesi amacıyla, duvarlar örülmüş, kale hendekleri çekilmiş, giriş çıkışı kontrol eden nöbetçiler görev yapmıştır. Gizlenmek istenen bilgiler her ne kadar korunsada her zaman güvenlik önlemlerinin zayıf yönleri ortaya çıkmıştır. Bu zayıf yönleri de ortadan kaldırmak için her zaman farklı gizleme yöntemleri geliştirilmiştir. Diğer bir güvenlik önlemi olan yayılım güvenliği ise, elektronik sistemlerin meydana getirdiği yayılımların yetkisiz kişilerce ele geçirilip analizinin önlenmesidir (Baykal, 2005). Bilgisayar güvenliğinden kastedilen şey, bilgisayar uzmanı olan kişilerin kötü niyetli saldırıları ile bilgisayar güvenliğini tehdit etmesidir. Ağ güvenliği ise, ağ ortamlarının temelinde yatan paylaşım ve uzaktan erişim imkânlarının kullanılması sonucunda yeni güvenlik açıkları meydana gelmiştir. Bu açıklar, kötü niyetli veya meraklı kişiler tarafından kullanıldığında bilgilere yetkisiz erişim, sistemler ve servislerin kullanılamaz olması, bilgilerin değiştirilmesi veya ifşa edilmesi vb. güvenlik ihlalleri oluşmaktadır (Vural, 2007).

Elektronik tehditlere karşı kullanılan bazı yöntemlerin karşılaştırılması Tablo 3.1'de görülmektedir.

Tablo 3.1. Elektronik tehditlere karşı kullanılan yöntemler

	Kimlik Doğrulama	Gizlilik	Bütünlük	İnkar Edememe
AntiVirüs	-	-	VAR	-
Güvenlik Duvarları	VAR	VAR	-	-
Erişim Denetimi	VAR	VAR	-	-
Şifreleme	-	VAR	-	-
Açık Anahtar Altyapısı	VAR	VAR	VAR	VAR

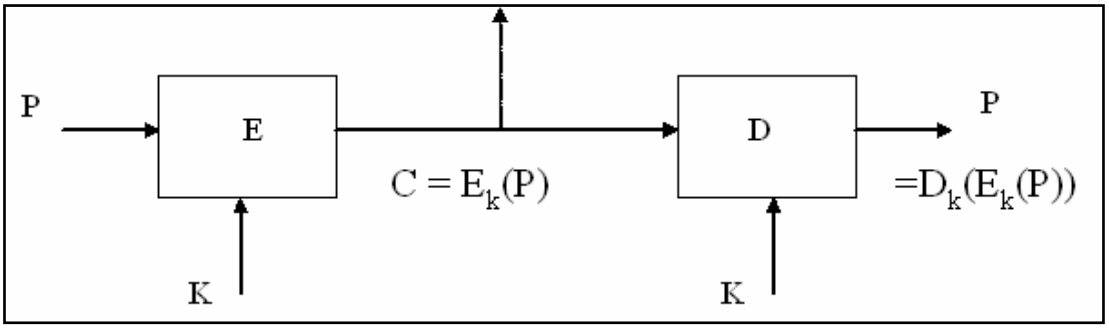
AntiVirüs programları, CRC32 gibi "checksum" (bir çeşit özet) kullanarak bilgisayardaki programların kontrol dışı değiştirilip değiştirilmediğini kontrol ederler. Bu nedenle sadece bütünlük hizmetini verebilirler. Güvenlik duvarları, kimlik doğrulama yaparak belirli kaynaklara erişimi sınırlarlar. Bu nedenle sadece

kimlik doğrulama ve gizlilik hizmetlerini sağlarlar. Şifreleme programları yöntemleri tek başlarına kullanıldığında sadece gizlilik hizmetini sağlayabilirler. Açık anahtar altyapısı kimlik doğrulama, gizlilik, bütünlük ve inkar edememe hizmetlerini sağlayarak çok daha kapsamlı çözüm sunmaktadır (Gülaçtı, 2010).

En güçlü savunma yöntemlerinden biri şifrelemedir. Özellikle verinin şifreli biçimde saklanması, veriye olan izinsiz erişimi de anlamsız hale getirir. Ayrıca şifreleme, kimlik doğrulama ve kimliğin inkar edilememesi gibi doğrulama mekanizmalarında da önemli bir yoldur. Şifreleme yalnız başına etkili olmadığı gibi, yanlış veya dikkatsiz kullanım sonucu kendisi bir güvenlik açığı haline gelebilir. Örneğin, açık anahtarlı şifreleme tekniğinde iki anahtar vardır, biri herkese açık, diğeri sadece kişiye özeldir. Bütün açık anahtarlı şifrelemenin güvenliği kişiye özel anahtarın ne denli iyi korunduğuna bağlıdır. İyi korunmayan veya iyi seçilmemiş bir özel anahtar kolayca bulunup şifreli verinin şifresi rahatlıkla çözülebilir. Üstelik şifreli olduğu için iyi korunduğu varsayılan bilgi için aslında olmayan bir güvenlik varmış gibi görünür. Bu yüzden şifreleme kullanırken diğer güvenlik önlemlerini gözden kaçırmamak gerekir (Karadere, 2010).

3.3. Şifreleme Yöntemleri

Kriptoloji şifreleme ile şifre çözme işleminin bir arada yapıldığı bir çalışma alanıdır. Burada şifreyi oluşturanlar ve şifreyi çözmeye çalışanlar olmak üzere iki önemli unsur vardır. Verilerin şifrelenmesi için şifreleme algoritmaları kullanılır. Algoritmalar, açık metin üzerinde yapılan karmaşık işlemlerden oluşan matematiksel formüllerdir. Bir algoritma, hem yazılımla hem de donanım bileşenleri ile gerçekleştirilebilir. Birçok algoritma, şifreleme ve şifre çözme işlemini gerçekleştirmek amacıyla, "anahtar" denen bir değer kullanır. Anahtar '0' ve '1' lerden oluşan uzun bir bit dizisidir. Her algoritmanın kullandığı anahtar uzunluğu farklıdır. Genellikle anahtar uzunluğu arttıkça, saldırganın bu şifreyi çözmesi güçleşir sistemin şifreleme ve şifre çözme hızı da yavaşlar (Pro-G, 2003).



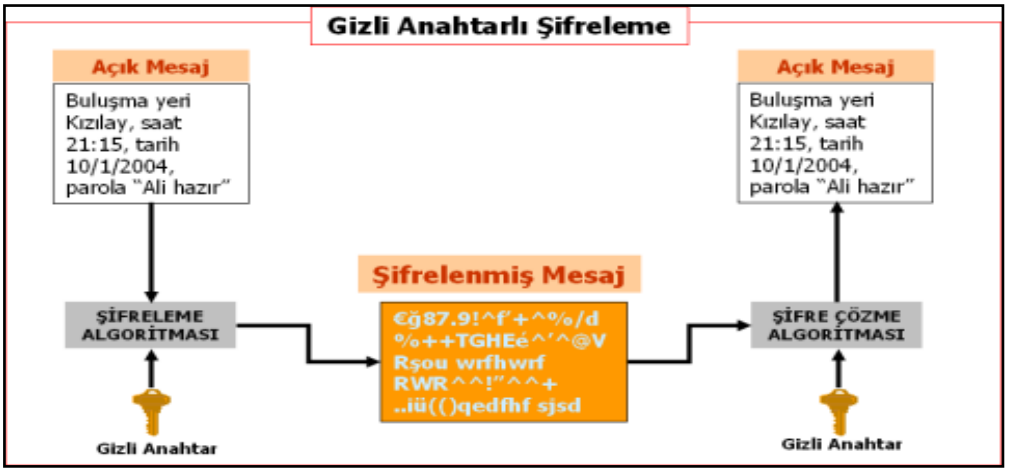
Şekil 3.2. Şifreleme ve şifre çözme işleminin blok şeması

Şekil 3.2'deki (Yıldırım, 2006) P ifadesi şifrelenmemiş bilgiyi, K ifadesi anahtarı, C ifadesi şifrelenmiş bilgiyi, E ifadesi şifreleme tekniğini ve son olarak D ifadesi ise şifre çözme bloğunu ifade etmektedir. Burada zorla sisteme girmeye çalışan kimsenin amacı şifrelenmiş bilgileri elde etmek ve onları çözmek olacaktır. Sistemdeki şifrelenmiş bilgiler elde edilebilir. Fakat şifreleme algoritması bilinmezse sadece şifrelenmiş bilgiler okunabilir. Bu yüzden şifreleme algoritması çok önemlidir. Çünkü uygun çözücü algoritması olmadan şifrelenen bilginin elde edilmesi oldukça zordur, hatta imkansızdır (Yıldırım, 2006). Şifreleme teknikleri genel olarak simetrik anahtarlı sistemler ve asimetrik anahtarlı sistemler olarak 2 başlık altında toplanabilir.

3.3.1. Simetrik anahtarlı şifreleme yöntemi

Simetrik kriptografide, şifreleme ve şifre çözme işlemi aynı anahtar ile yapılır. Simetrik kriptografide bu anahtar gizli tutulmalıdır. Bu nedenle, bu tip sistemlere gizli anahtarlı kriptografi sistemi adı da verilmektedir. Simetrik kriptografide güvenli bir şekilde iletişim kurmadan önce gönderici ile alıcının Şekil 3.3'deki gibi gizli anahtar olarak adlandırılan bir anahtar üzerinde uzlaşmaları gerekir (Gülaçtı, 2010).

Simetrik algoritmalar diğer algoritmalara nazaran daha hızlı çalışırlar. Bununla beraber, asimetrik algoritmalara nazaran saldırıya karşı daha az dirençlidirler. Simetrik algoritmalara TEA, SEA, AES, DES, Blowfish, IDEA ve RC4 algoritmaları örnek olarak verilebilir (Yıldırım, 2006) .



Şekil 3.3. Simetrik anahtarlı şifreleme

Simetrik şifreleme algoritmaları şifreleme ve şifre çözme işlemleri için tek bir gizli anahtar kullanmaktadır. Şifreleme işlemlerini gerçekleştirdikten sonra şifreli metni alıcıya gönderirken şifreli metinle birlikte gizli anahtarı da alıcıya güvenli bir şekilde göndermesi gerekmektedir. Simetrik şifreleme algoritmaları çok hızlı şifreleme ve şifre çözme işlemleri gerçekleştirebildiğinden dolayı günümüzde çok yaygın olarak kullanılmaktadır (Yerlikaya vd., 2006) .

Simetrik anahtar şifreleme algoritmaları blok ve akış şifreleme olmak üzere ikiye ayrılmaktadır. Blok şifreleme, şifresiz (gerçek) / şifreli metni bloklara bölerek şifreleme / şifre çözme işlemini yaparken, dizi şifreleme ise bir bit veya bayt üzerinde şifreleme / şifre çözme işlemlerini yapmaktadır. Simetrik anahtar şifreleme algoritmaları oldukça hızlıdır, donanımla gerçekleştirilmeleri kolaydır. Ama güvenli anahtar dağıtımı, bütünlük ve kimlik denetimi gibi gereksinimlerini gerçekleştirmek ise oldukça zordur (Altan vd., 2004).

3.3.1.1. Blok şifreleme algoritmaları

Bu tip algoritmalar şifrelenecek veriyi sabit uzunlukta bloklar olarak şifreleme fonksiyonuna alırlar ve aynı uzunlukta şifrelenmiş veri blokları üretirler. Bu algoritmalara AES, DES, IDEA, Skipjack, RC5, TEA, SEA örnek olarak verilebilir. Bu algoritmalar anahtar ve şifrelenmiş mesaj arasındaki ilişkiyi olabildiğince karışık ve tek bir açık mesaj karakterinin etkisini olabildiğince fazla şifrelenmiş karaktere yansıtıp iyi bir dağıtım yapmalıdırlar. Şifrelemeye başlamadan önce açık mesajın

içeriğini değişik bir sıraya koymalı ve tekrar eden blokları başka bloklarla yer değiştirerek şifreleme yapmalıdırlar. Blok şifreleme algoritmaları veriyi bloklar halinde işler. Bu işleme yöntemi bazen blokları birbirinden ayrı olarak bazende birbirine bağlı olarak da kullanır (Gülaçtı, 2010).

Bazı blok şifreleme algoritmaları açıklanacak olursa;

DES (Data Encryption Standard) algoritması, dünyada en yaygın kullanılan şifreleme algoritmalarından birisidir. IBM tarafından 1975 yılında "Federal Register" tarafından yayınlanmıştır. DES 64 bitlik veriyi 56 bitlik anahtar kullanarak şifreler (Stinson, 1995).

AES (Advanced Encryption Standard) Algoritması, John Daemen ve Vincent Rijmen tarafından Rijndael adıyla geliştirilmiş ve 2002 yılında standart haline gelmiştir. AES uzunluğu 128 bitte sabit olan blok ile uzunluğu 128, 192 ya da 256 bit olan anahtar kullanır. Kullanılan tekniklerden bazıları baytların yer değiştirmesi, 4x4'lük matrisler üzerine yayılmış metin parçalarının satırlarına uygulanan kaydırma işlemleridir. 2006 yılı itibariyle en popüler simetrik algoritmalardan olmuştur (Dalkılıç ve Yıldızoğlu, 2008).

SERPENT Cambridge, Halfa ve Bergen Üniversiteleri tarafından geliştirilen bir şifreleme algoritmasıdır. Serpent temel olarak DES'e benzeyen bir yapıya sahiptir (Yerlikaya vd., 2004).

MD5 **(**Message-Digest Algorithm 5) algoritması, veri bütünlüğünü test etmek için kullanılan, Ron Rivest tarafından 1991 yılında geliştirilmiş bir kriptografik özet (tek yönlü şifreleme) algoritmasıdır (Anonim, 2010c).

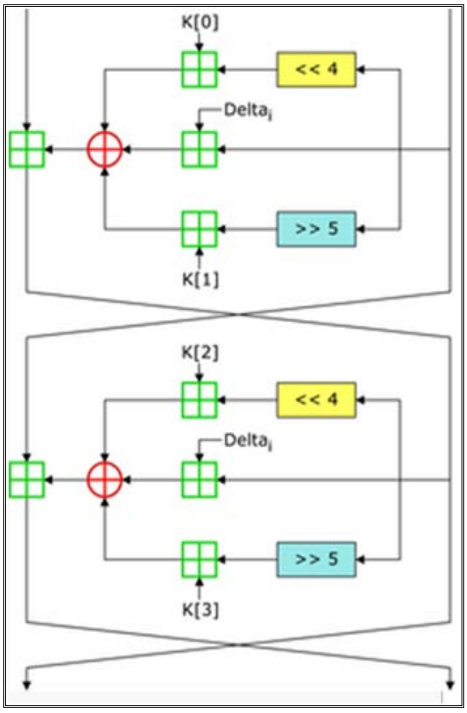
SEA (Scalable Encryption Algorithm), bellek büyüklüğü ve işlem gücü gibi sınırlı kaynaklara sahip gömülü sistemlere yönelik geliştirilmiş, bir şifreleme algoritmasıdır (Standaert vd., 2006). Simetrik blok şifreleme yaklaşımına dayanan SEA'nın tasarım kriterleri küçük bellek alanı, küçük kod büyüklüğü ve sınırlı komut setidir. Bu sebeple sadece, Özel veya, bit / kelime rotasyonları, mod 2_b toplama ve S box gibi bit operasyonlarını kullanır. Oldukça esnek bir yapıya sahip olan SEA, $SEA_{n,b}$

şeklinde ifade edilmektedir ve farklı metin, anahtar/kelime uzunlukları üzerinde çalışabilmektedir (Bayılmış ve Çakıroğlu, 2008).

BLOWFISH, 64 bit öbek büyüklüğüne ve 32 bit'ten 448 bit'e kadar anahtar uzunluğuna sahiptir. 16 tur Feistel Cipher'dır ve anahtar-bağımlı S-boxes kullanır. Sabit S-boxes kullanan CAST 128 yapısına benzer (Anonim, 2010d).

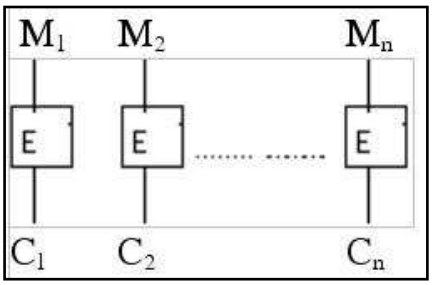
SKIPJACK, 64 bit uzunluğundaki veri, 80 bit anahtar kullanılarak ve 32 döngü sonunda şifrelemektedir. DES ile karşılaştırıldığında Skipjack, daha basit ve az işlem gerektiren bir algoritmaya ve daha uzun anahtar büyüklüğüne sahiptir. Ayrıca şifrelenmiş metnin 32 döngü sonunda elde edilmesi oldukça önemli bir avantaj sunmaktadır. Anahtar uzunluğunun ve döngü sayısının fazla olması Skipjack algoritmasını DES algoritmasından daha güvenli kılmaktadır (Bandırmalı vd., 2008).

TEA (Tiny Encryption Algorithm), David Wheeler ve Roger Needham tarafından geliştirilmiştir. TEA, "XOR, Add ve Shift" gruplarını içeren karışık cebirsel işlemleri ve Fiestel ağını kullanan şifrelemedir. Basitliği ve çoğu şifreleme algoritmalarından daha kısa satırdan oluşan uygulamasıyla dikkat çekmektedir. 64 bitlik bloklar kullanır. Bu 64 veri bloğunu 128 bitlik anahtar ile şifreler. 128 bitlik K anahtarı 32 bitlik bloklara bölünür. TEA, Shannon'un önerdiği ve güvenli bir blok şifreleme için gerekli olan karıştırma ve yayılma özelliklerini sağlayan önemli bir şifreleme yöntemidir. Karıştırma, şifreli metin ve açık metin arasındaki ilişkiyi gizlemeyi amaçlarken, yayılma açık metindeki izlerin şifreli metinde sezilmemesini sağlamak için kullanılır. Plain text, metinde yapılan tek bir bitin değişikliği cipher text, şifreli mesajda 32 bitlik değişikliğe sebep olur. Modern bir bilgisayardaki ya da çalışma alanındaki performansı oldukça etkilidir. TEA Tur Yapısı, değiştirilebilmesine rağmen 64 adet Fiestel turu ve 32 döngü halinde kullanılması en uygunudur (2 Fiestel turu = 1 döngü şeklinde). TEA için "2 Fiestel turu 1 çevrim" yapısı Şekil 3.4'de (Udea, 2010) gösterildiği gibidir (Çavuşoğlu, 2010).

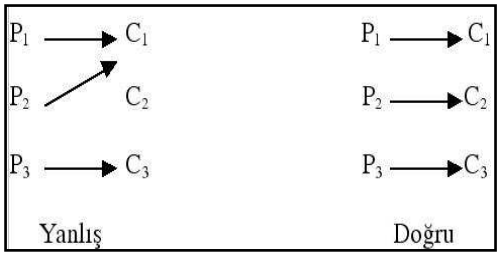


Şekil 3.4. 2 Fiestel turu ve 1 çevrim yapısı

Blok şifre sistemini, M_1; M_2; : : : ; M_n açık metnin blokları, yani her biri k bitten oluşan ardışık parçaları, C_1; C_2; : : : ; C_n bu bloklara karşılık gelen şifrelenmiş metinler ve E şifreleme işlemi olmak üzere, blok şifre sistemlerini Şekil 3.5'de olduğu gibi gösterebiliriz. Şekil 3.6'da ise doğru ve yanlış blok şifreleme örnekleri gösterilmiştir. Çoğu blok şifre sistemlerinde blok uzunluğu 64 bittir. İşlemcilerin hızı arttıkça blok uzunluğu da artabilmektedir. Son yıllarda üretilen sistemlerde 128 bit blok uzunluğu kullanılmaya başlanmıştır (Altan vd., 2004).



Şekil 3.5. Blok şifre sistemlerinde şifreleme



Şekil 3.6. Doğru ve yanlış blok şifreleme örneği

Blok şifreleme algoritmasının parametreleri; blok uzunluğu, anahtar ve gerçek anahtar uzunluğu olmak üzere iki kısımda incelenebilir.

Anahtar, döngü sayısı ve S kutuları blok şifreleme algoritmalarının önemli özelliklerindendir. Blok şifreleme algoritmalarında anahtarın uzunluğu ya da bit sayısı en temel saldırı olan geniş anahtar arama saldırısına karşın güçlü olmalıdır. Örneğin DES algoritması 56 bit anahtar kullanırken AES algoritması DES'in bu zaafını örter niteliktedir ve 128, 192, 256 bit anahtar seçenekleri mevcuttur. Ayrıca anahtarın rastlantısal olması gerekmektedir. Blok şifreleme algoritmalarında döngü sayısı iyi seçilmek zorundadır. Çünkü doğrusal transformasyon ve yer değiştirmelerin bu seçilen değerle algoritmaya yeterli gücü vermesi gerekmektedir. S kutuları, bir blok şifreleme algoritmasının en önemli ana elemanıdır. Çünkü algoritmadaki tek doğrusal olmayan yapıdır ve dolayısıyla algoritmaya gücünü veren en önemli unsurdur (Şahin vd., 2005).

Blok şifreleme algoritmalarına yönelik saldırı tiplerini; temel saldırılar ve gelişmiş saldırılar olarak iki başlık altında incelenebilir.

Temel Saldırılar: Blok uzunluğu n bit olan ve k bit anahtar uzunluğuna sahip bir blok şifresi için en temel saldırılardan biri sözlük saldırısıdır. Bu saldırıda k bitlik anahtarı kullanan saldırgan bir açık metni mümkün 2^k anahtarla şifreler ve şifreli metinleri sıralı bir sözlükte tutar. Daha sonra gizli anahtarla şifrelenmiş seçilmiş bir açık metni elde eder ve uygun bir eşleşmeyi sözlükten kontrol eder. Sözlükte arama ihmal edilebilir fakat saldırı için 2^k tane n-bit bellek word'ü gerekmektedir. Bu yüzden bu saldırı pahalı bir saldırı olarak nitelenebilir (Şahin vd., 2005).

Gelişmiş Saldırılar: Bu saldırılara doğrusal kriptanaliz, diferansiyel kriptanaliz, imkansız diferansiyel kriptanaliz ve çokluset saldırıları örnek olarak verilebilir. Doğrusal kriptanaliz, 1993 yılında Matsui tarafından teorik bir saldırı olarak keşfedilmiştir (Matsui, 1994). Daha sonra DES algoritmasına karşı başarı ile uygulanmıştır. Diferansiyel kriptanaliz, 1991 yılında Biham tarafından keşfedilmiştir (Biham ve Shamir, 1993). Doğrusal kriptanalize benzemektedir. Farkı seçilmiş açık metin saldırısı olmasıdır. İmkansız diferansiyel kriptanaliz, kesik diferansiyel kriptanalizin bir çeşididir. Kriptanalizde imkânsız durumların kullanılabileceği gerçeği eski bir fikirdir. Ortada ıskalama saldırısı ya da imkânsız diferansiyel saldırısı olarak isimlendirilen bu saldırılar bir blok şifrede imkânsız bir davranışın nasıl belirleneceği ve bunun nasıl anahtarı elde etmek için kullanılacağı ile ilişkili sistematik analizdir (Sakallı vd., 2005). Çokluset saldırıları, ilk defa J. Daemen, V. Rijmen ve L. Knudsen, Square algoritmasını ortaya koyduklarında öne sürülmüştür (Daemen vd., 1997). Dolayısıyla diğer ismi square saldırısı olarak bilinir. O zamandan beri diğer birçok algoritmaya uygulanmıştır (Twofish,IDEA, Camellia, Skipjack gibi). Seçilmiş açıkmetin saldırısıdır ve iyi seçilmiş açıkmetin setleri ile şifrenin ileri doğru incelenmesiyle gerçekleştirilir. Bu saldırı tipinde doğrusal ve diferansiyel kriptanalizden farklı olarak açık metinlerin tüm gurubunu düşünerek şifre hakkında bilgi toplanabilir (Sakallı vd.,2005).

3.3.1.2. Akış şifreleme algoritmaları

Akış şifreleme algoritmaları, bit katarı veya dizi şifreleme algoritmaları olarak da isimlendirilebilir. Akış şifreleme sistemi, açık metnin bir karakterine bir seferde zamanla değişen bir fonksiyon uygulayarak açık metnin karakterlerini ayrı ayrı şifreler. Genellikle hız gerektiren uygulamalarda kullanılmaktadırlar. Akış şifreler eşzamanlı ve eşzamansız olmak üzere temelde ikiye ayrılırlar. Eşzamanlı akış şifrelerde anahtar dizisi, açık metin ve gizli anahtardan bağımsız olarak üretilir. Her iki şifreleme tipi de sonlu durum otomatıdır ancak eşzamansız akış şifrelerde anahtar dizisi, sabit uzunluktaki bir önceki şifreli metinlerin ve anahtarın bir fonksiyonu ile elde edilir. Bu şifreleme algoritmalarından eşzamansız akış şifrelerde şifreleme şifreli metin sembolüne bağlı olduğu için bir iletim hatası durumunda sembol sonra şifrenin tekrar eş zamanlaması mümkün olacaktır. Böyle bir durum söz konusu

olduğunda öteki sembol hatalı olacaktır. Yani hata yayılması eşzamanlı şifrelere göre kötüdür. Ancak eş zamanlama düşünüldüğünde eşzamansız şifreler eşzamanlı olanlara göre daha iyidir. Eşzamanlı şifrelerde eş zamanlama tekrar sağlanamaz (Sakallı vd., 2007). Akış şifreleme algoritmalarına RC4, A5/1, A5/2, Panama algoritmaları örnek olarak verilebilir.

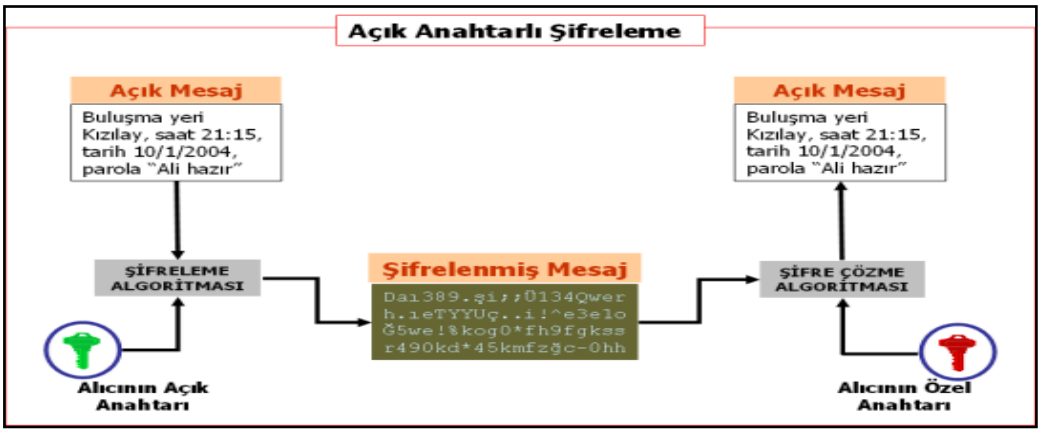
3.3.2. Asimetrik anahtarlı şifreleme yöntemi

Simetrik şifreleme tekniğinde bulunan anahtar dağıtım problemini çözmek için şifreleme ve şifre çözme işlemlerinin her birisi için ayrı ayrı anahtar kullanma prensibine dayanan bir şifreleme sistemi geliştirilmiştir. Bu sistemde şifreleme işlemi herkes tarafından bilinen açık anahtarla yapılır. Şifreleme ve şifre çözme işlemi birbirinin simetriği olmayan (yani aynısı olan) algoritmalarla gerçekleştirildiğinden dolayı da asimetrik şifreleme sistemi olarak bilinir (Yerlikaya vd., 2005).

Asimetrik kriptografide, şifreleme ve şifre çözme işlemi farklı anahtarlar ile yapılır. Bu anahtar çiftini oluşturan anahtarlara açık ve özel anahtar adı verilir. Bu kriptografi yönteminde özel anahtar gizli tutulmalıdır fakat açık anahtar yayınlanabilir. Bu özelliğinden dolayı asimetrik kriptografi, açık anahtarlı şifreleme adıyla da anılır. Asimetrik anahtar şifreleme algoritmalarında ise anahtar yönetimi, ölçeklenebilirlik, güçlülük, bütünlük ve kimlik denetimi gibi güvenlik hizmetleri kolaylıkla sağlanabilir. Bununla birlikte, simetrik anahtar şifreleme algoritmalarıyla karşılaştırıldıklarında yaklaşık 1500 kat kadar daha yavaştır. Ayrıca anahtar uzunlukları bazı uygulamalar için kullanışlı değildir. Simetrik kriptografinin gizlilik ve hızlı performans özelliğine karşı, asimetrik şifrelemenin de gizlilik, bütünlük, kimlik doğrulama, inkar edilememezlik özellikleri bulunmaktadır. Her iki şifreleme algoritmasında da güvenlik anahtar uzunluklarına bağlıdır (Gülaçtı, 2010).

Asimetrik anahtar şifreleme algoritmalarında, verinin şifrelenmesi için açık anahtar (public key), şifre çözme için ise matematiksel/mantıksal olarak açık anahtara bağlı özel bir anahtar (private key) kullanılmaktadır. Asimetrik anahtarlı şifreleme yöntemine Elgamal, RSA, ECC, Diffie-Hellman ve DSA algoritmaları örnek olarak

verilebilir. Asimetrik anahtar sisteminde gönderici ve alıcının gizli anahtarları paylaşmaları gereksinimi ortadan kalkmıştır. Tüm iletişimler sadece açık anahtar üzerinden gerçekleştirilir. Özel anahtarınız hiç bir şekilde paylaşılmaz ya da gönderilmez. Simetrik sistemlerde özellikle geniş ağ yönetiminde anahtar kullanımı ve dağıtımı oldukça zordur. Bu sistem ile anahtar kullanımı ve anahtar yönetimi problemleri ortadan kaldırılmıştır. Açık anahtara sahip bir kişi bilgiyi sadece şifreleyebilir fakat çözemez. Yalnızca özel anahtara sahip olan kişi bilgiyi okuyabilir. (Yıldırım, 2006).



Şekil 3.7. Asimetrik şifreleme

Asimetrik algoritmalar, simetrik algoritmalara göre daha güvenli ve kırılması zor algoritmalardır. Bununla birlikte, performansları simetrik algoritmalara göre oldukça düşüktür. Şekil 3.7'de de görüldüğü gibi (Gülaçtı, 2010) asimetrik algoritmalarda her şahsın bir anahtarı vardır. Bir şahsın özel anahtarı, yalnızca kendi kullanımı içindir ve başkalarının eline geçmemesi gerekir. Bu şahsın açık anahtarı ise, bu şahsa mesaj göndermek isteyen herhangi biri tarafından kullanılabilir. Gönderici mesajı, alıcının açık anahtarı ile şifreler. Alıcı, gelen mesajı kendi özel anahtarı ile açar. Mesaj gönderebileceğimiz kullanıcıların sayısı arttıkça, elde etmemiz gereken açık anahtar sayısı da artacaktır. Sistemde 100 kullanıcı varsa, her bir kullanıcının ayrı bir açık anahtarı olacağından, tüm bu açık anahtarlar, erişilebilir olmalıdır. Bu problemde sayısal sertifikalar teknolojisi yardımı ile çözülebilmektedir (Pro-G, 2003).

BÖLÜM 4. KIZILÖTESİ TABANLI GÜVENLİ İLETİŞİM

Kablosuz haberleşmede kızılötesi tabanlı sistem kullanılmasının en önemli nedenlerinden birisi hızlı ve ucuz olmasıdır. Ancak bu sistemler yeteri kadar güvenli değildir. Bu tez çalışmasında kızılötesi sistemlerin güvenliğini arttırmak için ilk olarak SATE isimli yeni bir protokol geliştirilmiştir. Kızılötesi iletişim için varolan protokollerden farklı olarak yeni bir protokolün tasarlanması bile güvenlik için yeterli bir önlemdir. Çünkü protokol kavramı alıcı ile verici arasındaki anlaşma dilidir diyebiliriz.

SATE protokolü kullanılarak verici devresinden gönderilen verilerin alıcı devresine ulaşana kadar istenmeyen kişiler tarafından dinlenebileceği düşünülerek, haberleşme bilgisinin şifrelenmesi amaçlanmıştır. Bunun içinde şifreleme sistemlerinden simetrik anahtarlı şifreleme sistemi tercih edilmiştir. Simetrik anahtarlı sistemler diğer sistemlere nazaran çok daha hızlı çalışırlar ve mikrodenetleyicili sistemlerde kullanılabilirler. Ancak her simetrik şifreleme algoritmasını mikrodenetleyicili sistemde kullanmamız mümkün değildir. Mikrodenetleyicili sistemlerde bellek ve hız problemleri nedeniyle uygun bir şifreleme algoritması seçmek önemlidir. Bu olumsuzluklar düşünerek sistem güvenliği için hem güçlü bir şifreleme yapısına sahip hem de bellekte az yer kaplayan bir algoritmanın tercih edilmesi gerekir. Yeni protokolü daha güvenli hale getirmek için mikrodenetleyici sistemlerin yapısı ve donanımsal kısıtlamaları gözönüne alınarak TEA şifreleme algoritması eklenmiştir. Bu sayede verici devresinden gönderilen bilgiler daha güvenli bir şekilde alıcı devresine yollanabilmektedir.

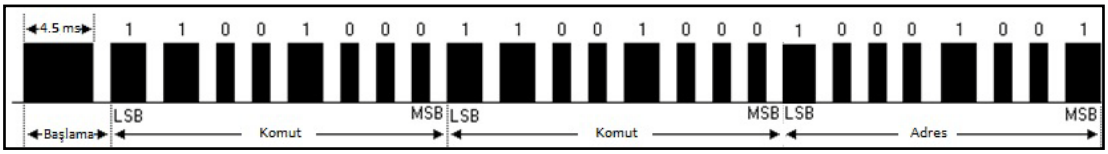
Yukarıda bahsedilen güvenlik duvarlarına ek olarak sisteme bir de kullanıcı arayüzü eklenmiştir. Bu arayüz sayesinde verici devresi istenmeyen kişiler tarafından ele geçirilmiş olsa bile, istenmeyen kişi tanımlı kullanıcı olmadığı için sistemi çalıştıramayacaktır. Tanımlı kişilerin yapmış olduğu girişler ve giriş zamanları

veritabanına kaydedilmektedir. Bu sayede kullanıcı arayüzündeki tanımlı kişiler, yetkili kişi tarafından kontrol edilebilmektedir. Burada yetkili kişi sistemin kim tarafından, ne zaman ve hangi sıklıkla kullanıldığını kontrol ederek sistemin kullanımını denetleyebilir.

Kızılötesi iletişimdeki bu güvenlik önlemlerinin bir arada bulunması kızılötesi tabanlı kablosuz haberleşme yöntemini çok daha güçlü hale getirmektedir. Ayrıca çalışmanın mikrodenetleyici ile gerçekleştirilmesi sistem kullanımını çok geniş alanlara taşımıştır. Sistemin en önemli avantajları; karmaşıklığının az, maliyetinin düşük ve güvenlik seviyesinin oldukça yüksek olmasıdır.

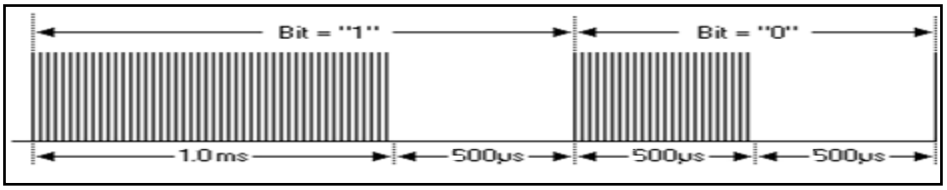
4.1. SATE Protokolü ve Tasarlanan Alıcı Verici Devreleri

SATE protokolü ile kızılötesi iletişimde ilk güvenlik duvarı oluşturulmuştur. Kızılötesi iletişimde standartlardan farklı bir protokolün kullanılması diğer sistemlere nazaran güvenliği arttırmıştır. Varolan protokollerin yapıları genel olarak başlangıç bit uzunluğu, lojik ‘0’ ve lojik ‘1’ durumundaki bit uzunlukları ile komut ve adres bit sayılarından oluşmaktadır. SATE protokolünde de bu temel özellikler değiştirilmiştir.



Şekil 4.1. SATE protokolünün yapısı

Şekil 4.1’de genel yapısı gösterilen SATE protokolünün başlangıç bit uzunluğu 4.5 ms, toplam bit sayısı ise 24 bitdir. 24 bitden ilk 16 bit komut bilgisini, kalan 8 bit ise adres bilgisini ifade etmektedir.



Şekil 4.2. SATE protokolünde veri iletişimi (Modülasyon)

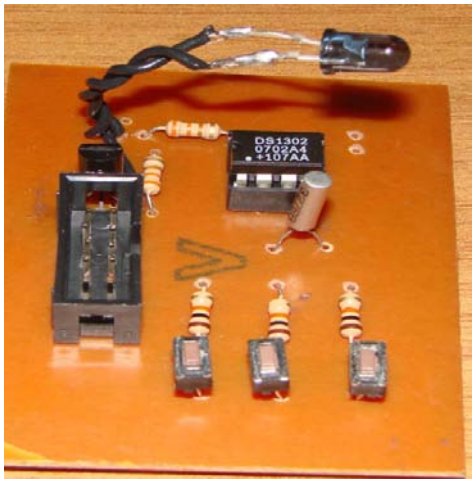
Her başlangıç bitinden sonra gelen lojik ‘1’ ve ‘0’ lar, Şekil 4.2’de görüldüğü gibi diğer protokollerden farklı olarak değiştirilmiştir. Lojik ‘1’ durumundaki bitler 1 ms, lojik ‘0’ durumundaki bitler 0.5 ms ve bekleme süreleri ise 0.5 ms olarak düzenlenmiştir.

İletişim esnasında gerçekleştirilen işlemleri yani verici devresinden alıcı devresine bilgiyi gönderip anlamlı hale getirme işlemlerini somut olarak açıklamak için Şekil 4.1’den faydalanabiliriz. Verici devresinden Şekil 4.1’deki gibi bir sinyal üretirsek göndermek istediğimiz komut bilgileri 0xC8 ve 0xC8, adres bilgimiz yani cihaz bilgisi (ID no) 0x89 olarak ayarlanmış olur. Eğer sonradan da tekrar veri göndermek istersek her baytda başlangıç biti 4.5 ms olarak gönderilir. Mikrodenetleyicide istenilen lojik ‘1’ ve lojik ‘0’ lar ayarlandıktan sonra Şekil 4.3’de görülen verici modül devresindeki IR LED’e aktarılan bilgi seri olarak alıcı devresine gönderilir.

Alıcı devresinde öncelikle IR sinyalin olup olmadığı kontrol edilir. Eğer sinyal varsa program alt rutinleri çalışmaya başlar. Sinyal geldiğinde başlangıç bitinden başlayarak toplam 24 bit lojik ‘1’ ve lojik ‘0’ alınmış olması gerekir. Bu şekilde bir sinyal alınmamışsa protokol hatalıdır ve sistem resetlenir. İletişim gerçekleşemez. Yeni ve farklı bir protokolün avantajı ise burada ortaya çıkmaktadır. Varolan protokollerde başlangıç bit uzunluğu ve diğer temel özellikler bilindiğinden alıcı devresi varolan protokollere göre tasarlanabilir. Ama geliştirilen protokolün özelliklerini geliştiren kişiden başkası bilmediğinden ona uygun bir alıcı devresi tasarlanamaz ve dolayısıyla iletişim gerçekleştirilip sistem çalıştırılamaz.

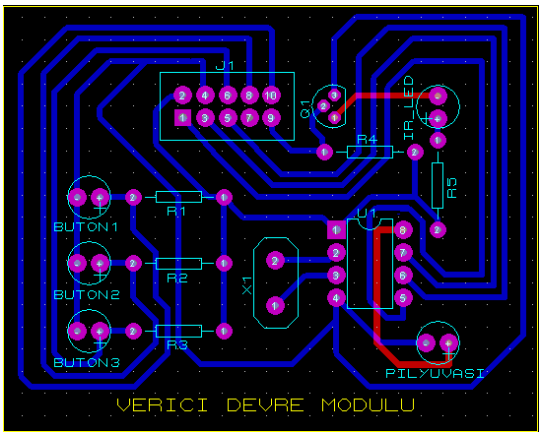
Sinyal alındığı zaman bir sayıcı devreye girer ve sinyal kesilene kadar saymaya devam eder. Sinyal kesilip sayma bittiğinde sayıcının değerine göre fonksiyonlara girilip işlemler icra edilir. Eğer gelen sinyal başlangıç bitine karşılık gelen bir değere

kadar sayılmışsa başlangıç bit fonksiyonu çalıştırılır. Lojik ‘1’ kadar sayılmışsa lojikbit ‘1’, lojikbit ‘0’ kadar sayılmışsa lojik ‘0’ fonksiyonuna girilerek gerekli işlemler yapılır. Toplam 24 bit olduğu için lojik ‘1’ ve lojik ‘0’ fonksiyonlarının olduğu kısım 24 kez çalıştırılır. Eğer 1 startbiti ve tam 24 bit gelmemişse protokol hatalıdır. Eğer gelen sinyal 1 startbiti ve 24 bitden oluşuyorsa işlem yapılır ve alınan bitler bir dizi işlemden geçirilerek komut ve adres bilgileri elde edilir. Belirlenen süre içerisinde sinyalde kesinti olursa veya yanlış bilgi gelirse sistem resetlenmektedir.



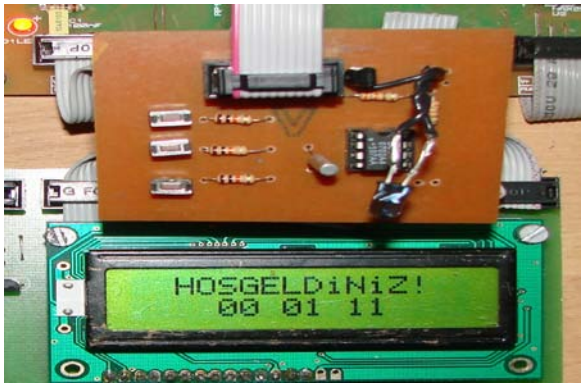
Şekil 4.3. Verici modül devresi

Yukarıdaki şekilde verilen verici devre modülünün baskı devre çizimi Şekil 4.4’de görüldüğü gibidir.



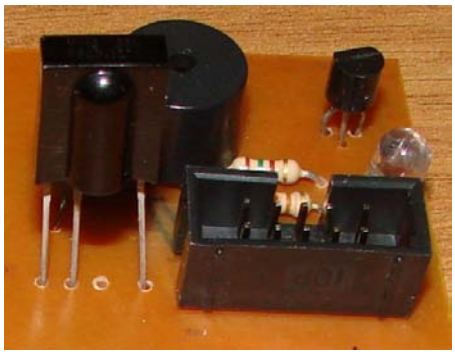
Şekil 4.4. Verici modül baskı devresi

Şekil 4.3 ve Şekil 4.6'da gösterilen verici ve alıcı devreleri ayrı modül olarak tasarlanmıştır. Verici ve alıcı modül kartları, 10'lu data kablo yardımıyla kolaylıkla mikrodenetleyici kartına bağlanarak sistem çalıştırılabilir. Modül kartlarından bahsedecek olursak; verici modül kart da kızılötesi iletişimi sağlamak için gerekli olan IR LED ve Şekil 4.5'deki gibi gerekli yerlerdeki zamanlama ile ilgili işlemler için DS1302 entegresi ile zaman parametrelerini düzenlemek için butonlar bulunmaktadır.



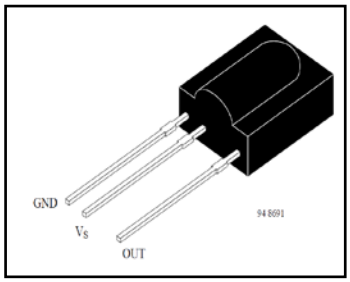
Şekil 4.5. DS1302 entegresi ile saat, dakika ve saniye

Şekil 4.6'da görülen alıcı modül kartında ise, TSOP1236 alıcı entegresi, led ve buzzer bulunmaktadır. Entegreye bağlı olan led, sinyalin olduğu durumlarda yanıp sönerek sinyalin olduğunu gözle görebilmemizi sağlamaktadır. Buzzer ise gelen bilginin doğru veya yanlış olduğunu sesli olarak ifade etmektedir.



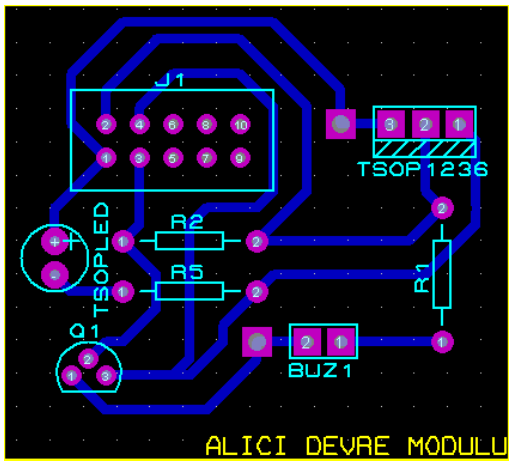
Şekil 4.6. Verici modül baskı devresi

Verici devresinden gönderilen sinyaller Şekil 4.7'deki (Vishay Telefunken, 2001) alıcı entegresinin OUT ucu ile alınarak mikrodenetleyicide anlamlı hale getirilmektedir. Gelen sinyaller doğru ise buzzer gelen bilginin doğru olduğunu belirten kesikli bir ses çıkarmaktadır. Eğer yanlış ise veya sinyalde kesinti olup belli bir süre sinyal alınamıyorsa buzzer bir problem olduğuna dair uzun süreli kesiksiz bir uyarı sesi vermektedir.

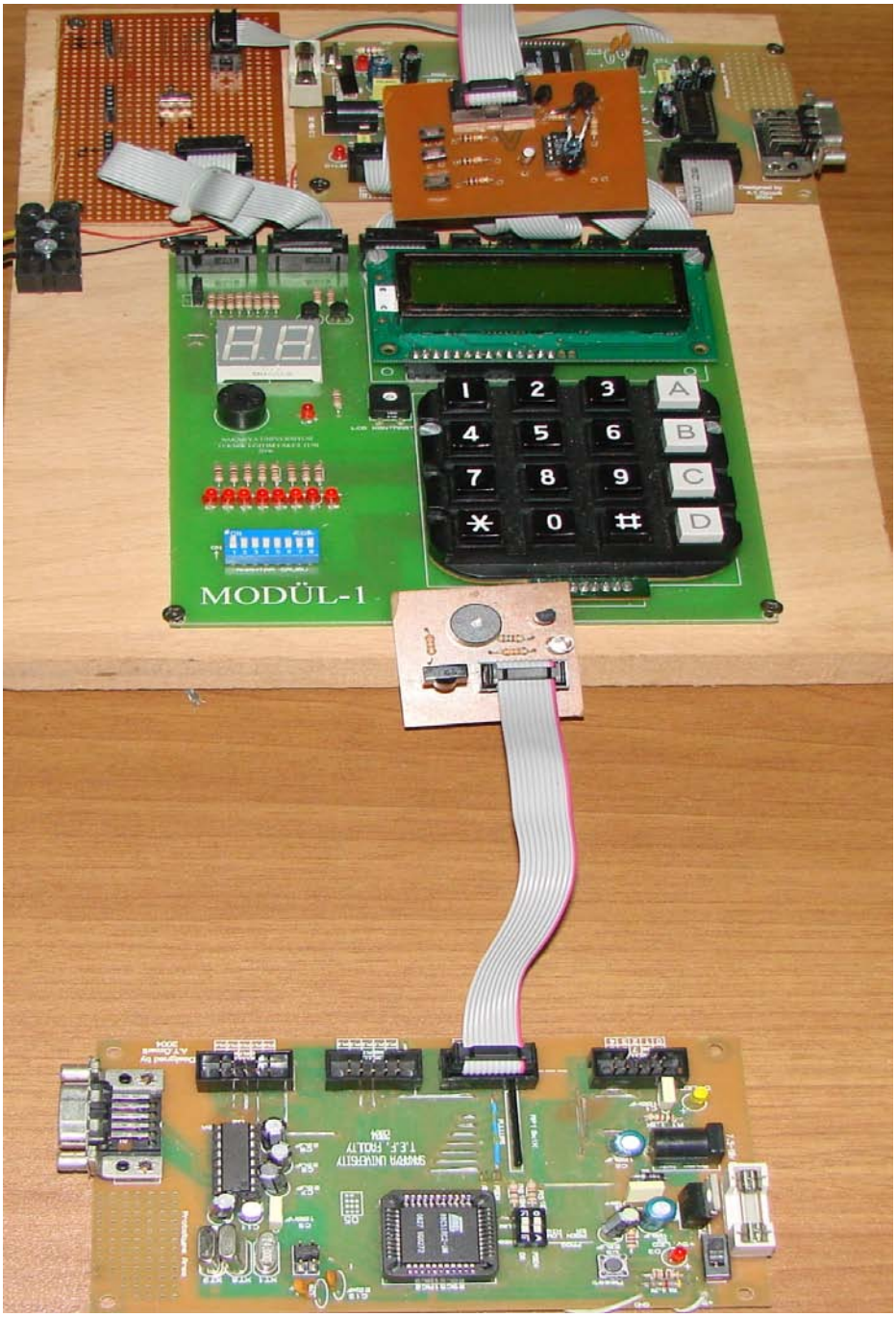


Şekil 4.7. TSOP12XX entegresi ayak bağlantıları

Tasarlanan alıcı devre modülünün baskı devre çizimi Şekil 4.8'de görüldüğü gibidir. Alıcı entegresi, vericiden gelen sinyalleri kesintisiz alabilmesi için kartın kenarına yerleştirilmiştir.



Şekil 4.8. Verici modül baskı devresi



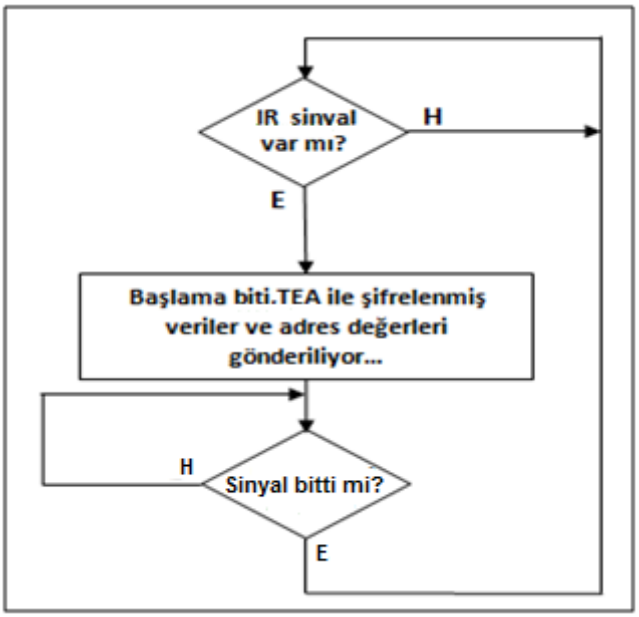
Şekil 4.9. Alıcı ve verici devre modülleri ile mikrodenetleyici kartları

Şekil 4.9'da gösterilen alıcı ve verici devrelerin çalışma mantığı şu şekildedir.

Kullanıcı panelinden şifre girilip onay tuşuna basıldığında IR LED'e 36 kHz frekanslı kare dalga sinyal uygulanır. LED'den geçen akım darbeleri sayesinde

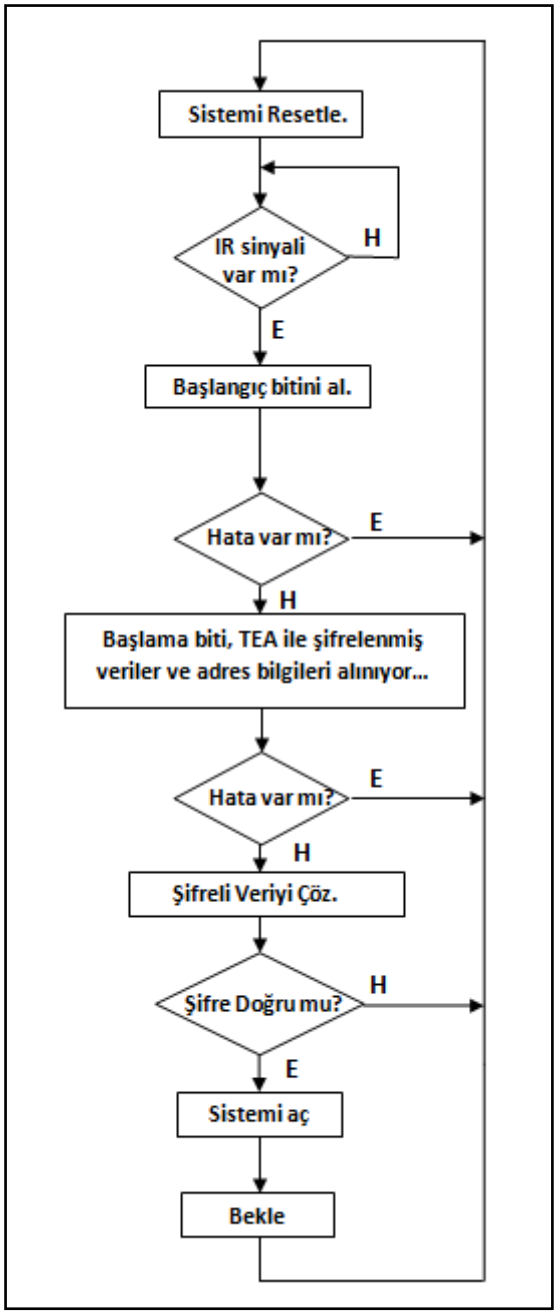
ortama kızılötesi ışın demeti gönderilmiş olur. IR LED'in ortama yaydığı kızılötesi ışınlar alıcı devresinde bulunan IR alıcı modül tarafından algılanır.

Alıcı modül üzerine 36 kHz frekanslı kızılötesi sinyal ulaştığında, alıcının 3 nolu (OUT) çıkış ucunda lojik '0' seviyesi görülür. Alıcıya herhangi bir kızılötesi sinyal ulaşmadığında ise çıkış ucu lojik '1' seviyesindedir. Böylece alıcı modülün çıkış geriliminin seviyesine bakılarak vericiden herhangi bir sinyalin gönderilip gönderilmediği anlaşılabilir (Erol, 2004).



Şekil 4.10. IR haberleşme verici devre algoritması

Şekil 4.10'daki akış diyagramından da görüldüğü gibi haberleşme sisteminin çalışması için öncelikle verici devresinden butona basılıp bir IR sinyali gönderilmelidir. Verici devresinde butona basıldıktan sonra IR sinyali ile istenilen veri şifrelenmiş olarak alıcı devresine yollanır.



Şekil 4.11. IR haberleşme alıcı devre algoritması

Şekil 4.11'deki alıcı devre algoritmasında alıcı devresi ilk olarak her zaman sinyalin olup olmadığını kontrol etmektedir. Eğer sinyal varsa yazılımda gerekli fonksiyonlar çalıştırılmaya başlanır. Öncelikle başlangıç biti fonksiyonu aktif edilerek başlangıç bitinin süresi kontrol edilir, hata varsa sistem resetlenir, yoksa sistem çalışmasına devam ederek bir diğer fonksiyona atlanır. Başlangıç bitinden sonra gelen '1' ve '0' bitlerinin süreleri ile gelen toplam bit sayısı kontrol edilip anlamlı hale getirilir ve

şifre çözme algoritması ile gelen bilgi çözülerek sistemdeki gerçek bilgi ile karşılaştırılır. Eğer yanlışlık varsa sistem resetlenir, problem yoksa sistem aktif edilir.

SATE protokolü ve diğer protokoller arasındaki temel farklar (başlangıç bit uzunluğu, frekans, lojik '1' ve lojik '0' durumundaki bit uzunlukları, toplam bit sayısı) aşağıdaki tabloda görülmektedir.

Tablo 4.1. SATE protokolü ile diğer protokollerin karşılaştırılması

	SATE	Sony (SIRC)	Sharp	Nec	Nokia
Başlangıç bit uzunluğu (ms)	4,5	2,4	0	9 + 4,5	4
Frekans (kHz)	36	40	38	38	38
Toplam bit sayısı	24	12	13	32	16
Lojik 1 iken bit uzunluğu(ms)	1	1,2	2	2,25	1
Lojik 0 iken bit uzunluğu(ms)	0,5	0,6	1	1,12	1

SATE protokolü, standart protokollerden olmadığından, sadece geliştirilen alıcı devresi ve geliştirilen verici devresi ile çalışacaktır.

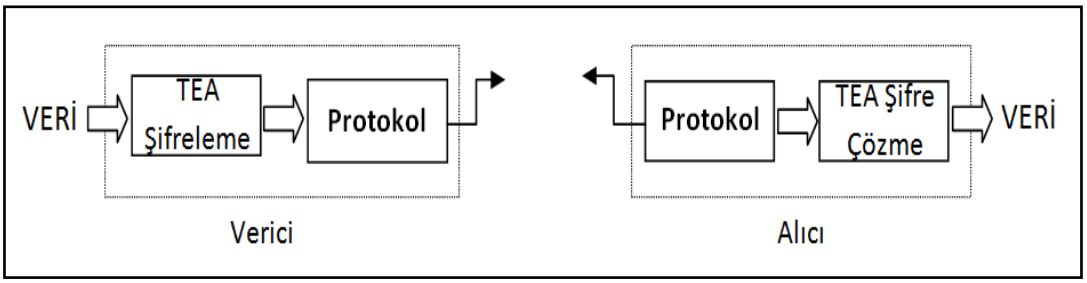
4.2. SATE Protokolü ile TEA Şifreli Haberleşme

SATE protokolü ile vericiden yollanan verilerin daha güvenli olarak alıcıya ulaşması ve verilerin şifresiz haliyle istenmeyen kişilerin eline geçebileceği düşüncesiyle gönderilecek verilerin şifrelenmesine gerek duyulmuştur. Kızılötesi haberleşmede iletişim hızı oldukça yüksektir. Sistemin hızı düşünülerek şifreleme simetrik şifreleme yöntemleriyle yapılmıştır. Simetrik şifreleme diğer şifreleme yöntemlerine göre daha hızlı ve maliyet olarak daha ucuzdur.

Simetrik şifrelemede birçok farklı algoritma bulunmaktadır. Mikrodenetleyicili sistemler üzerinde çalışılmak isteniyorsa seçilmesi gereken algoritmanın bellekte az yer kaplaması ve güvenli bir şifreleme olabilmesi için güçlü bir şifreleme algoritması olması gerekmektedir.

Simetrik şifrelemede blok şifreleme algoritmalarından olan TEA, çok kısa olan kod uzunluğu ve basit algoritması sayesinde özellikle sınırlı kod uzunluğuna sahip gömülü sistemlerde oldukça popüler olan bir şifreleme algoritmasıdır (Udea, 2010). Bu sebeple mikrodenetleyicili sistemlerde ve bellek sıkıntısı olan yerlerde tercih edilen bir şifreleme algoritmasıdır. Bu nedenle tez çalışmasında bu algoritma tercih edilmiştir. TEA var olan en hızlı ve en etkili algoritmalardan birisidir. Özellikle hafızada kaplanan yeri minimize etmek ve hızı maksimize etmek için geliştirilmiş bir algoritmadır.

TEA en güvenli algoritmalardan biridir. Massey ve Xuejia Lai tarafından tasarlanan IDEA algoritması kadar güvenli olduğu söylenebilir. IDEA'da kullanılan aynı karışık cebirsel grupları kullanmasına rağmen daha basit ve daha hızlıdır. Bununla birlikte TEA hiçbir kuruma ait olmamasına rağmen IDEA, İsviçre'de bulunan Ascom-Tech AG tarafından patentlenmiştir.



Şekil 4.12. Geliştirilen protokol ile TEA şifreli haberleşme

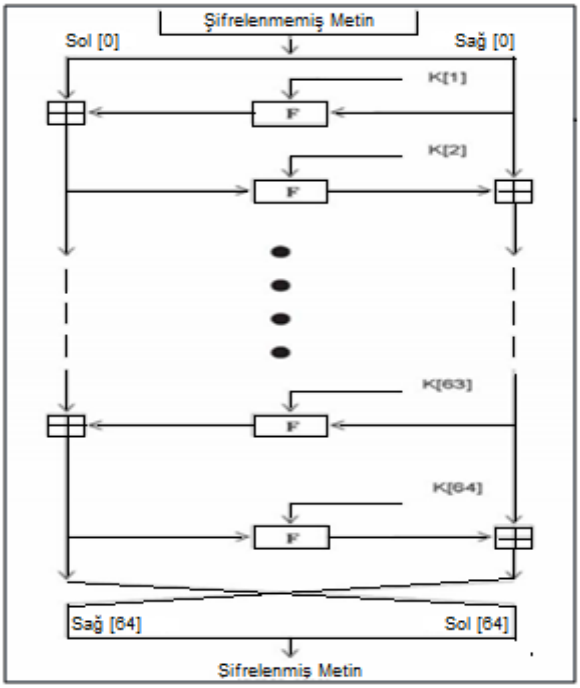
Verilerin güvenli bir şekilde gönderilebilmesi için Şekil 4.12'deki blok diyagramda görüldüğü gibi gerçek veriler öncelikle verici devresinde TEA ile şifrelenip, şifrelenen veriler protokole aktarılıp IRLED ile alıcı devresine gönderilir. Alıcı devresinde de öncelikle gelen sinyallere göre protokol analizi yapılıp veriler düzenlenerek şifre çözme işlemi gerçekleştirilerek gerçek veriler elde edilmiş olur.

4.2.1. TEA şifreleme yapısı

Bir sonraki sayfada C dilinde yazılmış TEA şifrelemesine ait bir fonksiyon bloğu görülmektedir (Wheeler ve Needham, 1994). Burada programın diğer fonksiyonlarından alınan şifrelenmemiş 2 adet sekizer bitlik veri, v[0] ve v[1]'de depolanmaktadır. Fonksiyon çalıştığında v[0] ve v[1] verileri y ve z değişkenlerine atılmaktadır. Altın sayı oranı dediğimiz sabit delta sayısı ve döngü sayısı while döngüsüne girmeden önce tanımlanmıştır. Döngü içerisinde ise bir takım işlemlerden sonra veriler şifreli hale getirilir. 128 bit olan k anahtar algoritması 32 bitlik 4 bloğa bölünerek şifreleme işlemi yapılmıştır (k[0], k[1], k[2], k[3]). Bu algoritma kod boyutunun çok az olması nedeniyle yazılımda DES algortimasının yerine kullanılabilir.

```
void code(long* v, long* k)  {
unsigned long y = v[0], z = v[1], sum = 0,
delta = 0x9e3779b9, n = 32 ;
while (n-->0) {
  sum += delta ;
  y +=  (z<<4)+k[0] ^ z+sum ^ (z>>5)+k[1] ;
  z +=  (y<<4)+k[2] ^ y+sum ^ (y>>5)+k[3] ;
     }
 v[0] = y ; v[1] = z ; }
```

Fonksiyon sonlandığında şifreleme tamamlanarak y ve z değerleri elde edilir. Elde edilen bu değerler v[0] ve v[1] değişkenlerine atılarak şifrelenmiş olan veriler elde edilmiş olur. Şifrelenmiş olan v[0] ve v[1] değerleri IR LED ile karşı tarafa yollanır.



Şekil 4.13. TEA şifreleme yapısı

Algoritmanın şifreleme yapısı Şekil 4.13'de (Andem, 2003) görüldüğü gibidir. Bu yapıyı bir önceki sayfadaki şifreleme kodlarının şekle dökülmüş haline benzetebiliriz. Şifrelenmemiş olan veri döngü içerisine sokularak anahtarlar yardımıyla gerekli işlemlere tabi tutularak döngü sonunda gerçek veriler şifrelenmiş olarak elde edilmiş olur.

4.2.2. TEA şifre çözme yapısı

TEA şifre çözme işleminin C dilindeki yazılışı aşağıdaki fonksiyon bloğunda görüldüğü gibi olacaktır (Wheeler ve Needham, 1994). Kod çözme aslında temel olarak şifreleme süreci ile aynıdır. Genel olarak sadece işlemlerin tersi yapılıyor denilebilir. Basit olarak şifreleme fonksiyonunda toplama işlemi yapılıyorsa, şifre çözme işleminde de çıkarma işleminin yapılması gerekmektedir. TEA yapısında da dikkat edilirse şifreleme işlemindeki döngü içerisinde y ve z değişkenleri toplanmaktayken, şifre çözme işleminde çıkarma işlemi yapılmaktadır. Aynı şifre çözme işleminde olduğu gibi öncelikle v[0] ve v[1] verileri y ve z değişkenlerine atılmakta, döngü sonunda ise y ve z verileri tekrar v[0] ve v[1] değişkenlerine

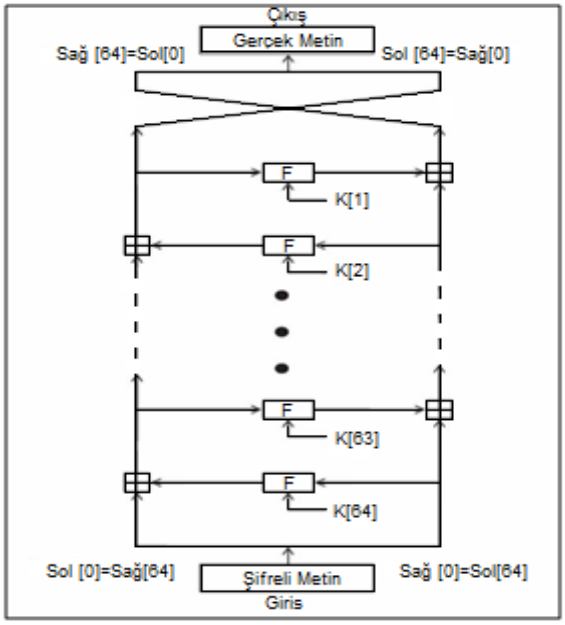
atılmaktadır. Şifreleme sonundaki v[0] ve v[1] değişkenleri şifreli veriler iken, şifre çözme işlemi sonundaki v[0] ve v[1] verileri gerçek yani ham metindir.

```
void decode(long* v, long* k)  {
 unsigned long n = 32, sum, y = v[0], z = v[1],
 delta = 0x9e3779b9 ;
 sum = delta<<5 ;

 while (n-->0) {
 z - = (y<<4)+k[2] ^  y+sum ^ (y>>5)+k[3] ;
 y -= (z<<4)+k[0] ^ z+sum ^ (z>>5)+k[1] ;
 sum -= delta ;  }

    v[0] = y ; v[1] = z ;  }
```

Şekil 4.14'de (Andem, 2003) gösterilen şifre çözme yapısı dikkat edilirse Şekil 4.13'de yapılan işlemlerin tersidir. Bu sefer şifrelenmiş veri döngü içerisine sokularak yukarıdaki şifre çözme kodlarında olduğu gibi şifreleme kodlarında yapılan işlemlerin tersi yapılarak gerçek veri çıkış olarak elde edilmiş olur. Anahtar, şifreleme ve şifre çözme işlemlerinde bloklar halinde her zaman sabit kalmaktadır.



Şekil 4.14. TEA şifre çözme yapısı

4.2.3. SATE protokolü ve TEA ile yüksek güvenlikli kızılötesi iletişim uygulaması

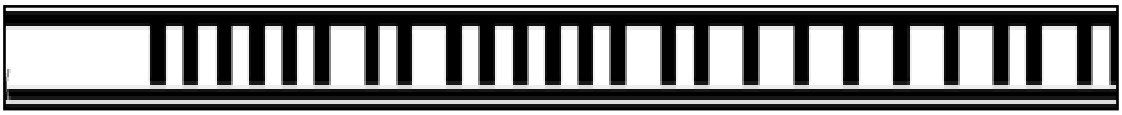
Geliştirilen sistemde TEA'nın kullanılmasının en önemli nedenlerinden birisi algoritmanın güçlü şifreleme yapısına sahip olması ve bellekte az yer kaplamasıdır. Bellekte az yer kaplaması sistemde mikrodenetleyici kullanılmasına olanak sağlamıştır. Günümüzde neredeyse her uygulamada mikrodenetleyiciler kullanıldığından TEA şifreleme algoritması çok geniş kullanım alanına sahiptir. Daha güçlü şifreleme algoritmalarının kızılötesi kablosuz haberleşmede kullanılması güvenilirliği arttıracağından bu algortimalar sistemleri daha da güvenli bir hale gelecektir.

SATE protokolündeki verilerin blok algoritma şifreleme türlerinden olan TEA ile şifrelenebilmesi için protokoldeki bit sayıları şifrelemedeki bit sayı oranına göre belirlenmiştir.

Normalde standart bir TEA şifrelemesinde 64 bitlik bloklar kullanır. Bu 64 bit veri bloğu 128 bitlik anahtar ile şifrelenmektedir. Veriler v[0] ve v[1] de depolanır. 128 bitlik anahtar ise 32 bitlik bloklar haline bölünerek K={k[0], k[1], k[2], k[3]} şeklinde depolanmaktadır. TEA şifreleme algoritmasının geliştirdiğimiz protokole uygun olabilmesi için anahtar bilgisi 32 bit, veri bilgisi ise 16 bit olarak değiştirilmiştir. 32 bit anahtar bilgisi TEA'da olduğu gibi yine 4 bloğa ayrılarak k[0], k[1], k[2] ve k[3] şeklinde 8'er bitlik hale getirilmiştir. 16 bit olan veri bilgisi ise 2 blok halinde v[0] ve v[1] değişkenlerinin içine atılarak şifreleme işlemi gerçekleştirilmiştir.

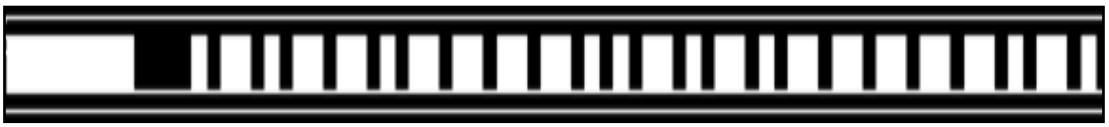
Şifreleme işlemi aşağıdaki şifreleme fonksiyonunda görüldüğü gibi yapılmaktadır (Wheeler ve Needham, 1994). V[0] ve v[1] içine atılan veri bilgileri fonksiyon çalıştırıldıktan sonra bilgileri tutması amacıyla farklı değişkenlere atılarak 32 bitlik anahtar yardımıyla şifrelenir. Şifreleme işlemi sonunda geçici olarak farklı değişkenlere atılan veri bilgileri tekrar v[0] ve v[1] değişkenlerine atılarak şifrelenmiş olan veri IR LED ile alıcı tarafına gönderilmeye hazır hale gelmiş olur.

```
void code(long* v, long* k)  {
unsigned long y = v[0], z = v[1], sum = 0,
delta = 0x9e3779b9, n = 32 ;
while (n-->0) {
 sum += delta ;
 y +=  (z<<4)+k[0] ^ z+sum ^ (z>>5)+k[1] ;
 z +=  (y<<4)+k[2] ^ y+sum ^ (y>>5)+k[3] ;
    }
v[0] = y ; v[1] = z ; }
```



Şekil 4.15. SATE protokolünde TEA ile şifrelenmemiş veri (0x05 ve 0x05)

Şekil 4.15'deki protokolün yapısı incelendiğinde başlangıç bitinden sonraki 16 bit şifrelenmemiş komut bilgisini göstermektedir. Daha sonraki 8 bit ise adres bilgisidir. Verici devresindeki şifreleme işlemi sonucu 8 bitlik bloklar haline getirilen v[0] ve v[1] veri bilgileri protokoldeki 16 bitlik komut bilgisi içine atılarak, adres bilgisiyle birlikte toplam 24 bit olarak IR LED ile alıcı devresine şifrelenmiş şekilde yollanmaktadır. Şekil 4.15'de şifrelenmemiş hali gösterilen veri bilgisi, Şekil 4.16'da ise şifrelendikten sonra aradaki dinleyici veya istenmeyen kişi tarafından dinlenen protokoldeki şifrelenmiş veriler görülmektedir.



Şekil 4.16. SATE protokolünde TEA ile şifrelenmiş veri (0x5B ve 0xCA)

Verici devresinden gönderilen 24 bit komut ve adres bilgileri alıcı devresine alındıktan sonra elde edilen veriler şifre çözme işlemine tabi tutulmaktadır. Şifre çözme işlemi bir sonraki sayfada görülen fonksiyona göre yapılmaktadır (Wheeler ve

Needham, 1994). Alıcı devresindeki şifre çözme fonksiyonunda da veri bilgileri öncelikle v[0] ve v[1] değişkenlerine bölünür. Bölünmüş olan veri bilgileri geçici olarak farklı değişkenlere atılarak 32 bit anahtar yardımıyla döngü içerisindeki işlemler yapılarak gerçek veri elde edilmiş olur. Anahtar her zaman olduğu gibi şifreleme ve şifre çözme işlemlerinde sabit kalmaktadır, buradaki tek farklılık anahtarın parçalanarak bloklar halinde kullanılmasıdır.

```
void decode(long* v, long* k)  {
 unsigned long n = 32, sum, y = v[0], z = v[1],
 delta = 0x9e3779b9 ;
 sum = delta<<5 ;

 while (n-->0) {
 z - = (y<<4)+k[2] ^  y+sum ^ (y>>5)+k[3] ;
 y -= (z<<4)+k[0] ^ z+sum ^ (z>>5)+k[1] ;
 sum -= delta ;  }

    v[0] = y ; v[1] = z ;  }
```

Şifre çözme fonksiyonu sonucunda, orijinal bilgi v[0] ve v[1] değişkenlerinde elde edilmiş olur. Son olarak elde edilen gerçek veriler şifre doğrulama işlemine tabi tutularak hata yoksa sistem çalıştırılır. Sinyal kesintiye uğrayıp belli bir süre istenen bilgiler alınamazsa veya yanlış bilgiler gelirse sistem çalışmayarak resetlenecektir. Verilerin değiştirilip şifrelenerek kızılötesi iletişim sağlanması sistemi oldukça güvenli kılmaktadır.

4.3. İletişim Sisteminin Kullanıcı Arayüzü

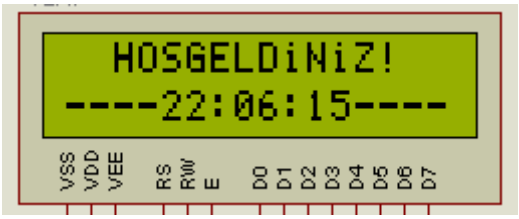
Kablosuz ortam kızılötesi haberleşmede son güvenlik önlemi olarak sisteme kullanıcı arayüzü eklenmiştir. Kullanıcı arayüzünün eklenmesiyle verici devresi istenmeyen kişiler tarafından ele geçirilse bile sistemde tanımlı olan kullanıcı şifreleri bilinmediğinden sistem aktif hale getirilip çalıştırılamayacaktır. Kullanıcı arayüzü sayesinde sistem hem daha kullanışlı, hem de daha güvenli hale gelmiştir.

Kullanıcı arayüzü, yönetici ve kullanıcı panellerinden oluşmaktadır. Sistemde ne kadar kullanıcı tanımlıysa iletişimi o kadar kullanıcı sağlayarak sistemi aktif hale getirebilir. Sistemde önceden tanımlı olan yönetici hangi kullanıcının, ne zaman, hangi sıklıkla sistemi aktif ettiğini yönetici panelinden öğrenebilir.

Sistemi kullanan kişilerin sistemi ne zaman aktif ettiklerinin veritabanına kaydedilebilmesi ve saatin her an kontrol edilebilmesi için gerçek zaman saati (RTC) kullanılmıştır. Sistemdeki saat ve dakika bilgileri DS1302 RTC entegresiyle elde edilmektedir. Bu entegre sayesinde sistemin enerjisi kesilse bile entegreye bağlı olan pil sayesinde entegre çalışmaya devam ederek zaman bilgisini saklayacaktır. Bu sayede sistem ne zaman aktif edilirse edilsin zaman bilgisi sisteme kaydedilip yönetici tarafından kullanıcıların sistemi ne zaman akullandıkarı öğrenilebilecektir.

4.3.1. Yönetici paneli

Yönetici panelinden kullanıcıların sistemi ne zaman, hangi sıklıkla aktif ettikleri istenilen zamanda kontrol edilebilir.



Şekil 4.17. Ana ekran

Şekil 4.17'de gösterilen ana ekranda klavyeden bir tuşa basılmasıyla aşağıdaki Şekil 4.18'de görüldüğü gibi yönetici ve kullanıcı paneli seçeneklerinden oluşan bir ekran açılacaktır.

Şekil 4.18. Yönetici ve kullanıcı paneli

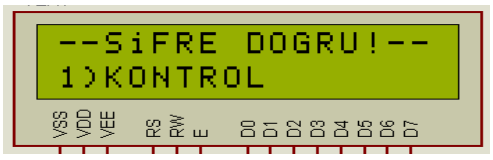
Yönetici paneline girip kullanıcıları kontrol etmek için klavyenin “1” tuşuna bastığımızda Şekil 4.19’da verilen yönetici paneli giriş ekranı görülecektir.

Şekil 4.19. Yönetici paneli şifre ekranı

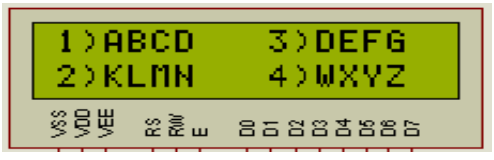
Klavyeden şifre girilip “#” tuşuna basıldıktan sonra girilen şifre sistem tarafından kontrol edilir.

Şekil 4.20. Yönetici paneli şifre kontrol ekranı

Şifre doğru girilmişse şifrenin doğruluğunu teyit amaçlı Şekil 4.21’de gösterilen bilgilendirme ekranı açılır. Burada “1” tuşuna basıldığında kullanıcı kontrol işlemleri için gerekli olan Şekil 4.22’deki ekrana geçiş yapılmaktadır.

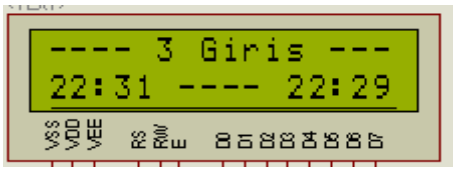


Şekil 4.21. Doğru şifre ara bilgi ekranı



Şekil 4.22. Kullanıcı Bilgileri Kontrol Ekranı

Ekrana çıkan kullanıcı isimleri sayesinde istenen kullanıcının sistemi ne zaman, kaç kere kullandığı öğrenilebilir. Şekil 4.23, 4.24 ve 4.25 de bazı kullanıcıların örnek kontrol ekranları bulunmaktadır.



Şekil 4.23. ABCD kullanıcısı bilgileri

Örnek kontrol ekranları incelenecek olursa, Şekil 4.23 ABCD kullanıcısının sistemi 3 kere kullandığı ve son 2 kullanışının saat 22.31 ve 22.29'da olduğunu göstermektedir.

Şekil 4.24. KLMN kullanıcısı bilgileri

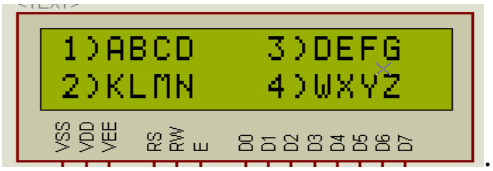
Şekil 4.24'de KLMN kullanıcısının sistemi 1 kere, saat 22.29'da kullanığını, Şekil 4.25 ise DEFG kullanıcısının sistemi hiç kullanmadığını göstermektedir.

Şekil 4.25. DEFG kullanıcısı bilgileri

4.3.2. Kullanıcı paneli

Kişiler kendi adlarına tanımlı olan kullanıcı adı ve şifresini kullanarak bu panelden sistemi aktif edebilirler. Sistemde kayıtlı olmayan kullanıcılar alıcı devresini aktif edemezler. Yönetici panelinde olduğu gibi Şekil 4.17'deki ana ekrandan bir tuşa

basıldığında Şekil 4.18'deki menü açılır. Kullanıcı panelini aktif etmek için klavyeden "2" tuşuna basılırsa Şekil 4.26'daki ekran açılacaktır.



Şekil 4.26. Kullanıcı ekranı

Ekranda görülen kullanıcı isimlerinden birini seçmek için klavyeden istenen kullanıcı seçilerek o kullanıcıya ait olan numara tuşlanır. Her kullanıcı için farklı şifre tanımlı olduğundan sistemi aktif edebilmek için seçilen kullanıcının şifresi doğru girilmelidir. Bu çalışmada 4 kullanıcı tanımlanmıştır. İstenildiği takdirde kullanıcı sayısı arttırılabilir.

Kullanıcı seçimi yapıldıktan sonra Şekil 4.27 ve Şekil 4.28'de görüldüğü gibi ekranlar açılacaktır. Açılan ekranda sistemi aktif etmek isteyen kullanıcın, birinci satırda kendisi adına tanımlı ismi, ikinci satırda ise şifresini girmesi için gerekli olan alan açılmaktadır.

Şekil 4.27. ABCD kullanıcısı şifre ekranı

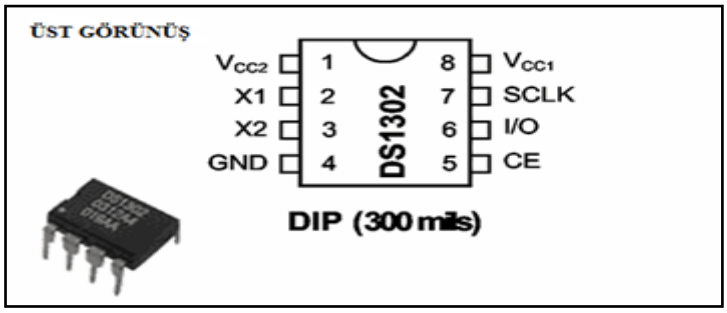
Şekil 4.28. WXYZ kullanıcısı şifre ekranı

Şifre doğru girildiği takdirde Şekil 4.29'deki ekran görüntülenecektir. Şifre doğru girildiği için alıcı devresini aktif etmek için gerekli olan sinyal karşı tarafa TEA ile şifrelenmiş olarak gönderilip alıcı devre kısmında da herhangi bir problem oluşmazsa sistem aktif edilmiş olacaktır.

Şekil 4.29. Kullanıcı doğru şifre ekranı

4.3.3. Gerçek Zaman Saati (Real Time Clock – RTC)

Sistemin zaman bilgisi RTC DS1302 entegresi ile elde edilmektedir. Sistemi çalıştırabilmek için yazılımda RTC başlık dosyası tanımlanması gerekmektedir. Gerekli olan zaman bilgileri bu dosyadaki veriler yardımıyla elde edilebilir. Entegrenin üstden görünüşü ve ayak bağlantıları ise Şekil 4.30'da (Maxim, 2005) olduğu gibidir.

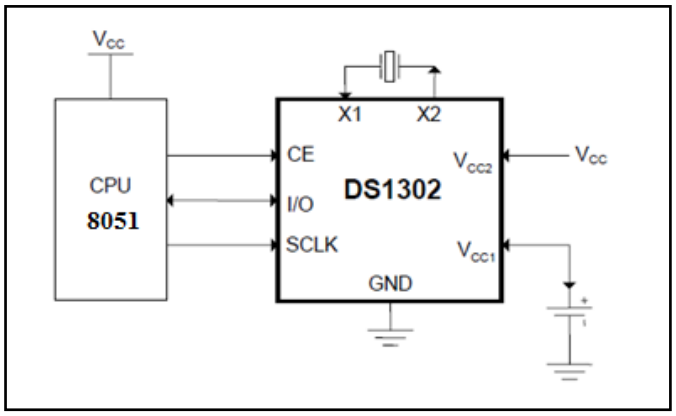


Şekil 4.30. Entegrenin üstden görünüşü ve ayak bağlantıları

DS1302 entegresi; RTC, takvim ve 31 baytlık pil korumalı RAM'e sahiptir. DS1302 entegresi mikrodenetleyici ile senkron seri haberleşme yoluyla iletişimi sağlar. Haberleşmeyi sağlayan üç tane önemli pin vardır. Bunlar CE (Chip Enable), I/O ve SCLK (serial clock) pinleridir. Mikrodenetleyici haberleşmeyide bu uçlar yapar. Seri clock (SCLK) ucu, seri ara yüzde senkronize olarak verileri taşır. I/O ucu, üç kablo ara yüzü ile iki yönlü veri ucudur. CE (Chip enable) ucu, saat veya RAM'den veri

okuma yada veri yazma için kullanılır. Gerçek zaman saati (RTC) saniyeyi, dakikayı, saati, günü, ayı, yılı, haftanın gününü sayar ve 2100 yılına kadar ki tarih bilgileri ile yüklüdür. Örneğin ayın sonunda tarihi otomatik olarak bir sonraki aya ayarlarlayabilir. Aynı şekilde saat bilgisini de 24 saat formatında veya 12 saat AM/ PM formatında üretir. 2 V ve 5 V gerilimle çalışabilir. TTL ile uyumludur (Vcc=5V). 2 V'da 300 nA'den daha az akım tüketebilir. Saat ve RAM hafızasına yazma ve okuma için seri olarak okuma ve yazma işlemi yapabilme moduna sahiptir. - 40^{o}C ile + 85^{o}C arasında çalışabilir. (Taştan, 2005).

Şekil 4.31'de (Maxim, 2005) gösterilen pin uçlarından CE ucu, DS1302 yani RTC entegresinin aktif olmasını sağlar. Clock sinyalini üretmek için X1, X2 uçları kullanılarak RTC ye 32768 KHzlik bir kristal bağlanır (Aslan, 2008).

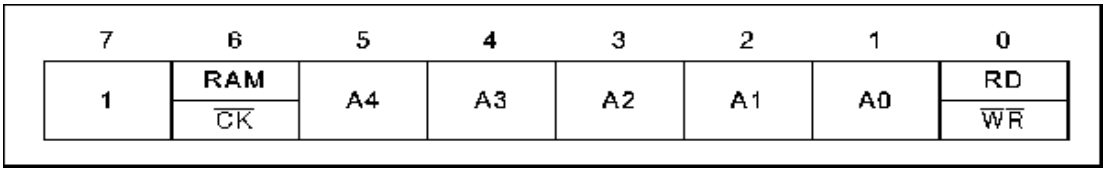


Şekil 4.31. DS1302 (RTC) entegresinin bağlantı şekli

DS1302'nin iki farklı besleme giriş ucu (V_{CC1} ve V_{CC2}) vardır. Bu uçlardan bir tanesine bağlanan bir pil vasıtasıyla devreye enerji verilmediğinde dahi DS1302 saat ve zaman bilgilerini hafızasında tutmaya devam eder. V_{CC1}, V_{CC2} + 0.2 V olduğunda DS1302 beslemesini V_{CC1} üzerinden yapar. Aynı şekilde V_{CC2}, V_{CC1} + 0.2 veya daha büyük bir değere ulaştığında DS1302 otomatik olarak besleme gerilimi için V_{CC2} pinini kullanmaya başlar (Taştan, 2005).

Şekil 4.32'de de (Maxim, 2005) gösterilen DS1302 ile yapılan tüm haberleşmeler komut baytı ile başlar. Komut baytının 7. biti (MSB) her zaman için lojik '1' seviyesindedir. Komut baytının 7. bit lojik '0' olursa DS1302 ye veri yazılamaz. 6.

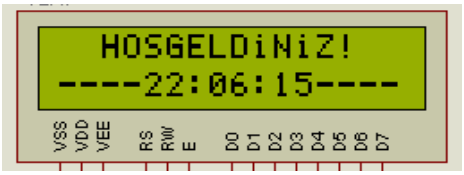
bit lojik ‘0’ iken saat verisi ile ilgili işlemler lojik ’1’ iken de RAM verisi ile ilgili işlemler gerçekleştirilir. 5. bitten 1. bite kadar A4- A0 kayıtçıları I/O olarak düzenlenebilir. LSB biti lojik ‘0’ iken DS1302’ye veri yazılabilir, lojik ‘1’ iken de veri okuma işlemi yapılabilir (Aslan, 2008).



Şekil 4.32. DS1302 komut bayt

Komut baytının DS1302’ye iletimi ilk önce en küçük değerlikli bit ile başlar. DS1302’nin RST ucu (5 nolu pin) normalde lojik 0 olarak tutulmaktadır. Veri transferi yapılacağı zaman bu pin lojik ‘1’ yapılmalıdır. Ayrıca RST ucu lojik ‘1’ yapılmadan önce SCLK ucu mutlaka lojik 0 olmalıdır. Komut baytının DS1302’ye aktarılması ve DS1302’ye istenen herhangi bir verinin yazılması SCLK ucunun çıkan kenarlarında olmaktadır. SCLK ucu lojik ‘0’ dan lojik ‘1’ e çekildiğinde DS1302’ye iletilmek istenen bitin DS1302’nin I/O ucunda hazır olması gerekmektedir. Benzer şekilde DS1302’den herhangi bir verinin okunması için gönderilecek olan komut baytı SCLK ucunun çıkan kenarlarında DS1302’ye aktarılmakta, okuma işlemi ise son çıkan kenardan itibaren düşen kenarlarda gerçekleştirilmektedir (Taştan, 2005).

DS1302 entegresi yardımıyla gerekli olan zaman bilgisi Şekil 4.33’de görüldüğü gibi elde edilebilir. Kullanıcılar sistemi kullandıkça, sistem aktif edildiği zamanlar mikrodenetleyici aracılığıyla RTC dosyasından sistemin aktif ediliş dakika ve saat bilgisi kaydedilip daha sonra yönetici tarafından istenilen zamanda kontrol edilebilir.



Şekil 4.33. DS1302 ile elde edilmiş zaman bilgisi

Şekil 4.34'de örnek kontrol ekran paneli bulunmaktadır. Veritabanına atılan veriler sayesinde gerektiğinde tüm bilgiler kontrol edilebilmektedir.

Şekil 4.34. Örnek kontrol paneli

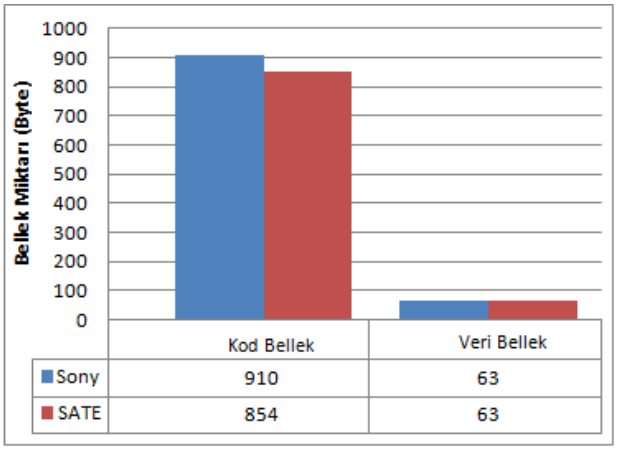
Sistem aktif edildikçe kayıtlı kullanıcıların bilgileri (sistemi ne zaman, hangi sıklıkla kullandıkları) yöneticinin kontrol edebilmesi için kayıt altına alınmaktadır. Eğer sistem gereksiz zamanlarda ve çok sık kullanılıyorsa kayıt edilen kullanıcı bilgileri sayesinde o kullanıcının sisteme erişimi istenildiği takdirde iptal edilebilir.

4.4. SATE Protokolünün Başarım Değerlendirmesi

SATE protokolünün başarım değerlendirmesi sürecinde var olan protokoller içerisinde en çok tercih edilen ve sıklıkla kullanılan SONY firmasının geliştirmiş olduğu SIRC protokolü seçilmiştir. Değerlendirme aşamasında KEIL µVision programı tercih edilmiştir. Değerlendirme işleminde protokollerin bellek boyutları ve çalışma performansları ölçüt olarak kullanılmıştır. KEIL µVision programında simülasyon işlemleri gerçekleştirilirken donanım olarak AT89C51RC2 8051 mikrodenetleyicisi donanım platformu olarak seçilmiştir.

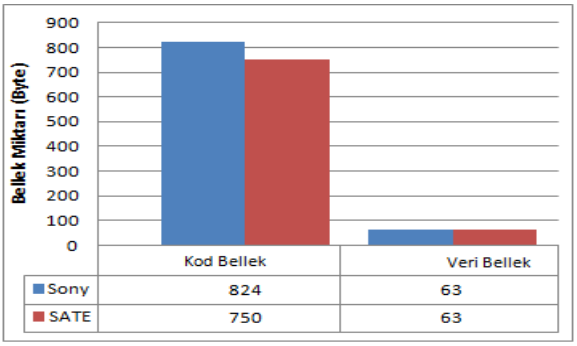
4.4.1. Bellek boyutu değerlendirmesi

Aşağıda verilen grafiklerde, şifreli ve şifresiz haberleşme esnasında SATE ve Sony protokollerinin adres ve komut bilgisi gönderme işlemlerinde ihtiyaç duydukları bellek miktarları görülmektedir.



Şekil 4.35. Şifreli veri gönderme

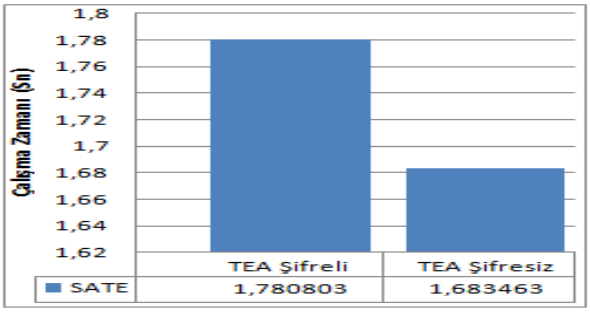
Şekil 4.35'de görüldüğü gibi, TEA algoritması ile şifreli haberleşme gerçekleştirilirken SATE protokolü 910 bayt kod bellek miktarı, Sony protokolü ise 854 bayt kod bellek miktarı kullanmaktadır. Bunun nedeni şifreleme için bazı sabit değişkenlerin kod bellekte tanımlanmasından kaynaklanmaktadır. Şekil 4.36'da ise şifresiz haberleşme esnasında SATE protokolünün kod bellek miktarının Sony protokolü kod bellek miktarına göre 74 bayt fazla olduğu görülmektedir. Bu durum SATE protokolündeki bit uzunlukları ve sürelerdeki farklılıklardan kaynaklanmaktadır. Veri belleğinin kullanılması haberleşme bilgisine bağlı olduğu için protokolün yapısı veya şifreli haberleşme olup olmamasının bir önemi yoktur. Bu yüzden de her iki haberleşme durumunda da veri belleklerinde bir değişim olmadığı grafiklerde görülmektedir.



Şekil 4.36. Şifresiz veri gönderme

4.4.2. Çalışma performansı değerlendirmesi

Çalışma perfeormansını değerlendirme aşamasında SATE protokolü kullanılarak şifreli ve şifresiz haberleşme sırasındaki sistem performansı test edilmiştir. Şifreleme algoritmasının sisteme eklenmesi durumunda protokolün yapısı da değiştiğinden Sony protokolü burada değerlendirme için kullanılmamıştır.



Şekil 4.37. SATE protokolü çalışma zamanı

Şekil 4.37'de verilen grafikte SATE protokolünün şifreli ve şifrelemesiz çalışma zamanları görülmektedir. Şifreli SATE protokolü ile şifresiz SATE protokolü arasındaki 97 ms'lik zaman farkı TEA algoritmasından kaynaklanmaktadır. Şifrelemedeki en büyük zaman kaybı algoritmadaki 2 Feistel 1 çevrim yapısından kaynaklanmaktadır. Şifreli haberleşmedeki çalışma zamanı daha uzun olsa da, haberleşme güvenliğinin daha üst seviyede olacağı da aşikârdır.

BÖLÜM 5. SONUÇ VE DEĞERLENDİRMELER

Bu tez çalışmasında kablosuz ortamda yüksek hızla çalışabilen ve maliyeti düşük olan kızılötesi tabanlı sistemlerin güvenliğini arttırmaya yönelik tasarım ve uygulamalar yapılmıştır. Kızılötesi sistemler için yapılan çalışmalarda güvenli haberleşmeye yönelik önemli bir teknik geliştirilememiştir. Bu nedenle kızılötesi iletişim de güvenlik seviyesi oldukça düşüktür.

Tez çalışmasında öncelikle düşük olan güvenlik seviyesini arttırmak için SATE isimli yeni bir kızılötesi protokol geliştirilmiştir. İletişimde protokolü, konuşmak için gerekli olan bir dil gibi kabul edersek, dilini bilmediğimiz kişileri anlayamayız. Anlaşma sağlamak için insanlar arasındaki iletişim için dili, kızılötesi ortamda haberleşme için ise protokolü öğrenmemiz gerekmektedir. Anlaşılamayan bir ortamda iletişimin olması düşünülemez.

Konuşulan bir dilin anlaşıldığı ortamlarda ise, sözlerimizi sadece istediğimiz kişilerin anlamasını istediğimiz durumlar olabilmektedir. Özellikle de karşı tarafa iletilecek bilgilerin gizli olması durumda bilgilerin gizliliğinin sağlanması gerekmektedir. Mesajın anlaşılabilirliğini gizlemek amacı ile iki farklı yöntem uygulanabilir. Bunlardan birincisi mesajın fark edilebilirliğinin engellenmesi, diğeri ise belirli bir teknikle mesajın anlaşılamaz bir biçime dönüştürülmesidir. Bunlardan ilkine stenografi, diğerine ise kriptografi denmektedir (Schneider, 1996). Mesajı kısaltarak veya şifreleyerek gizlemek önemli bilgilerin olduğu her yerde tercih edilen bir durumdur. Bu tez çalışmasında geliştirilen protokole, simetrik şifreleme yöntemlerinden blok şifreleme algortiması olan TEA (Tiny Encryption Algorithm) eklenerek kızılötesi ortamda haberleşmenin gizli olması sağlanmıştır. TEA, çok kısa olan kod boyutu ve basit algoritması sayesinde özellikle kod boyutunun oldukça sınırlı olduğu gömülü sistemlerde oldukça popüler olan bir şifreleme algoritmasıdır.

Algoritmanın mikrodenetleyici de uygulanabilir olması sistemin birçok yerde kullanılabilmesine olanak sağlamaktadır (Udea, 2010).

Kızılötesi ortamda güvenliği arttırmaya yönelik son olarak sisteme kullanıcı arayüzü eklenmiştir. Kullanıcı arayüzünde yönetici ve kullanıcı panelleri bulunmaktadır. Yönetici panelinden yönetici olan kişi sistemi hangi kullanıcının, hangi sıklıkla, ne zaman aktif ettiğini kontrol ederek gerektiğinde sisteme müdahale edebilmektedir. Kullanıcı arayüzü ise, sadece tanımlı olan kullanıcıların sistemi aktif etmesine izin vermektedir. Kullanıcı arayüzü sayesinde verici devresi istenmeyen kişiler tarafından ele geçirilse bile şifre bilinmediğinden ya da tanımlı bir kullanıcı olunmadığı için sistem aktif edilemeyecektir.

Tüm bu şartların sağlanmadığı durumlarda iletişim gerçekleşmemektedir. Sinyal geldikten sonra bir kesinti olursa veya yanlış bilgiler gelirse alıcı devresi tarafından belli bir süre sonunda sistem aktif edilmeyerek resetlenecektir. Sistemin aktif edilebilmesi için öncelikle protokol yapısının ve şifreleme tekniğinin çözülmesi gerekmektedir. Protokol yapısı ve şifreleme tekniği çözülmüş olsa bile verici devresinde tanımlı bir kullanıcı olunması gerekmektedir. Tanımlı kullanıcı için gerekli olan şifre bilinmiyorsa sistem aktif edilmeyecektir.

Kızılötesi sistemler hem sivil hem de askeri kullanım alanları bulmuştur. Özellikle askeri alanlarda kullanılan hedef tesbiti, gözlemleme, gece görüşü, güdüm ve takip sistemleri gibi önemli kullanım yerlerinde, tez çalışmasındaki kızılötesi tabanlı haberleşme güvenliğini arttırmaya yönelik geliştirilen teknikler kullanılabilir.

KAYNAKLAR

AKGÜL, A., KARACA, A., AKAR, F., ÇETİN, Ö., Kablosuz Ortamda IR Tabanlı Güvenli İletişim Uygulaması, 4.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISCTURKEY 2010), ODTÜ, Ankara 06-08 Mayıs, 2010.

ALTAN, K., KAŞKALOĞLU, K., KINDAP, N., ÖZAKIN, Ç.,SAYGI, Z., YILDIRIM, E., YILDIRIM, M., YILDIZ, S., Kriptolojiye Giriş, Seminer Notları,Uygulamalı Matematik Enstitüsü, Kriptografi Bölümü, ODTÜ, Şubat 2004.

ANDEM, V. R., A Cryptanalysis of the Tiny Encryption Algorithm, Master Thesis, Department of Computer Science in the Graduate School of The University of Alabama, 2003.

ANONİM, Blowfish, Vikipedi Özgür Ansiklopedi, http://tr.wikipedia.org/ wiki/ Blowfish , [14.09.2010], 2010d.

ANONİM, Görünür ışık, Vikipedi Özgür Ansiklopedi, http://tr.wikipedia.org/ wiki/ Görünür_ışık, [14.09.2010], 2010a.

ANONİM, Kızılötesi, Vikipedi Özgür Ansiklopedi, http://tr.wikipedia.org/wiki/Kızılötesi, [14.09.2010], 2010b.

ANONİM, MD5, Vikipedi Özgür Ansiklopedi, http://tr.wikipedia.org/wiki/MD5, [14.09.2010], 2010c.

ASLAN, A., 8051 RTC DS1302 ile LCD Gösterimli Dijital Saat, http://320volt.com/8051-rtc-ds1302-ile-lcd-gosterimli-dijital-saat/, [24.12.2010], 2008.

BANDIRMALI, N., ERTÜRK, İ., ÇEKEN, C., BAYILMIŞ, C., Yüksek Riskli Kablosuz Algılayıcı Ağlarda Güvenlik ve Şifreleme Uygulaması, Ağ ve Bilgi Güvenliği Sempozyumu, Kıbrıs, 16-18 Mayıs, 2008.

BAYILMIŞ, C., ÇAKIROĞLU, M., Sea Şifreleme Algoritması Kullanarak Güvenli Kablosuz Algılayıcı Ağ Haberleşmesinin Gerçekleştirilmesi, 3.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı , ODTÜ, Ankara 25-27 Aralık, 2008.

BAYKAL, N., Bilgi Teknolojisinin, Ulusal Güvenlik ve Ulusal Güvenlik Stratejisi ile ilgili Boyutu, Hava Harp Akademileri Sempozyumu, 2005.

BEZEN, Ş., Bluetooth ve Kızılötesi, http://www.cyber-warrior.org/FORum/bluetooth-ve-kizilotesi_332813,0.cwx, [18.09.2010], 2010.

BIHAM, E., SHAMIR, A., Differential Cryptanalysis of the full 16 round DES, Advances in Cryptology: Proceedings of CRYPTO'92, Springer-Verlag, Berlin , pp 487-496, 1993.

CANBEK, G., SAĞIROĞLU, Ş., Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Politeknik Dergisi, Cilt: 9, Sayı:3, s.165-174, 2006.

CARRUTHERS, J. B., Wireless Infrared Communications, Wiley Encyclopedia Of Telecommunications, 2002.

CHANDRA, X-Rays - Another Form of Light, http://chandra.harvard.edu /xray_ astro /xrays.html, [07.10.2010], 2010.

COPE, R. B., LOEHR, C., DASHWOOD, R., KERKVLIET, N. I., Ultraviolet radiationinduced non-melanoma skin cancer in the Crl: SKH1: hr-BR hairless mouse: augmentation of tumor multiplicity by chlorophyllin and protection by indole 3 carbinol, Photochem. Photobiol. Sci., 5, 599-507, 2006.

CRISP, Electromagnetic Radiation, http://www.crisp.nus.edu.sg /~research/tutorial/ em.htm, [12.09.2010], 2010.

ÇAVUŞOĞLU, H., TEA (Tiny Encryption Algorithm), http://www.bilgisayarkavramlari.com/2009/06/10/tea-tiny-encryption-algorithm, [12.09.2010], 2010.

DAEMEN, J., KNUDSEN, L. R., RIJMEN, V., The Block cipher Square, Proceedings of Fast Software Encryption, New York: Springer Verlag, pp. 149-165, 1997.

DALKILIÇ, G.,YILDIZOĞLU, G., Tek Anahtarlı Yeni Bir Şifreleme Algoritması Daha, Akademik Bilişim 2008, Çanakkale OnSekiz Mart Üniversitesi, Çanakkale, 30 Ocak – 01 Şubat 2008.

EROL, Y., Kızılötesi Işıkla Cihaz Kontrolü, Bilim ve Teknik Dergisi, Kasım 2004.

FISHER, R. E., Gray-code analog-to-digital converter, IEEE Trans. On Microwave Theory and Techniques, 16 (No:8), 541-547, 1968.

GENÇ, B., Elektromanyetik Spektrumun X-Işını Ve Görünür Bölgesinde, Ortamlardan Yayılan Fotonları Kaydetmek İçin Spektrometre Ve Görüntüleme Sistemlerinin Tasarımı, Yüksek Lisans Tezi, Kocaeli Üniversitesi Fen Bilimleri Enstitüsü, 2006.

GREEN, R. J., Secure Communications: The Infrared Alternative, ICTON Mediterranean Winter Conference, 1 – 4, 2007.

GÜLAÇTI, E., Milli Açık Anahtar Altyapısı Eğitim Kitabı, http://www.kamusm.gov.tr/tr/Bilgideposu/Belgeler/teknik/aaa/index.html, [23.09.2010], 2010.

GÜNEŞ, M., YILMAZ, Ş., Kızıl Ötesi Algılayıcılar Kullanılarak Balık Sayıcı ve Boyut Belirleyici Tasarımı ile Tesis Takip Yazılım Sisteminin Geliştirilmesi, KSÜ Fen ve Mühendislik Dergisi, 10(2), 2007

HEATLEY, D., WISELY, D., NEILD, I., COCHRANE, P., Optical wireless: The story so far, IEEE Communications Magazine, 72-82, 1998.

KAÇMAZ, S. E., KABDAŞLI, S., Uydu Görüntüleri Yardımıyla Plaj Alanlarında Dane Çapının Belirlenmesi, 6.Ulusal Kıyı Mühendisliği Sempozyumu, İzmir, 2007.

KAHN, J. M., BARRY, J. R., Wireless infrared communications, Proceedings of the IEEE, 85, 265 – 298, 1997.

KARADERE, T., Bilgi Güvenliği, http://security.metu.edu.tr/ Documents/Bilgi%20 Guvenligi.html, [08.10.2010], 2010.

KNUDSEN L. R., Truncated and Higher Order Differentials, Fast Software Encryption, Springer-Verlag, 196-211, 1995.

MAIWALD, E., Network Security: A Beginner's Guide Summary, McGraw- Hill Osborne Media, California, 2003.

MATSUI, M., Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology - Eurocrypt '93, Springer-Verlag, 386-397, 1994.

MAXIM, Trickle-Charge Timekeeping Chip-DS1302, Datasheet, Dallas Semiconducter Corporation, USA, 2005.

PRO-G, Bilişim Güvenliği, Sürüm 1.1, Pro-G Bilişim Güvenliği ve Araştırma Ltd., http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf, [06.10.2010], 2003.

RIZ, D., GARAUDE, F., HOURY, M., CANAUD, B., Neutron and photon emission of a high-gain direct-drive target for laser fusion, Nucl. Fusion 46, 864–867, 2006.

SAKALLI, M, T., BULUŞ, E., ŞAHİN, A., BÜYÜKSARAÇOĞLU, F., Akış Şifrelerinde Tasarım Teknikleri Ve Güç İncelemesi, Akademik Bilişim, Dumlupınar Üniversitesi, Kütahya, 31 Ocak-2 Şubat 2007.

SAKALLI, M. T., BULUŞ, E., ŞAHİN, A., BÜYÜKSARAÇOĞLU, F., Bir Blok Şifreleme Algoritmasına Karşı Square Saldırısı, Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, İstanbul, Haziran 2005.

SAKALLI, M. T., Modern şifreleme yöntemlerinin gücünün incelenmesi, Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, 2006.

SB-PROJECTS, NEC Protocol, Knowledge Base, San Bergmans, Oisterwijk, The Netherlands http://www.sbprojects.com/knowledge/ir/nec.htm, [08.09.2010], 2001c.

SB-PROJECTS, Nokia NRC17 Protocol, Knowledge Base, San Bergmans, Oisterwijk, The Netherlands http://www.sbprojects.com/knowledge/ir/nrc17.htm, [08.09.2010], 2001d.

SB-PROJECTS, Sharp Protocol, Knowledge Base, San Bergmans, Oisterwijk, The Netherlands, http://www.sbprojects.com/knowledge/ir/sharp.htm, [08.09.2010], 2001b.

SB-PROJECTS, Sony SIRC Protocol, Knowledge Base, San Bergmans, Oisterwijk, The Netherlands http://www.sbprojects.com/knowledge/ir/sirc.htm, [08.09.2010], 2001a.

SCHNEIDER, B., Applied Cryptography, Second Edition, John Wiley & Sons, Inc., New York, 1996.

SENGUPTA, D. L., SARKA, T. K., Maxwell, Hertz, the Maxwellians, and the Early History of Electromagnetic Waves, IEEE Antennas and Propagation Magazine, 45 (No. 2), 13-19, 2003.

SHARP, E. D., Information Security in the Enterprise, Information Security Management Handbook Fifth Edition, Tipton, F. H., Krause, M., Auerbach Publications, New York, 1199-1200, 2004.

STANDAERT, F. X., PIRET G., GERSHENFELD N., QUISQUARTER J. J., SEA: A Scalable Encryption Algorithm for Small Embedded Applications, CARDIS 2006, Lecture Notes in Computer Science, vol. 3928, April 2006.

STINSON D. R., Cryptography, Theory and Practice, CRC Press, 1995.

STINSON, D. R., Cryptography: Theory and Practice, Second Edition, CRC Press, 2002.

ŞAHİN, A., BULUŞ, E., SAKALLI T. M., Modern Blok Şifreleme Algortimalarının Gücünün İncelenmesi, II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi, İstanbul, Kasım 2005.

TAŞTAN, T., DS1302 RTC Kullanımı, http://www.aadf.net /elektronik_files/ ds1302 kullanimi.pdf, [24.12.2010], 2005.

UDEA, UN-0506v01_Şifreleme, Uygulama Notu, UDEA wireless technologies, http://www.udea.com.tr/dokumanlar/UN-0506v01_Sifreleme.pdf, [26.09.2010], 2010.

VISHAY TELEFUNKEN, Photo Modules for PCM Remote Control Systems, Datasheet, Vishay Semiconductor GmbH, Heilbronn Germany, 2001.

VURAL, Y., Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri , Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 2007.

WHEELER, D. J., NEEDHAM, R. J., TEA,A Tiny Encryption Algorithm, In Fast Software Encryption, Proceedings of the 2nd International Workshop ,1994.

YERLİKAYA , T., BULUŞ, E., ARDA, D., Asimetrik Kripto Sistemler ve Uygulamaları, II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi (MBGAK), İstanbul, 2005.

YERLİKAYA, T., BULUŞ, E., ARDA, D., Aes Aday Şifreleme Algoritmalarının Yazılım Ve Donanım Performans Karşılaştırılması ve Uygulamaları, Elektrik Elektronik Bilgisayar Mühendisliği Sempozyumu, Bursa, Aralık 2004.

YERLİKAYA, T., BULUŞ, E., BULUŞ, N., Asimetrik Şifreleme Algoritmalarında Anahtar Değişim Sistemleri, 54. Akademik Bilişim Konferansı , Denizli, Şubat 2006.

YILDIRIM, K., Veri Şifrelemesinde Simetrik ve Asimetrik Anahtarlama Algoritmalarının Uygulanması (Hybrid Şifreleme) , Yüksek Lisans Tezi, Kocaeli Üniversitesi Fen Bilimleri Enstitüsü, 2006.

YÜCEL, E., Elektromanyetik Spektrum, http://www.akat.org/sizin_icin/elektromagnetik_tayf.pdf, [26.12.2010], 2005.

ÖZGEÇMİŞ

Akif AKGÜL, 12.08.1986 tarihinde Karşıyaka'da doğdu. İlköğrenimini İzmir, Mardin ve İstanbul'daki farklı okullarda tamamladı. 2004 yılında Üsküdar Haydarpaşa Anadolu Meslek Lisesi'nden mezun oldu. 2005 yılında başladığı Kocaeli Üniversitesi Teknik Eğitim Fakültesi Elektronik Öğretmenliği Bölümü'nü 2009 yılında tamamladı. Aynı yıl Sakarya Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Bilgisayar Eğitimi Anabilim Dalı'nda yüksek lisansa başladı. Kasım 2009'da Sakarya Üniversitesi Teknik Eğitim Fakültesi Elektronik ve Bilgisayar Eğitimi Bölümü'nde araştırma görevlisi olarak çalışmaya başladı. Halen aynı görevini sürdürmektedir.