**KARADENİZ TEKNİK ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

**ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI**

# ANALOG EL TELSİZLERİNDE SAYISAL ŞİFRELEME

**YÜKSEK LİSANS TEZİ**

**Elektrik-Elektronik Müh. Sibel ARSLAN**

**EKİM 2009**
**TRABZON**

**KARADENİZ TEKNİK ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

**ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI**

# ANALOG EL TELSİZLERİNDE SAYISAL ŞİFRELEME

**Elk.-Elkn. Müh. Sibel ARSLAN**

**Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünce**
**"Elektronik Yüksek Mühendisi"**
**Unvanı Verilmesi İçin Kabul Edilen Tezdir.**

**Tezin Enstitüye Verildiği Tarih: 23.09.2009**
**Tezin Savunma Tarihi : 19.10.2009**

**Tez Danışmanı : Doç. Dr. İsmail Hakkı ÇAVDAR**
**Jüri Üyesi : Yrd. Doç. Dr. Haydar KAYA**
**Jüri Üyesi : Prof. Dr. Vasif V. NABİYEV**

**Enstitü Müdürü : Prof. Dr. Salih TERZİOĞLU**

**Trabzon 2009**

# ÖNSÖZ

Güvenli iletişimin her geçen gün önem kazandığı günümüzde, emniyet birimleri ve silahlı kuvvetler gibi kolluk kuvvetleri için güvenli telsiz iletişiminin sağlanabilmesi ön plana çıkmaktadır. Şifreleme özelliği bulunmayan analog telsizlerde güvenli iletişimin sağlanması amacıyla yapılan bu tez çalışması aynı zamanda telefon görüşmesinin de güvenli hale getirilmesini sağlayacaktır.

Tez çalışmam boyunca her türlü görüş ve düşünceleriyle bana yol gösteren, destek olan, yardım ve katkılarını esirgemeyen değerli danışman hocam Sn. Doç. Dr. İsmail Hakkı ÇAVDAR'a sonsuz teşekkürlerimi sunarım.

Ayrıca, Gate Elektronik San. ve Tic. A.Ş. firmasına katkılarından dolayı teşekkürü bir borç bilirim.

Son olarak, hayatımın her aşamasında olduğu gibi, bu çalışma süresince de yanımda olan, desteklerini esirgemeyen çok değerli aileme teşekkür ederim.

Sibel ARSLAN
Trabzon 2009

# İÇİNDEKİLER

**Sayfa No**

# ÖZET

Analog el telsizleri ile yapılan ses iletişiminin istenmeyen kişiler tarafından kolayca dinlenememesi amacı ile düşük maliyetli ve analog el telsizlerine mikrofon ve hoparlör girişinden kolayca takılabilecek yapıda olan küçük bir ses şifreleme birimi tasarlanmıştır.

Tasarım öncesi analog el telsizinin yapısı, telsiz iletişimi, modülasyon türleri ve kriptoloji konularında araştırmalar yapılmıştır. Yazılım dili olarak C programlama, mikroişlemci olarak dspic kullanılmıştır. Bu çalışmada gömülü yazılım içeren donanım tasarımına dayalı bir çözüm önerilmiştir.

Verici konumundaki telsiz şifreleme biriminde, ses sinyali telsiz mikrofonuna verilmeden önce, sayısallaştırılıp şifrelendikten sonra tekrar analog işaret haline getirilmiştir.

Alıcı konumundaki telsiz şifreleme biriminde ise, alınan analog şifreli ses sinyali hoparlör çıkışına verilmeden önce tasarlanan denkleştirici (equalizer) devresi ile lojik–1 ve lojik–0 işaretlerine atanan sinüsoidal sinyallerin seviyeleri ayarlanmıştır. Denkleştirici devresi çıkışında elde edilen analog şifreli bu ses sinyali, sayısallaştırılıp şifre çözme işlemi gerçekleştirildikten sonra tekrar analog şifresiz ses sinyaline dönüştürülmüştür.

Geliştirilen şifreleme birimi önce laboratuar ortamında daha sonra UHF bandında çalışan PMR telsizleri ile test edilmiş ve başarılı sonuçlar elde edilmiştir.

**Anahtar Kelimeler:** Telsiz, Analog Telsiz, Telsiz İletişimi, Half-Duplex, Bas-konuş (PTT), Güvenli Haberleşme, MSK, Kripto, Sayısal Kripto, Şifreleme, Ses Şifreleme.

## SUMMARY

### Digital Encryption on the Analog Handheld Two-Way Radios

In order to prevent the unwanted eavesdropping to the communications over the analog handheld two-way radios, a low cost, small voice encryption unit with easy integration capability through the radio microphone and speaker jacks has been designed.

Before the design phase, subjects like analog handheld two-way radio, two-way radio communication, modulation types and cryptology have been studied. C programming language and dspic microprocessor is used in the design. Hardware with embedded software was used in the design approach.

Before the audio signal is sent to the microphone input of the transmitting radio, signals are digitized, encrypted and converted back in to the analog signal by the Digital Encryption unit.

On the receiving end, the encrypted analog audio signal levels are adjusted through an equalizer in order to attain the appropriate logic–1 and logic–0 signal levels. The adjusted signals are digitized, decrypted and converted back in to the analog audio signal by the Digital Encryption unit.

The developed Digital Encryption unit has been tested in the laboratory environment as well as with the PMR handheld two-way radios in the UHF band and successful results has been achieved.



**Key Words:** Two Way Radio, Analog Two Way Radio, Two Way Radio Communication, Half-Duplex, Push-to-Talk (PTT), Secure Communication, MSK, Crypto, Digital Crypto, Encryption, Audio Encryption.

# ŞEKİLLER DİZİNİ

**Sayfa No**

# TABLOLAR DİZİNİ

**Sayfa No**

## SEMBOLLER DİZİNİ

ADC : Analog Sayısal Çevirici (Analog Digital Converter)

AES : İleri Şifreleme Standardı (Advanced Encryption Standard)

AM : Genlik Modülasyonu (Amplitude Modulation)

ANI : Otomatik Numara Tanıma (Automatic Number Identification)

APCO : Kamu Güvenliği Haberleşme Yetkilileri Birliği (Association of Public Safety Communications Officials)

ASK : Genlik Kaydırmalı Anahtarlama (Amplitude Shift Keying)

DAC : Sayısal Analog Çevirici (Digital Analog Converter)

DES : Veri Şifreleme Standardı (Data Encryption Standard)

DSP : Sayısal İşaret İşleme (Digital Signal Proccessing)

EEA : Elektronik Mühendisleri Birliği (Electronic Engineering Association)

GMSK : Gaussian MSK

FDMA : Frekans Bölmeli Çoklu Erişim (Frequency Division Multiple Access)

FEC : İleri Hata Düzeltme (Forward Error Correction)

FM : Frekans Modülasyonu (Frequency Modulation)

FSK : Frekans Kaydırmalı Anahtarlama (Frequency Shift Keying)

NIST : Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology)

PAMR : Ortak Paylaşımlı Mobil Telsiz (Public Access Mobile Radio)

PM : Faz Modülasyonu (Phase Modulation)

PMR : Özel Mobil Telsiz (Private Mobile Radio)

PSK : Faz Kaydırmalı Anahtarlama (Phase Shift Keying)

PTT : Bas-Konuş (Push-To-Talk)

SMD : Yüzey Montajlı Eleman (Surface Mount Device)

TDMA : Zaman Bölmeli Çoklu Erişim (Time Division Multiple Access)

TKS : Ton Kodlu Susturma

ZVEI : Elektrik ve Elektronik Endüstrisi Merkezi (Zentralverband Elektrotechnik- und Elektronikindustrie)

# 1. GENEL BİLGİLER

## 1.1. Giriş

Telsiz cihazları günümüzde tüm dünyada kamu ve özel sektör kullanıcıları tarafından yoğun bir şekilde kullanılmaktadır. Ülkemizde de telsiz kullanımı 1983 yılında Telsiz Genel Müdürlüğü'nün kuruluşu ile birlikte gün ve gün artmaktadır. Telsiz kullanımını diğer haberleşme cihazlarından ayıran önemli farklar konuşma ücretinin (veya gözardı edilebilir seviyede) olmaması ve doğrudan birebir kişiler ile veya bir grup veya tüm gruplardaki kullanıcıların hepsi ile birden iletişim kurulabilmesidir. Bu farklar; telsiz cihaz ve sistemlerinin hastanelerden ulaşım hizmetlerine, silahlı kuvvetlerden emniyet teşkilâtlarına, tarım kuruluşlarından maden arama sahalarına, kısaca kara, hava, deniz, denizaltı ve hatta uzayda çok büyük alanlarda ve geniş kullanıcı yelpazesi tarafından kullanılabilir hale getirmiştir.

Emniyet birimleri ve silahlı kuvvetler gibi kolluk kuvvetleri için güvenli telsiz iletişiminin sağlanabilmesi yani telsiz görüşmelerinin istenmeyen kişiler tarafından dinlenilmesinin önlenmesi büyük önem taşımaktadır. Sayısal telsiz sistemlerinde güvenli haberleşmenin sağlanabilmesi amacı ile sayısal şifreleme (digital encryption) kullanılmaktadır. Bazı analog telsiz sistemlerinde ise şifreleme bir opsiyon olarak sunulmaktadır. Fakat bir kısım analog telsizlerde böyle bir opsiyon bulunmaması nedeniyle haberleşmenin istenmeyen kişiler tarafından dinlenilmesi söz konusudur. Şifreleme özelliği bulunmayan analog telsizlerde güvenli haberleşmenin sağlanması amacıyla yapılan bu tez çalışması aynı zamanda telefon görüşmesinin de güvenli hale getirilmesini sağlayacaktır.

## 1.2. Telsiz

Telsizler, kabloya ihtiyaç duymadan haberleşme yapabilmemizi sağlayan cihazlardır. Ünlü bilim insanı Marconi tarafından Dünya'ya tanıtılmış olsa da Nikola Tesla'nın araştırmalarında da kablosuz haberleşmenin izlerine rastlanır.

Bir telsiz haberleşmesinin varlığından söz edebilmek için aynı frekanslarda çalışabilen, teknik özellikleri birbirinin aynı olan en az iki cihaz gereklidir. Haberleşme;

verici konumundaki (gönderme yapan) cihazdan çıkarak anten vasıtasıyla boşluğa yayılan elektromanyetik dalgaların, alıcı durumundaki cihazın anteni yoluyla alıcı cihaza (dinleme yapan) ulaşması şeklinde olur. Telsiz cihazlarını ve telsiz haberleşme sistemlerini, farklı şekilde gruplara ayırmak mümkündür.

Telsiz kullanım alanlarına göre:

- Kara
- Hava
- Deniz

haberleşmesinde kullanılan telsiz sistem ve cihazları olarak üçe ayrılır.

Bir başka gruplandırma:

- El
- Araç
- Sabit

telsiz cihazları olarak yapılabilir.

Çalışma frekanslarına göre:

- HF (3 – 30MHz)
- VHF (30 – 300 MHz)
- UHF (300 – 3000 MHz)

olarak ayrılabilir.

Tüm bu gruplandırmalardan ayrı olarak özel kullanım amaçlarına yönelik telsiz cihaz ve sistemleri de vardır.

Telsiz cihazlarının kullanılacağı arazi şekilleri ve haberleşme mesafesi frekans bantlarının seçiminde etkili olmaktadır. Buna göre UHF bandında çalışan bir telsiz sisteminde haberleşme mesafesi birkaç km ile sınırlıyken, HF bandında kıtalararası haberleşmeden bahsetmek mümkündür.

Telsiz cihazlarını meydana getiren ana parçalar; verici/alıcı donanım kısmı, besleme birimi, anten, anten kablosu ve mikrofon gibi parçalardır.

Telsiz cihazının çalışması için gerekli elektrik enerjisini sağlayan besleme birimleri, el cihazlarında doldurulabilir Ni-Cd, Li-Ion gibi pillerden oluşan batarya bloğudur.

Araç cihazlarında beslemeyi, aracın elektrik tesisatı, aküsü sağlar. Anten aracın dışına takılan ve koaksiyel bir anten kablosuyla cihaza bağlanır. Bu cihazlarda spiral kablolu bir el mikrofonu bulunur.

Sabit telsiz cihazları, 220V AC şebeke gerilimini 13.8V DC gerilime çeviren ve yaklaşık 10~15 A akım verebilen bir besleme sistemiyle çalıştığı gibi besleme sistemi içerisinde olan cihazlar da vardır. Bu cihazlarda bina dışına takılan bir sabit anten ve anten ile cihaz arası mesafeye göre uygun tipte koaksiyel kablo kullanılır. Mikrofon olarak masa ya da el mikrofonu kullanılır.

### 1.3. Telsiz Cihazlarının İç Yapısı

Bir telsiz cihazı çeşitli bölümlerden meydana gelir. Ana hatlarıyla bölümler şunlardır:

- Alıcı bölümü
- Verici bölümü
- Çıkış ya da güç katı
- Kontrol bölümü
- Frekans sentezleyici
- Ses çıkış katı
- Ara frekans bölümü

Telsiz cihazları, çalışma frekanslarının belirlenmesinde kullanılan teknikler, modülasyon tipleri, bant genişlikleri gibi bir takım teknik özellikler yönünden de farklı özellikler gösterirler.

Telsiz haberleşmesinde ve elektromanyetik dalgalar yardımıyla yapılan yayınlarda (Radyo, TV) değişik modülasyon tiplerinden bahsetmek mümkündür. Bunlardan başlıcaları: Genlik (AM) ve Frekans (FM) modülasyonlarıdır.

Modülasyon; gönderilmek, yayınlanmak istenen işarete bağlı olarak taşıyıcı dalganın bazı özelliklerinin değiştirilmesi işlemidir. Bu işlemin alıcı cihazda yapılan tersi işleme ise demodülasyon denir.

Frekans modülasyonu (FM), gönderilmek istenen işarete bağlı olarak taşıyıcı dalga frekansının sıklığının değiştirilmesidir.

Genlik modülasyonu (AM), gönderilmek istenen işarete bağlı olarak taşıyıcı dalganın genliğinin değiştirilmesidir.

Günümüz kara haberleşmesinde genel olarak VHF, UHF bantlarında, FM modülasyonlu, frekans sentezleyicili telsizler kullanılmaktadır.

Deniz bandında ise VHF, 156–163 MHz arası, frekans sentezleyicili, uluslararası standartlarla belirlenmiş özellikleri olan FM modülasyonlu telsizler kullanılmaktadır. Yine, uluslararası standartlar gereği hava telsizleri, 118–136 MHz arası AM modülasyonlu olarak çalışırlar [1].

### 1.4. Aktarıcı Sistemler (Röle, Repeater Cihazları)

VHF, UHF bantlarında arazi şekilleri ve/veya istasyonlar arası mesafe haberleşmeyi güçleştiren, bazen de imkânsız hale getiren faktörlerdir. Bu gibi durumlarda röle ya da aktarıcı istasyon (röle, repeater cihazları) denilen birtakım cihazlardan yararlanılır.

Temel olarak bir röle cihazı yüksek kazançlı bir anten, az kayıplı bir anten kablosu, süzgeç birimi (duplexer), alıcı ve verici bölümler ile bunların kontrol biriminden meydana gelir. Alıcı ve verici frekansları arasında farklılık bulunan röle cihazları süzgeç biriminin yardımıyla, alıcısının duyduğu işaretleri aynı anda vericisinden güçlendirilmiş olarak yayınlar. Röle cihazları full duplex çalışan cihazlardır.

Rölenin konulduğu yerin yükseltisi ile doğru orantılı olarak geniş bir haberleşme alanı elde edilmiş olur.

### 1.5. Telsizlerin Çekim Mesafesi

Telsizlerin çekim mesafesi birçok parametreye göre değişebilmektedir. Bu parametreler; telsizin çıkış gücü, telsiz kullanılan bölgenin coğrafi yapısı, telsizin kullandığı modülasyon tipi ve kullanılan antenin kazancı ve yapısıdır. Standart olarak UHF/VHF telsiz haberleşmesinde kullanılan el telsizleri maksimum 5 Watt, araç ve sabit telsizler 25 Watt çıkış gücündedir. HF telsiz kullanılan araç ve sabit telsizler 150 Watt çıkış gücündedir. Yukarıdaki parametrelere göre bir el telsizi ile simplex (aktarıcı olmadan) olarak 3–10 km, araç ve sabit telsiz ile 10–30 km, bir HF telsiz ile iyonosferin durumuna göre tüm dünya ile görüşebilirsiniz [2].

## 1.6. Telsiz Haberleşmesi

Telsiz haberleşme sistemlerinde iletilmek istenen mesaj (ses veya veri), taşıyıcı görevi yapan elektromanyetik bir dalga sayesinde iletilir. Belli bir frekanstan verici ile yayınlanan bu dalga, bir anten vasıtasıyla alıcıya aktarılır. Alıcıda elde edilen mesaj, ses ise bir hoparlöre, veri ise başka bir dış birime gönderilir ve bu yolla iletişim gerçekleşir.

Telsiz sistemleri kullanım yerine ve amacına göre çeşitli şekillerde isimlendirilmiştir. Bu isimler Avrupa'da PMR (Private Mobile Radio) ve PAMR (Public Access Mobile Radio) olarak sayılabilir. PMR kullanıcı gruplarına özel tahsisli kanal kullanımı ve sistemin kullanıcı grubu tarafından işletilmesi ya da işletiminin kontrol edilmesi anlamına gelirken, PAMR da konuşma kanallarının birden fazla kullanıcı grubu tarafından ortak kullanımı ve sistemin bir operatör tarafından işletilmesi anlamına gelmektedir.

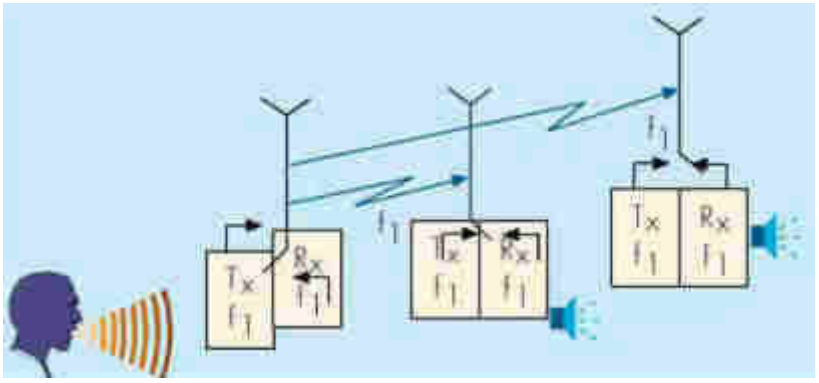
Telsiz haberleşme sistemleri, diğer tüm haberleşme sistemlerinde olduğu gibi teknolojik gelişime paralel olarak, belirli zaman aralıklarında sınırlı bir çerçeve içinde gelişmelerini sürdürmüşler, ancak teknolojik gelişmenin evrimsel olduğu zamanlarda ise evrimsel bir gelişmeye tabi olmuşlardır. Bu anlamda analog teknolojilerin kullanıldığı aralıkta tasarlanan telsizler birinci nesil, sayısal teknolojilerin kullanıldığı aralıkta tasarlanan telsizler ise ikinci nesil telsizler olarak adlandırılmışlardır.

### 1.6.1. Birinci Nesil Telsiz Sistemleri

#### 1.6.1.1. Konvansiyonel Sistemler

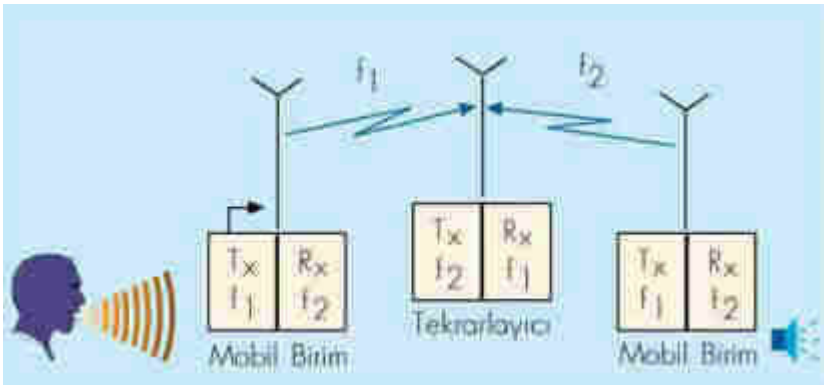
Konvansiyonel sistemler, bir çevrim içindeki bütün kullanıcıların aynı kanalda beklediği ve bu kanaldan alma gönderme yaptığı sistemlerdir. Telsizlerin, alma ve göndermede aynı frekansı kullanarak çalışmasına simplex çalışma; farklı frekanslar üzerinden çalışmasına ise duplex çalışma adı verilmektedir. Simplex çalışmada sistemdeki tüm birimler alma ve gönderme işlemlerini tek bir frekans üzerinden yaparlar. Telsizin alma sırasında vericisi, gönderme sırasında ise alıcısı pasif konuma geçer. Simplex kanalda kısa mesafede haberleşme yapılabilir. Tek röleli çalışmada alma ve gönderme işlemi alma-gönderme frekans çifti kullanarak yapılır. Telsizler aynı anda ya alma ya da gönderme işlemi yapar. Röle kanaldaki yayını tekrarlarken, eş zamanlı olarak alma ve gönderme işlemi yapar. Alandaki telsizler birbirleri ile direk görüşemezler, rölenin tekrarladığı

bilgileri alabilirler. Kapsama alanı rölenin gücüne, konumuna ve coğrafik koşullara bağlıdır. Simplex çalışma metodu şekil 1'de görülmektedir.




Şekil 1. Simplex sistem

Duplex çalışmada ise telsizler alma ve gönderme işlemlerini farklı frekanslar üzerinden yaptıklarından sistemde iki taraflı telefon görüşmesi şeklinde görüşme gerçekleşebilir. Tam duplex ve yarı duplex olmak üzere iki çeşit duplex çalışma metodu vardır. Tam duplex çalışan bir sistemde, sistemdeki tüm birimler aynı anda alma ve gönderme yapma özelliğine sahiptirler. Yarı duplex çalışan bir sistemde ise yalnızca tekrarlayıcı telsiz bu özelliğe sahiptir; diğer telsizler aynı anda alma ve gönderme yapamaz. Yarı duplex çalışma prensibi şekil 2'de gösterilmiştir.




Şekil 2. Yarı duplex sistem

Klasik Telsiz Sisteminde haberleşme, aldığını gönderen bir aktarıcı (repeater) aracılığıyla olur. Sistemde birden fazla kanal olabilir. Telsiz kullanıcıları hangi kanalda görüşmek isterlerse telsizlerini o kanala getirirler.

Geniş alan konvansiyonel telsiz sistemi birden çok röle kapsama alanı bir araya getirilerek oluşturulur. Kapsama alanı sisteme yeni röleler eklenerek genişletilebilir. Sistem kontrol birimi tarafından yönetilir. Röleler bölge aktarıcıları olarak kullanılır. Bölge aktarıcıları birbirlerine mikrodalga linklerle bağlanır.

#### 1.6.1.2. Telsiz Sistemlerinde Kullanılan Özellikler

Konvansiyonel telsizlerde telsizlerin daha verimli kullanılabilmesi ve konvansiyonel telsiz ve tekrarlayıcılardan birçok kullanıcı grubunun sistem olarak yararlanabilmesi için sistemlere çeşitli ilave özellikler kazandırılmaktadır. Bu özellikler aşağıda anlatılmıştır:

- Ton Kodlu Susturma
- Seçmeli Çağrı
- Kimlik Tanıtma
- Kanal Tarama
- Gönderme Zamanını Sınırlama
- Meşgul Kanalda Yayın Kilidi

##### 1.6.1.2.1. Ton Kodlu Susturma (TKS)

Susturma tekniklerinden olan TKS, sistemdeki telsizlere yazılım ile kazandırılabilen bir özelliktir. TKS özelliğine sahip bir sistemde, telsizlerin gönderdiği mesajlara özel bir ton eklenir. Gönderilen mesajı etkilememesi için ses işaret bandının (300Hz-3kHz) altında yer alan bu ton (67-250Hz), telsiz göndermeye geçtiğinde üretilerek gönderilen mesaja eklenir. TKS özelliğine sahip telsizler bu özel tonu tanıyarak alıcı devrelerinin açılmasını sağlarlar. Böylelikle telsizler yalnızca doğru tonu içeren mesajlara tepki verirler; diğer mesajları dikkate almazlar. TKS özelliği sayesinde sisteme aşağıda anlatılan nitelikleri kazandırmak mümkün olmaktadır:

- Sistemde aynı frekans kanalını paylaşan birbirinden bağımsız haberleşme grupları oluşturulabilir. Sistemde oluşturulmak istenen her kullanıcı grubu için, o

gruba özel, sistem içinde tek olan bir ton seçilir. Belli bir gruba ait telsiz göndermeye geçtiğinde o gruba ait ton mesaja eklenir. Bu ton sayesinde, gönderilen mesaja sadece ilgili gruba ait telsizler tepki verirler. Böylelikle aynı kanalı paylaşan telsizler gruplar halinde kanalı sıralı olarak kullanabilirler.

- Bir susturma tekniği olan TKS, rastgele yayınların telsizleri etkilemesini önler.
- TKS özelliği ile tekrarlayıcı telsizlerin istenmeden yayına geçmesi engellenebilir. Bu uygulamada; tekrarlayıcı telsizler programlanırken hizmet verecekleri telsizlere ait ton grupları belirlenerek girilir.

#### 1.6.1.2.2. Seçmeli Çağrı

Seçmeli çağrı, telefon sistemlerinde olduğu gibi istenilen kullanıcıya numara çevrilerek erişme özelliğidir. Seçmeli çağrı özelliği olmayan sistemlerde her kullanıcı kendisini ilgilendiren konuşmayı kaçırmamak için kanalda geçen tüm konuşmaları dinlemek zorunda kalmaktadır.

Seçmeli çağrı özelliği olan sistemlerde her telsize ve/veya gruba birer "çağrı numarası (kimlik numarası)" verilmektedir. İstenen telsiz veya gruba bu numara vasıtasıyla çağrı yapılır. Böylece yapılan çağrı sadece ilgili telsize yönlendirilmiş olur. Normalde tüm kullanıcılar tarafından duyulan konuşmalar, seçmeli çağrı özelliği sayesinde sadece istenen kullanıcılar tarafından duyulur. Böylece kullanıcılar, kendileri çağrılmadıkça kanaldaki diğer konuşmaları dinlemek zorunda kalmazlar.

Seçmeli çağrı sistemlerinde kullanılan çeşitli yöntemler mevcuttur. Yaygın olarak kullanılan yöntemler 2-ton ve 5-ton seçmeli çağrı sistemleridir. Günümüzde 2-ton sisteminin gelişmiş şekli olan 5-ton sistemler tercih edilmektedir. Bu sistemde her "adres" 5 rakamdan oluşur. 0–9 arası rakamların her birini temsil eden birer ton seçilir. İki aynı rakamın yan yana geldiği durumlar için bir tekrar tonu üretilir. Her bir "5 ton dizisi" bir adresi temsil eder.

Seçmeli çağrı özelliği olan sistemlerde ulusal ve uluslararası olmak üzere çeşitli standartlar kullanılmaktadır. Bu standartlar şunlardır:

- CCIR
- EEA
- ZVEI

Yukarıdaki standartlardan başka EIA, ZVEI (S), NATE1, ZVEI II, DZVEI ve Metropage standartları da kullanılmaktadır. Yaygın olarak kullanılan standartların (CCIR, EEA, ZVEI) frekans kümeleri tablo 1'de verilmiştir.

Tekrarlayıcı telsizlere istenmeyen yayınların ulaşmasını engellemek amacı ile tekrarlayıcı telsizlere bir Kimlik Numarası verilebilir. Böylece tekrarlayıcı telsiz gelen sinyalde kendine ait kimlik numarası tonlarının olup olmadığını kontrol edecek ve ona göre hizmet verecektir. Bunun sağlanması için tekrarlayıcı telsizlerde seçmeli çağrı özelliği donanım birimleri (kodlayıcı ve kod çözücü) bulunmalıdır.

Seçmeli Çağrı sistemlerinin bir yan özelliği olan "kimlik gönderme" telsize programlanmış olan kimliğin (**ANI-**Automatic Number Identification) bas-konuş mandalına basılmasıyla gönderilmesidir. Bu özellik sayesinde kanalda sürdürülmekte olan konuşmalar kontrol edilebilmektedir. Bu özelliğin bir başka kullanımı, telsizin bir çağrı aldığında kimliğini göndermesidir (auto acknowledge). Böylece yapılan bir çağrının istenen telsize ulaştığı anlaşılmış olur. Tekrarlayıcı telsizler ANI tonu barındıran çağrıları sorunsuz bir şekilde bozmadan ve geciktirmeden tekrarlayacaktır.

#### 1.6.1.2.3. Kanal Tarama

Kanal Tarama özelliği telsizin yayın olan kanalı bulup, o kanalı izlemesi işlevidir. Bu özellik, birden fazla kanalı izlemek ve izlediği kanallardan herhangi birinden çağrı aldığında, o kanaldan gelen çağrıya cevap vermek isteyen kullanıcılar için tasarlanmıştır.

#### 1.6.1.2.4. Gönderme Zamanını Sınırlama

Bu özellik telsizin göndermede kalma süresini sınırlayarak bas-konuş mandalının sürekli basılı kalması halinde kanalın meşgul edilmesini önler.

#### 1.6.1.2.5. Meşgul Kanal Kilidi

Meşgul Kanal Kilidi olan bir telsizin, kanalda yayın varken gönderme yapması engellenebilir. Böylece kanalda yayın varsa, bas-konuş mandalına basılsa bile bir anda birden fazla telsiz gönderme yapamaz.

Tablo 1. Frekans kümeleri [3].

| FORMAT KARAKTERLERİ | İKİLİ KOD KARŞILIĞI | TON FREKANS KÜMESİ | | |
|---|---|---|---|---|
| QTC | KOD | CCIR | EEA | ZVEI |
| 0 | 0000 | 1981 | 1981 | 2400 |
| 1 | 0001 | 1124 | 1124 | 1060 |
| 2 | 0010 | 1197 | 1197 | 1160 |
| 3 | 0011 | 1275 | 1275 | 1270 |
| 4 | 0100 | 1358 | 1358 | 1400 |
| 5 | 0101 | 1446 | 1446 | 1530 |
| 6 | 0110 | 1540 | 1540 | 1670 |
| 7 | 0111 | 1640 | 1640 | 1830 |
| 8 | 1000 | 1747 | 1747 | 2000 |
| 9 | 1001 | 1860 | 1860 | 2200 |
| A | 1010 | 2400 | 1055 | 2800 |
| B | 1011 | 930 | 930 | 810 |
| C | 1100 | 2247 | 2247 | 970 |
| D | 1101 | 991 | 991 | 886 |
| E | 1110 | 2110 | 2110 | 2600 |
| F | 1111 | Ton Yok | Ton Yok | Ton Yok |

#### 1.6.1.3. Trunk Telsiz Sistemleri

Klasik Telsiz Sistemlerinde kanallar sürekli olarak kullanılmamaktadır. Bundan ötürü farklı kullanıcılara yeni kanallar verilmeksizin var olan kanalları zaman paylaşımlı kullandırarak frekans spektrumu daha verimli kullanılabilir. Bu çözüm Trunk Telsiz Sistemidir. Trunk Telsiz Sistemi bir akıl etrafında toplanmış birden fazla kanallı klasik telsiz sistemi olarak düşünülebilir. Kanallardan birisi sistem ve telsizler arasında işaretleşme için kullanılır ve Kontrol Kanalı olarak adlandırılır. Diğer kanallar ses veya data haberleşmesi için kullanılır ve Trafik Kanalı olarak adlandırılır.

Trunk Telsiz Sisteminde telsiz kullanıcıları görüşmek istedikleri telsiz kullanıcısını ya da grubu sisteme bildirir. Kontrol kanalından gelen istekleri değerlendiren Trunk Telsiz Sistemi ses veya data haberleşme isteğine boş olan trafik kanallarından birisini atar.

Görüşme bitimine kadar kanal, görüşme isteğinde bulunan telsiz ve görüşülmek istenen telsiz veya grup tarafından kullanılır. Kullanılan trafik kanalı görüşme bitimi sonunda boş trafik kanalı listesine dahil edilir ve yeni bir istek için kullanılabilir. Trunk Telsiz Sistemi içindeki trafik kanallarının tümü kullanımdayken gelen data veya ses haberleşme istekleri Kanal Sırası'na alınır. Trafik kanallarından biri boşaldığında, sırada bekleyen isteklerden birisi için kullanılır.

1979'da ABD'de tanıtılan Trunk Telsiz Sistemi üzerinde çalışmalar 1980'lerde hızlandı. ABD'de bazı büyük telsiz firmaları tarafından geliştirilen Trunk Telsiz Sistemleri ortak bir standarda sahip değildir. Buna karşın İngiltere'de DTI (Department of Trade and Industry) telsiz ve sistem arasında işleyecek olan açık işaretleşme standardı olan MPT 1327'nin geliştirilmesini sağladı. Aynı zamanda, bu standarda uygun olarak çalışacak telsizler için de MPT 1343 standardını geliştirdi.

### 1.6.2. İkinci Nesil Telsiz Sistemleri

İkinci nesil telsiz sistemlerinde kullanılan erişim teknikleri;

- TDMA (Time Division Multiple Access- Zaman Bölmeli Çoklu Erişim):

Bir radyo kanalının birden fazla kullanıcı tarafından kullanımına imkân veren iletim modudur. GSM ağlarda yaygın olarak kullanılan bu metod sayesinde tek bir kanal aynı anda 8 abone tarafından kullanılabilir.

- FDMA (Frequency Division Multiple Access- Frekans Bölmeli Çoklu Erişim):

Bireysel çağrıların sık kullanılmadığı, grup başına düşen kullanıcı sayısının yoğun olduğu sistemler için gerekli iletim modudur. Fakat büyük kaplama alanı gereksinimi duyan bir erişim tekniğidir.

İkinci nesil telsiz sistemleri; TETRAPOL, APCO 25 ve TETRA sistemleridir.

#### 1.6.2.1. Tetrapol

TETRAPOL, Fransız PMR üreticisi olan MATRA tarafından ortaya atılmış bir sistemdir. Bu sistem temel olarak FDMA kanal erişim tekniği ve GMSK modülasyon yöntemi üzerine kurulmuştur. Sistemin temel özelliği denenmiş ve karmaşık olmayan teknolojileri kullanmasıdır. Bu sistem TETRAPOL adıyla standartlaşma aşamasına

girmeden önce MATRA tarafından ACROPOL adıyla tasarlanmış ve üretilmiştir. Sistemin özellikleri tablo 2‘de verilmiştir.

Tablo 2. TETRAPOL sistem özellikleri

| | |
|---|---|
| Erişim Tekniği | FDMA |
| Kanal Aralığı | 10/12.5kHz |
| İletişim Modu | Yarı duplex |
| Modülasyon Tipi | GMSK |
| RF Bit Hızı | 8kbps |
| Net Bit Hızı | 4.8–7.2kbps |

#### 1.6.2.2. Apco 25

APCO (Association of Public Safety Communications Officials), ilk olarak 1976–1979 yılları arasında güvenlik grupları tarafından kullanılacak trunk sistemi ile ilgili fonksiyonel sistem gereksinimlerini APCO 16 projesi ile yayınladı. Ancak APCO 16'da belirtilen gereksinimleri karşılamak üzere farklı firmalar tarafından ortaya atılan ürünlerde birlikte çalışma problemleri ortaya çıktı. Bu çalışmada ortaya çıkan problemlerden yola çıkılarak APCO 25 projesi çalışmaları başlatıldı. ABD, APCO 25 sistemi FDMA ve C4FM tekniklerini kullanmaktadır. Sistem ABD ve Kanada güvenlik kuruluşlarının üretici firmalarla ortak çalışmaları sonucunda ortaya çıkmıştır. APCO sisteminin özellikleri tablo 3‘de verilmiştir.

Tablo 3. APCO sistem özellikleri

| | |
|---|---|
| Erişim Tekniği | FDMA |
| Kanal Aralığı | 12,5kHz, 6,25kHz planlanıyor |
| İletişim Modu | Yarı duplex |
| Modülasyon Tipi | C4FM,QPSK-C planlanıyor |
| RF Bit Hızı | 9.6kbps |
| Net Bit Hızı | 6.1–9.6kbps |

#### 1.6.2.3. Tetra

1990 yılında ETSI tarafından geliştirilmesine başlanmıştır. Bu amaçla RES (Radio Equipments and Systems) bünyesinde bir çalışma grubu oluşturulmuştur. TETRA, bütün profesyonel telsiz kullanıcılarının kapsandığı ses+veri ve/veya optimize paket veri sistemlerinden oluşan sayısal ve hücresel bir telsiz haberleşme şebekesidir. TETRA sistem özellikleri tablo 4'de gösterilmiştir.

Tablo 4. TETRA sistem özellikleri

| | |
|---|---|
| Erişim Tekniği | TDMA |
| Kanal Aralığı | 25kHz/4 zaman dilimli |
| İletişim Modu | Tam/yarı duplex |
| Modülasyon Tipi | p/4 DQPSK |
| RF Bit Hızı | 36kbps |
| Net Bit Hızı | 2.4…28.8kbps |

### 1.7. Kriptoloji

Kriptoloji kelimesi, köken olarak eski Yunanca'da yer alan "kryptos logos" kelimelerinden gelmektedir. "Kryptos" kelimesi "gizli dünya" anlamını, "logos" ise sebep-sonuç ilişkisi kurma, mantıksal çözümleme alanı anlamını taşımaktadır. Kelimenin birçok dünya dilindeki karşılığı da bu orijinal halini korumaktadır.

Kriptoloji, kavram olarak şöyle tanımlanabilir: "Kriptoloji, haberleşen iki veya daha fazla tarafın bilgi alışverişini güvenli olarak yapmasını sağlayan, temeli matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bütünüdür."

Günümüzde kriptoloji, matematik, elektronik, optik, bilgisayar bilimleri gibi birçok disiplini kullanan özelleşmiş bir bilim dalı olarak kabul edilmektedir. Kriptolojinin iki temel alt dalı vardır: kriptografi ve kriptoanaliz.

Kriptografi, belgelerin şifrelenmesi ve şifresinin çözülmesi için kullanılan yöntemlere verilen addır.

Kriptoanaliz, kriptografik sistemlerin kurduğu mekanizmaları inceler ve çözmeye çalışır. Kriptoanalizin kriptoloji içindeki önemi çok büyüktür çünkü ortaya konan bir

şifreleme sistemini inceleyerek, zayıf ve kuvvetli yönlerini ortaya koymak için kriptoanaliz kullanılır.

Günümüzde elektronik bilgi sistemlerinin yaygınlaşması kriptolojinin önemini çok fazla arttırmıştır. Kriptolojinin başlıca kullanım alanı hareket halindeki veya depolanmış bilginin şifrelenmesi ve istendiğinde bu şifrenin çözülmesidir. Kriptolojinin temel malzemesi bilgi olduğu için neredeyse sınırsız sayıda uygulamada kullanılması söz konusu olmuştur. Kriptolojinin tarihçesi Ek 1.'de verilmiştir [4].

### 1.8. Haberleşmede Güvenlik

Haberleşen iki tarafın güvenlikle ilgili çeşitli beklentileri vardır. Bu beklentiler haberleşmenin güvenlik öğeleri olarak sınıflandırılmıştır. Haberleşmede güvenlik öğeleri aşağıdaki görülmektedir [4]:

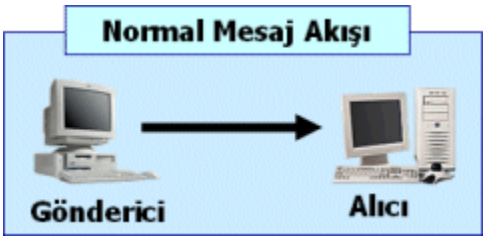
- Gizlilik: Taşınan bilginin içeriğinin gizli kalmasıdır.
- Bütünlük: Taşınan bilginin içeriğinin yolda değiştirilememesidir.
- Kimlik Doğrulama: Bilgiyi gönderen kişinin kimliğinin doğruluğundan emin olmaktır.
- İnkâr Edememezlik: Bilgiyi gönderen veya işleyen kişinin yaptığı işi sonradan inkâr edememesidir.
- Haberleşmenin Sürekliliği: Haberleşmenin kesintiye uğramadan yapılmasıdır.

Günlük hayatta bu güvenlik gereksinimlerini karşılamak için aşağıdaki yöntemler kullanılmaktadır:

- Gizlilik sağlamak için mühürlü zarf,
- Bütünlük sağlamak için imza, barkod, damgalama,
- Kimlik doğrulaması için noter, kimlik kartı, trafik ehliyeti, kişinin şahsen başvuru yapması,
- İnkâr edememezlik için imza, alındı, onay,
- Haberleşmenin sürekliliğini sağlamak için farklı, birbirine alternatif iletişim yolları.

### 1.8.1. Elektronik Tehditler

Haberleşen iki taraf, bilgisayar ağları, kablolu veya kablosuz iletişim kanalları kullanarak bir bilgiyi, mesajı bir taraftan diğerine iletirler. Elektronik ortamda haberleşen taraflar çeşitli tehditlerle karşı karşıya kalırlar. Şekil 3'de normal mesaj akışı verilmiştir.




Şekil 3. Normal mesaj akışı

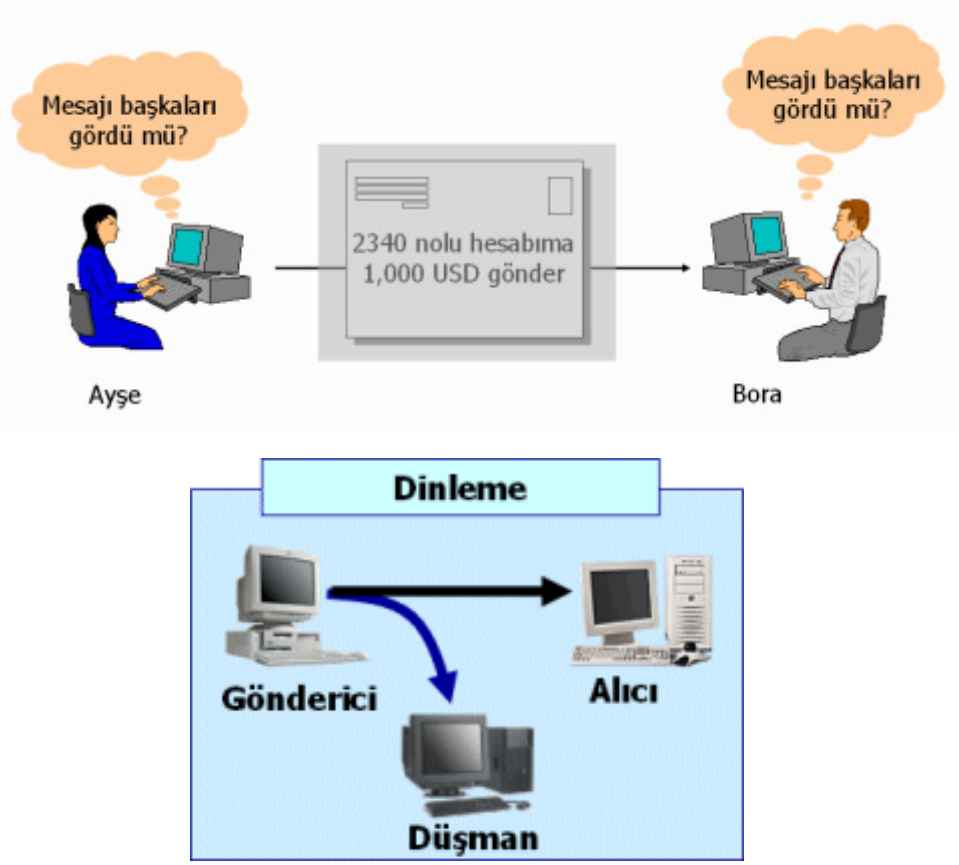
- Gizlilik İhlali
- Bütünlük İhlali
- Kimlik Doğrulama İhlali
- İnkâr Edememezlik İhlali
- Süreklilik İhlali

#### 1.8.1.1. Gizlilik İhlali

Haberleşme kanalını dinleyen saldırgan gönderici ile alıcı arasındaki mesaj trafiğini dinleyebilir ve elde ettiği mesajları okuyarak bu haberleşmenin gizliliğini bozar. Bu tehdit dinleme tehdidi olarak bilinir. Gizlilik ihlali şekil 4'de görülmektedir.

#### 1.8.1.2. Bütünlük İhlali

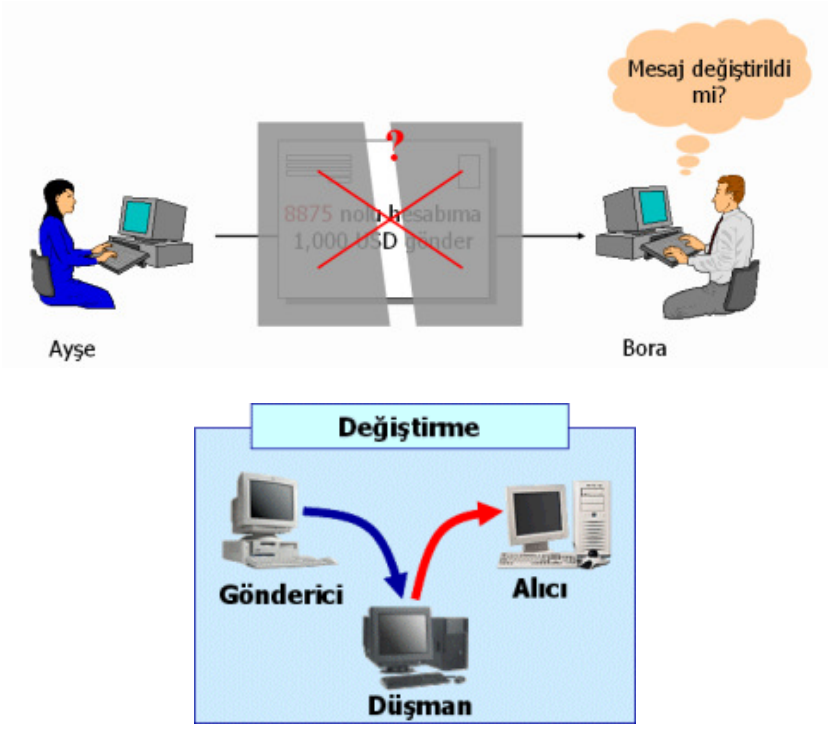
Haberleşmeye müdahale edip göndericinin mesajlarını değiştiren saldırgan, alıcıya giden mesajı istediği şekle sokabilir. Bu tehdit mesajın bütünlüğünü bozan değiştirme tehdididir. Bütünlük ihlali şekil 5'de görülmektedir.



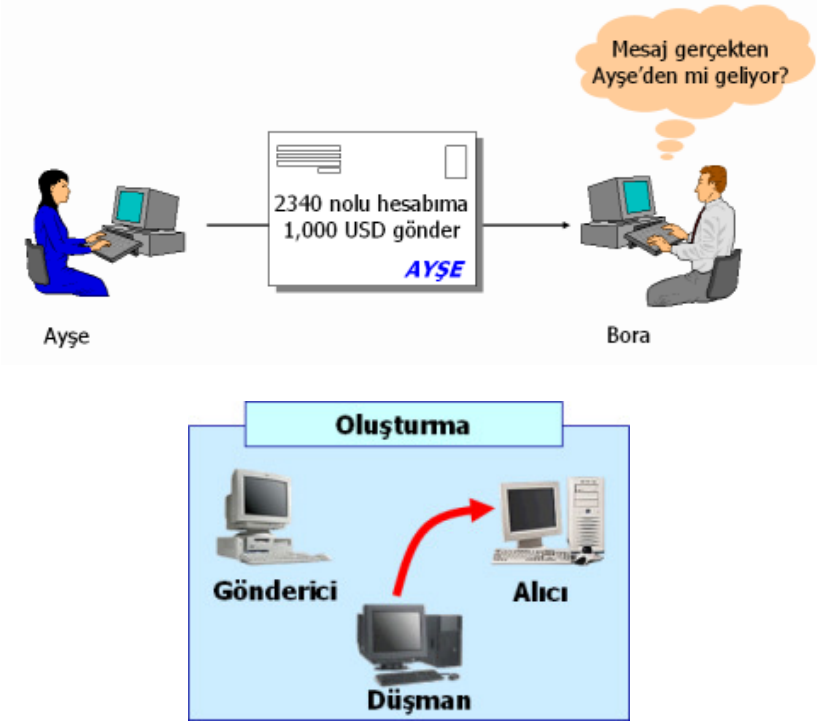

Şekil 4. Gizlilik ihlali

### 1.8.1.3. Kimlik Doğrulama İhlali

Saldırgan, alıcıya göndericinin kimliğini taklit ederek bir mesaj gönderebilir. Bu durumda eğer alıcı güvenilir bir kimlik doğrulaması yapmıyorsa yanlış mesajlarla kandırılabilir. Bu tehdit oluşturma tehdidi olarak bilinir. Kimlik doğrulama ihlali şekil 6'da gösterilmiştir.




Şekil 5. Bütünlük ihlali




Şekil 6. Kimlik doğrulama ihlali

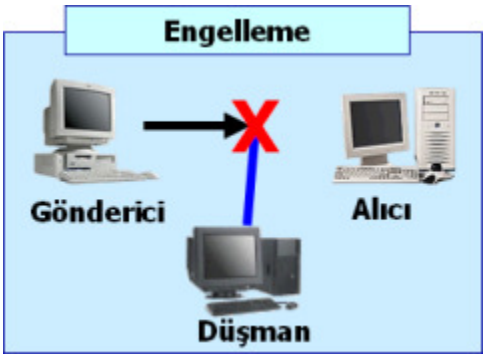
#### 1.8.1.4. İnkâr Edememezlik İhlali

Mesajı gönderen veya alan tarafın bu işi yaptığını inkâr etmesi söz konusu olabilir. Bu kötü niyetli girişimi boşa çıkaracak mekanizmalara ihtiyaç vardır. İnkâr edememezlik ihlali şekil 7'de gösterilmiştir.


Şekil 7. İnkâr edememezlik ihlali

#### 1.8.1.5. Süreklilik İhlali

Saldırgan, haberleşen iki taraf arasındaki hattı veya haberleşme araçlarını kullanılmaz hale getirerek haberleşmenin sürekliliğini engellemeye çalışır. Süreklilik ihlali şekil 8'de gösterilmiştir.




Şekil 8. Süreklilik ihlali

### 1.8.2. Elektronik Tedbirler

Elektronik haberleşmedeki tehditlere karşı yine elektronik tedbirler alınarak korunma sağlanabilir. Bu tehditlere karşı alınabilecek tedbirler ve kullanılabilecek yöntem ve araçlar aşağıda görülmektedir.

- Gizlilik sağlamak için veri şifreleme yöntemleri kullanılır.
- Bütünlük sağlamak için özetleme algoritmaları, mesaj özetleri, sayısal (elektronik) imzalar kullanılır.
- Kimlik doğrulaması için özetleme algoritmaları, mesaj özetleri, sayısal (elektronik) imzalar, sertifikalar kullanılır.
- İnkâr edememezlik için sayısal (elektronik) imzalar, işlem kayıtları kullanılır.
- Süreklilik için yedek sistemler, bakım, yedekleme, alternatif haberleşme kanalları kullanılır.

### 1.8.3. Elektronik Güvenlik Yöntemlerinin Karşılaştırılması

Elektronik tehditlere karşı kullanılan yöntemlerin karşılaştırması tablo 5'de gösterilmiştir.

Tablo 5. Elektronik güvenlik yöntemleri

| | Kimlik Doğrulama | Gizlilik | Bütünlük | İnkâr Edememe |
|---|---|---|---|---|
| Anti-virüs | | | ✓ | |
| Güvenlik Duvarları | ✓ | ✓ | | |
| Erişim Denetimi | ✓ | ✓ | | |
| Şifreleme | | ✓ | | |
| Açık Anahtar Altyapısı | ✓ | ✓ | ✓ | ✓ |

- Anti-virüs programları, CRC32 gibi "checksum" (bir çeşit özet) kullanarak bilgisayardaki programların kontrol dışı değiştirilip değiştirilmediğini kontrol ederler. Bu nedenle sadece bütünlük hizmetini verebilirler.
- Güvenlik duvarları (firewall), kimlik doğrulama yaparak belirli kaynaklara erişimi sınırlarlar. Bu nedenle sadece kimlik doğrulama ve gizlilik hizmetlerini sağlarlar.
- Şifreleme programları veya yöntemleri tek başlarına kullanıldığında sadece gizlilik hizmetini sağlayabilirler.
- Açık anahtar altyapısı kimlik doğrulama, gizlilik, bütünlük ve inkâr edememe hizmetlerini sağlayarak çok daha kapsamlı çözüm sunmaktadır.

## 1.9. Şifreleme

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.

Şifreleme yönteminde aranan bir takım özellikler vardır. Bunlar aşağıda listelenmiştir:

- Şifreleme ve şifre çözme işleminin zorluğu ihtiyaç duyulan güvenlikle doğru orantılı olmalıdır. Çok önemli olmayan bir bilginin şifrelenmesi için bilginin kendisinden daha fazla işgücü ve zaman harcanması verimli olmayacaktır.
- Anahtar seçimi ve şifreleme algoritması özel koşullara bağlı olmamalıdır. Şifreleme yöntemi her türlü bilgi için aynı şekilde çalışmalıdır.
- Sürecin gerçeklenmesi mümkün olduğunca basit olmalıdır. 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. Saldırılara karşı bu özellik koruyucu olacaktır. Ayrıca haberleşme hattında meydana gelen bir hata bütün mesajın bozulmasına neden olmayacağı için bu özellik tercih edilmektedir.
- Kullanılan algoritmanın karıştırma özelliği olmalıdır. Mesajın şifrelenmiş hali ile açık hali arasında ilişki kurulması çok zor olmalıdır.

- Kullanılan algoritmanın dağıtma özelliği olmalıdır. Mesajın açık hali şifreli hale gelirken içerdiği kelime ve harf grupları şifreli mesajın içinde olabildiğince dağıtılmalıdır.

### 1.9.1. Basit Şifreleme Yöntemleri

Basit şifreleme yöntemleri genellikle kâğıt kalem kullanarak gerçekleştirilebilen, çok karışık matematik temellere dayanmayan sistemlerdir. En gelişmiş örnekleri mekanik cihazlar olan basit şifreleme yöntemleri, elektronik cihazların kullanılmaya başlanmasıyla beraber ortadan kalkmıştır.

#### 1.9.1.1. Mono Alfabetik Şifreleme

En eski ve basit şifreleme yöntemlerinden birisi olan Sezar yöntemi mono alfabetik şifrelemenin tipik bir örneğidir. Sezar döneminde kullanılan bu yöntemde harflerin yeri değiştirilir. Şifrelenecek metindeki harfler alfabede 3 harf kaydırılarak değiştirilir.

**Sezar Şifresi :** $ci = E(pi) = pi + 3 \bmod 29$ (1)

Açık Mesaj : Gizli Bilgi
Şifreli Mesaj : Ilcol Dloıl

Bu yöntemin biraz daha gelişmişi olan tablo yönteminde ise alfabedeki her harf başka bir harfle yer değiştirir ama bu bir kurala bağlı olmadan karışık bir şekilde yapılır.

ABCÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZ

CÇAVYJŞÜZKÖTUENOİPFGILĞHRMBDS

Mono alfabetik şifreleme yöntemleri bilgisayar yardımıyla çok kısa sürede kırılabilir. Bu yöntemler kullanılan dildeki harflerin yerini değiştirir ama harflerin kullanım sıklığını (frekansını) değiştirmez. Örneğin Türkçe'de en çok kullanılan harf olan "a" harfi tablo

yöntemi kullanılarak "c" harfi ile yer değiştirilirse elde edilecek şifreli metinde en çok tekrar eden harfin "c" olduğu görülür ve bunun "a" harfi olabileceği tahmin edilerek şifre çözülmeye başlanabilir.

### 1.9.1.2. Poli Alfabetik Şifreleme

Bu tip şifrelemede, mono alfabetik yöntemlerden farklı olarak bir harf değiştirilince her seferinde aynı harfe dönüşmez. Bu yöntemlere güzel bir örnek Vigenere tablosudur. Vigenere tablosu tablo 6'da gösterilmiştir.

Tablo 6. Vigenere tablosu [4].

| | 0 | | | | | 5 | | | | | 10 | | | | | 15 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **A** | **B** | **C** | **Ç** | **D** | **E** | **F** | **G** | **Ğ** | **H** | **I** | **İ** | **J** | **K** | **L** | **M** | **N** | **O** |
| **A** | a | b | c | ç | d | e | f | g | ğ | h | ı | i | j | k | l | m | n | o |
| **B** | b | c | ç | d | e | f | g | ğ | h | ı | i | j | k | l | m | n | o | ö |
| **C** | c | ç | d | e | f | g | ğ | h | ı | i | j | k | l | m | n | o | ö | p |
| **Ç** | ç | d | e | f | g | ğ | h | ı | i | j | k | l | m | n | o | ö | p | r |
| **D** | d | e | f | g | ğ | h | ı | i | j | k | l | m | n | o | ö | p | r | s |
| **E** | e | f | g | ğ | h | ı | i | j | k | l | m | n | o | ö | p | r | s | ş |
| **F** | f | g | ğ | h | ı | i | j | k | l | m | n | o | ö | p | r | s | ş | t |
| **G** | g | ğ | h | ı | i | j | k | l | m | n | o | ö | p | r | s | ş | t | u |
| **Ğ** | ğ | h | ı | i | j | k | l | m | n | o | ö | p | r | s | ş | t | u | ü |
| **H** | h | ı | i | j | k | l | m | n | o | ö | p | r | s | ş | t | u | ü | v |
| **I** | ı | i | j | k | l | m | n | o | ö | p | r | s | ş | t | u | ü | v | y |
| **İ** | i | j | k | l | m | n | o | ö | p | r | s | ş | t | u | ü | v | y | z |
| **J** | j | k | l | m | n | o | ö | p | r | s | ş | t | u | ü | v | y | z | a |
| **K** | k | l | m | n | o | ö | p | r | s | ş | t | u | ü | v | y | z | a | b |
| **L** | l | m | n | o | ö | p | r | s | ş | t | u | ü | v | y | z | a | b | c |
| **M** | m | n | o | ö | p | r | s | ş | t | u | ü | v | y | z | a | b | c | ç |

Bu yöntemde oluşturulan tablo ve bir anahtar kelime kullanılarak şifreleme yapılır.

Şifreleme

Açık Mesaj (sütun) : BULUŞ MAYER İANKA RA

Anahtar Kelime (satır) : KALEM KALEM KALEM KALEM...

Şifreli Mesaj : LUZAĞ ZAJIF UABÖM DA...

Şifre Çözme

Şifreli Mesaj (tablo) : LUZAĞ ZAJIF UABÖM DA...

Anahtar Kelime (satır) : KALEM KALEM KALEM KALEM...

Açık Mesaj (sütun) : BULUŞ MAYER İANKA RA

Poli alfabetik şifreleme yöntemleri de bilgisayar yardımıyla ve frekans sayımı ile çok kolay ve çabuk çözülebilmektedir.

#### 1.9.1.3. Tek Kullanımlık Karakter Dizisi (One-time Pad)

Bu basit şifreleme yönteminde rastgele üretilen bir karakter (harf veya rakam) dizisi kullanılarak şifreleme yapılır. Açık mesaj içinde yer alan her karakter, üretilen dizide karşısına denk gelen karakterle işleme sokularak (Örneğin modüler toplama işlemi) şifreli mesaj elde edilir. Mesajı çözmek için rastgele dizinin bilinmesi gereklidir. Bu yönteme Vernam şifreleme yöntemi denir.

Açık Mesaj : BULUSMAYERIANKARA

Rastgele Dizi : DEFRYPLCNMLJKHFGH

Şifreli Mesaj : RLDYDOY...

Bu yöntemin güvenliği rastgele üretilen diziye bağlıdır. Bu dizi gerçekten rastgele üretilmelidir, eğer bir kurala bağlı olarak üretilirse ve bu kural saldırgan tarafından bilinirse sistem kırılabilir. Bu tehdit dışında sistem mükemmel bir şifreleme sistemidir ve ilk olarak 1917'de bulunup "teletype" makinelerinde kullanılmıştır.

### 1.9.2. Kriptoanaliz Yöntemleri

Kriptoanaliz, bir şifreleme sistemini veya sadece şifreli mesajı inceleyerek, şifreli mesajın açık halini elde etmeye çalışan kriptoloji disiplinidir. Kriptoanaliz çalışması sırasında kriptoanaliz yapan kişinin elinde çoğu zaman çok az bilgi vardır. Değişik durumlar aşağıda listelenmiştir:

- Şifrelenmiş mesaj analizi: Kriptoanaliz yapan kişinin elinde sadece şifreli bir mesaj vardır. Mesajın açık hali ile ilgili hiç bir ipucu yoktur.
- Tam bir açık mesajın analizi: Kriptoanaliz yapan kişinin elinde bütün bir mesajın hem açık hali hem de şifreli hali vardır.
- Yarım olarak elde edilmiş açık mesajın analizi: Kriptoanaliz yapan kişi bir mesajın açık halinin belirli bir kısmına ve şifreli halinin tamamına sahiptir.
- İstenen açık mesajın şifrelenmiş halinin analizi: Kriptoanaliz yapan kişi istediği açık mesajın şifreli halini elde edebilmektedir. Bu şifrelemeyi yapan cihazın veya yazılımın çalışan bir kopyasına sahip olarak veya şifrelemeyi yapan sistemi fark edilmeden kullanmakla mümkün olur.
- Şifreli mesajın şifreleme algoritması bilinerek analizi: Kriptoanaliz yapan kişi elindeki şifreli mesajın hangi yöntemle şifrelendiğini bilmektedir.

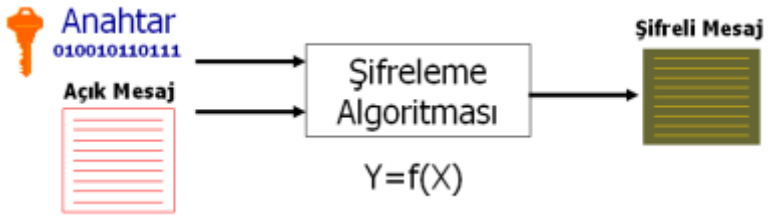
Kullanılan kriptoanaliz yöntemleri ise aşağıda listelenmiştir:

- Kaba kuvvet yöntemi: Bu yöntem bir şifreleme algoritması tarafından kullanılabilecek tüm anahtarları tek tek veya belirli bir mantık çerçevesinde deneyerek şifreyi çözmeye çalışır.
- Diferansiyel kriptoanaliz: Bu yöntem bilinen açık-şifreli mesaj çiftleri arasındaki farkların hesaplanması temeline dayanır.

### 1.9.3. Güvenli Şifreleme Yöntemleri

Güvenli şifreleme yöntemleri klasik şifreleme yöntemlerinin zayıf yönlerini ortadan kaldıran ve kriptoanalize karşı dirençli olan algoritmalarla gerçeklenir. Bu yöntemler elektronik sistemlerde (bilgisayar, telekomünikasyon vb) kullanılır ve ikili düzende (binary) saklanan ve taşınan bilgi üzerinde uygulanır. Bu nedenle anahtar olarak bit dizileri kullanılır. Güvenli şifreleme şekil 9'da görülmektedir.

Bir şifreleme algoritmasının güvenliğini belirleyen en önemli değişkenlerden birisi anahtar uzunluğudur. Örneğin 64 bitlik bir anahtar kullanan şifreleme algoritması için toplam anahtar sayısı $2^{64}= 1,8 \times 10^{19}$ adettir. Şifrelemede bu anahtarlardan herhangi birisi kullanılabileceği için bu anahtarı tahmin yoluyla elde etme olasılığı çok düşüktür.




Şekil 9. Güvenli şifreleme

64 bitlik Anahtar;

1100101010110001 0001101000000111 0110100010011110 1100111010011011

Güvenli şifreleme temel olarak iki çeşittir:

- Simetrik Kriptografi
- Asimetrik Kriptografi

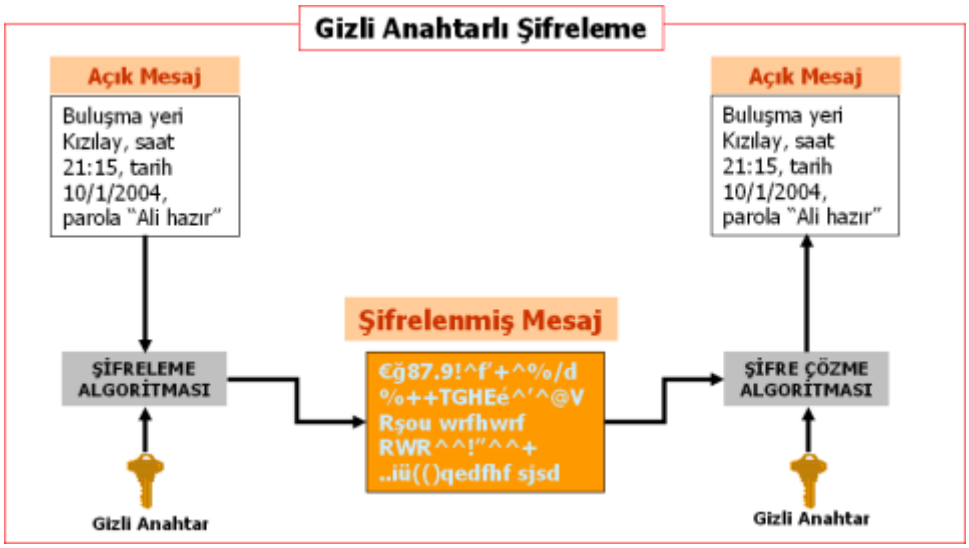
#### 1.9.3.1. Simetrik Kriptografi

Simetrik kriptografide, şifreleme ve şifre açma işlemi aynı anahtar ile yapılır. Simetrik kriptografide bu anahtar gizli tutulmalıdır. Bu nedenle, bu tip sistemlere gizli anahtarlı kriptografi sistemi adı da verilmektedir. Gizli anahtarlı şifreleme şekil 10'da görülmektedir.

Bu sistemde haberleşen taraflar:

- Aynı şifreleme algoritmasını kullanırlar.
- Birbirine uyumlu gerçeklemeler kullanırlar.
- Aynı anahtarı kullanırlar.

Simetrik kriptografinin en önemli öğesi anahtar gizliliği olduğu için birden fazla kişinin haberleştiği bir ortamda anahtar yönetimi büyük dikkat gerektirmektedir.




Şekil 10. Gizli anahtarlı şifreleme

#### 1.9.3.1.1. Simetrik Kriptografi Anahtar Yönetimi

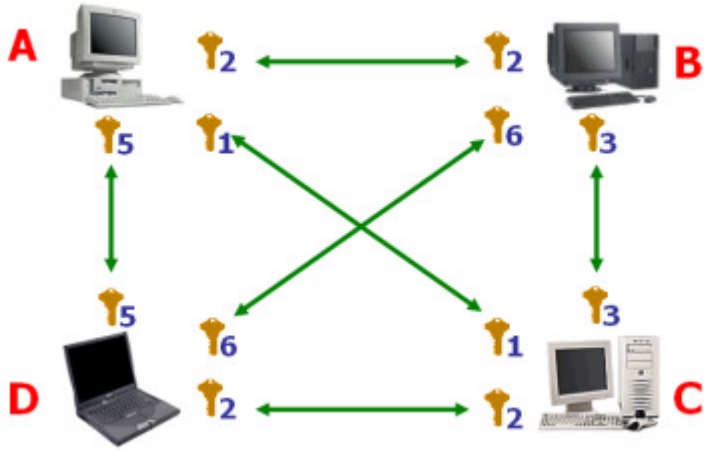
##### 1.9.3.1.1.1. Birden-Çoğa (One-to-Many) Anahtar Yönetimi

Bu yöntemde haberleşen tüm taraflar aynı gizli anahtarı kullanırlar. Bu nedenle herkes birbirinin şifreli mesajlarını açıp okuyabilir (Şekil 11).


Şekil 11. Birden-çoğa (one-to-many) anahtar yönetimi

#### 1.9.3.1.1.2. Çoktan-Çoğa (Many-to-Many) Anahtar Yönetimi

Bu yöntemde haberleşen tüm taraflar kendi aralarında bir gizli anahtar kullanmak üzere anlaşırlar. Bu nedenle herkes şifreli haberleşeceği her kişi için bir anahtar tutar (Şekil 12).




Şekil 12. Çoktan-çoğa (many-to-many) anahtar yönetimi

Bu yöntem sistemdeki kişi sayısına bağlı olarak çok fazla anahtar üretimini gerektirdiği için çok kullanışlı değildir. Anahtar sayısının kullanıcı sayısına bağlı olarak artışı tablo 7'de görülmektedir.

Tablo 7. Simetrik kriptografide anahtar sayısının kullanıcı sayısına bağlı olarak artışı

| **Kullanıcı Sayısı** | **Anahtar Sayısı** |
|---|---|
| 3 | 3 |
| 4 | 6 |
| 10 | 45 |
| 100 | 4,950 |
| 1000 | 499,500 |
| 10000 | 49,995,000 |
| N | n*(n–1) /2 |

#### 1.9.3.1.2. Simetrik Kriptografinin Artıları Eksileri

Simetrik kriptografinin kuvvetli yönleri aşağıdaki gibi özetlenebilir:

- Algoritmalar hızlıdır.
- Algoritmaların donanımla gerçeklenmesi kolaydır.
- "Gizlilik" güvenlik hizmetini yerine getirir.

Simetrik kriptografinin zayıf yönleri aşağıdaki gibidir:

- Ölçeklenebilir değildir.
- Güvenli anahtar dağıtımı zordur.
- "Bütünlük" ve "Kimlik Doğrulama" güvenlik hizmetlerini gerçeklemek zordur.

#### 1.9.3.1.3. Simetrik Kriptografi Algoritmaları

Simetrik kriptografi algoritmaları başlıca iki sınıfta ele alınabilir:

- Blok Şifreleme Algoritmaları:

Bu tip algoritmalar şifrelenecek veriyi sabit uzunlukta bloklar olarak şifreleme fonksiyonuna alırlar ve aynı uzunlukta şifrelenmiş veri blokları üretirler. Bu algoritmalara örnek olarak AES, DES, IDEA, Skipjack, RC5 vb. verilebilir. Bu algoritmalar aşağıdaki özellikleri gerçeklemeye çalışırlar:

- Karıştırma: Anahtar ve şifrelenmiş mesaj arasındaki ilişki olabildiğince karışık olmalıdır.
- Dağıtma: Tek bir açık mesaj karakterinin etkisi olabildiğince fazla şifrelenmiş karaktere yansıtılmalıdır.
- Transpoze İşlemi: Şifrelemeye başlamadan önce açık mesajın içeriği değişik bir sıraya konur.
- Yer Değiştirme İşlemi: Tekrar eden kalıplar başka kalıplarla değiştirilir.

- Bit Katarı (dizi) Şifreleme Algoritmaları:

Bu tip algoritmalar veriyi akan bir bit dizisi olarak alırlar. Vernam tipindeki bu algoritmalarda rastgele bit dizisi üretiminin kendini tekrarlamayan bir yapıda olması gereklidir. Örnek algoritmalar RC2, RC4 vb.

#### 1.9.3.1.3.1. Blok Şifreleme Algoritmaları

Blok şifreleme algoritmaları veriyi bloklar halinde işler. Bu işleme yöntemi bazen blokları birbirinden ayrı olarak bazen de birbirine bağlı olarak kullanır. Bu nedenle blok şifrelemede değişik kullanımlar ortaya çıkmıştır. Bunlardan iki tanesi aşağıda görüldüğü gibi çalışır.

Elektronik Kod Kitabı (Electronic Codebook, ECB):

- Her açık mesaj bloğu ayrı ayrı şifrelenir.
- Biçimi belli olan veri için güvenli değildir.
- Şifrelenmiş mesaj blokları birbirinden bağımsızdır.

Şifre Bloğu Zincirleme (Cipher Block Chaining, CBC):

- Bir şifreleme adımının çıktısı diğer şifreleme adımının girdisini etkiler.
- Kendi kendini işlemci saatine uygun olarak senkronize eder.
- Şifrelenmiş bloklardan biri hatalıysa en fazla iki bloğun şifresiz hali hatalı olur.

En fazla kullanılan blok şifreleme algoritmaları aşağıda ele alınmıştır.

➢ DES (Data Encryption Standard) Algoritması:

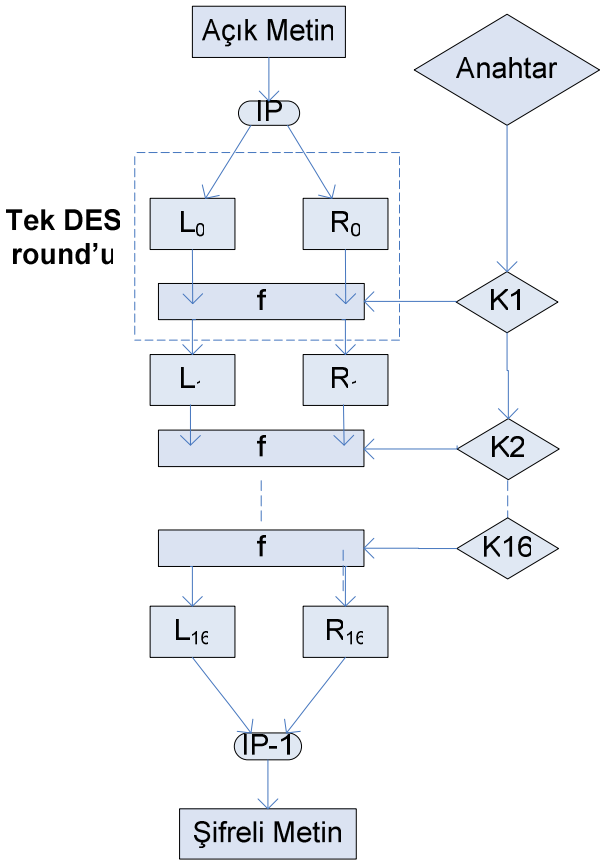
Bankacılık ve finans sektöründe ağırlıklı olarak kullanılan bu algoritma IBM firması tarafından 1974 yılında bulunmuş ve 1977 yılında Amerikan Standardı olarak kabul edilmiştir. Üzerinde en çok çalışılmış olan algoritmadır. DES core algoritması şekil 13'de verilmiştir.

DES'in en büyük zaafı onun 56 bit anahtarıdır. Geliştirildiği zamanlarda çok iyi bir şifreleme algoritması olmasına rağmen modern bilgisayarlar tarafından yapılan anahtar saldırılarına karşı yetersiz kalmaya başladı. Günümüzde bu algoritma 3 DES (triple DES) şeklinde, üç farklı anahtarla aynı bloğa 3 defa DES uygulanarak da kullanılmaktadır. Algoritmanın kullanılması için herhangi bir lisans ödenmesi gerekmemektedir.

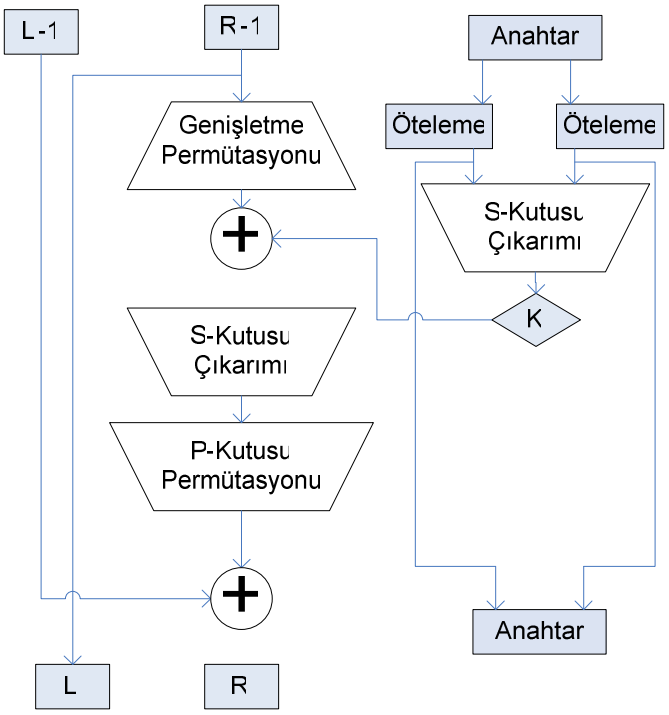
Daha büyük şifreleme ihtiyacının bir sonucu olarak DES Triple-DES şeklinde geliştirildi. Triple-DES, 3 adet 56 bitlik anahtarı kullanarak şifreleme yapar. Bu 168 bitlik anahtar gücüne eşit bir güç demektir. Bu uygulama bununla beraber şifreleme ve şifreleme çözme için 3 kat fazla çevrim gerektirir. Bu da DES'in ikinci bir zayıflığına dikkati çeker. O da hızdır. DES donanım üzerinde yürütülmek üzere geliştirildi. Ve yazılımda DES'in yürütülmesi yazılım performansının iyi olması niyetiyle geliştirilen diğer standartlardan sıkça daha az etkilidir [5].

DES karıştırma ve yayılma şifreleme tekniğine dayanır. Karıştırma yer değiştirme ile başarılır. Özellikle verinin seçilen bölgeleri orijinal veriden takip eden bölgeler ile yer değiştirilir. Yer değiştirilen verinin seçimi anahtara ve orijinal sade metne bağlıdır. Yayılma permütasyon ile başarılır. Farklı kısımların sırası yeniden düzenlenerek veri permute (değiş tokuş) edilir. Bu permütasyonlar, yer değiştirmeye benzer şekilde, anahtar ve orijinal yalın metne bağlıdır. Yer değiştirmeler ve permütasyonlar DES algoritması tarafından belirlenir. Veri ve anahtarın seçilen kısımları matematiksel olarak işlenir. Ve bir look-up tablosuna giriş olarak kullanır. DES'de bu tablolar sırasıyla yer değiştirme tabloları ve permütasyon tabloları S kutuları ve P kutuları olarak adlandırılır. Yazılımda bu look-up tabloları diziye indeks olarak kullanılan anahtar/veri girişi ve diziler olarak gerçekleştirilir. Genellikle S ve P kutuları yer değiştirme ve takip eden permütasyon bir tek look-up ile her roundun yapılabilmesi için birleştirilir. S ve P kutu dizilerine girişleri hesaplayabilmek için veri parçaları anahtar parçaları ile OR (veya)'lanır. 64 bitlik verinin 32 bitlik yarılarından biri ve anahtar kullanılır. Veri yarısından anahtar daha uzun olduğu için 32 bit veri yarısı bitlerini tekrar düzenleyen kesin bitleri tekrar eden 48 bitlik ürünü oluşturmak üzere genişletilmiş bir permütasyona yollanır. Benzer şekilde 56 bitlik anahtar bitlerini tekrar düzenleyen sıkı bir permütasyon işlemine uğrar. Bazı bitler atılarak 48 bitlik ürüne dönüştürülür. Bu look-up tablolarına girişleri üreten anahtar, veri üzerin-deki hesaplamalar ve S ve P kutu look-upları DES'in bir tek çevrimini meydana getirir (Şekil 14).

S ve P kutu yer değiştirme permütasyon süreci 16 defa tekrar edilerek DES algoritmasının 16 roundu oluşur. Aynı zamanda başlatma ve sonuç permütasyonlarıda vardır. 16 rounddan önce ve sonra meydana gelirler. Bu başlatma ve final permütasyonları tarihsel nedenlerden dolayı donanım üzerinde uygulama ile uğraşmak için vardır. Algoritmanın güvenliğini geliştirmez. Bu nedenden dolayı onlar bazı zamanlar DES'in uygulamasına ayrılır. Bununla beraber onlar bu analizde DES'in teknik tanımının parçası olarak bulunur.




Şekil 13. DES core algoritması




Şekil 14. Genişletilmiş tek round

➢ AES (Advanced Encryption Standard) Algoritması:

A.B.D'de NIST (National Institute of Standards and Technology) tarafından açılan bir yarışma sonucunda yeni Amerikan standardı olarak seçilmiş olan algoritmadır (Kasım 2001). Algoritmanın tasarımcıları Belçikalı Joan Daemen ve Vincent Rijmen'dir. Algoritmanın orijinal adı Rijndael'dir. 2003 yılından itibaren yaygın olarak kullanıma girmiştir. Bu algoritma seçime göre 128 bit, 192 bit ve 256 bit uzunluğunda anahtarlar kullanmaktadır. Algoritmanın blok boyu 128 bit olarak standartlaştırılmıştır.

#### 1.9.3.1.3.2. Bit Katarı (Dizi) Şifreleme Algoritmaları

Bu tip algoritmalar veriyi akan bir bit dizisi olarak alırlar. Başlıca iki grup altında toplanırlar:

➢ Senkron Algoritmalar:

- Anahtarı oluşturan bit katarı açık mesajdan bağımsız olarak üretilir.
- Hata izole olarak kalır, katarı etkilemez.
- Açık mesajla anahtar arasında mükemmel senkronizasyon gerektirir.

➢ Kendi Kendine Senkronize Algoritmalar:

- Anahtarı oluşturan bit katarı önceden üretilmiş şifreli mesaj bloklarıyla ilişkilidir.
- Hata izole olarak kalır.
- Kendi kendine senkronize olabilir.

Bit katarı şifreleme algoritmaları genellikle hız gerektiren uygulamalarda kullanılırlar. Bunlar arasında SSL protokolü tarafından da kullanılan RC4 algoritması yer almaktadır.f

##### 1.9.3.1.3.2.1. RC4 Algoritması

Ronald Rivest, RSA tarafından 1987 yılında bulunmuştur. 1994 yılında meçhul kişilerce kaynak kodu internette yayınlanmıştır. Kullanımı lisans gerektirmektedir.

- Değişken anahtar uzunluğuna sahiptir.
- Güvenliği rasgele bir permütasyon kullanımına bağlıdır.
- Tekrarlama periyodu 10100'den daha büyüktür.
- Bilinen kötü anahtar yoktur.

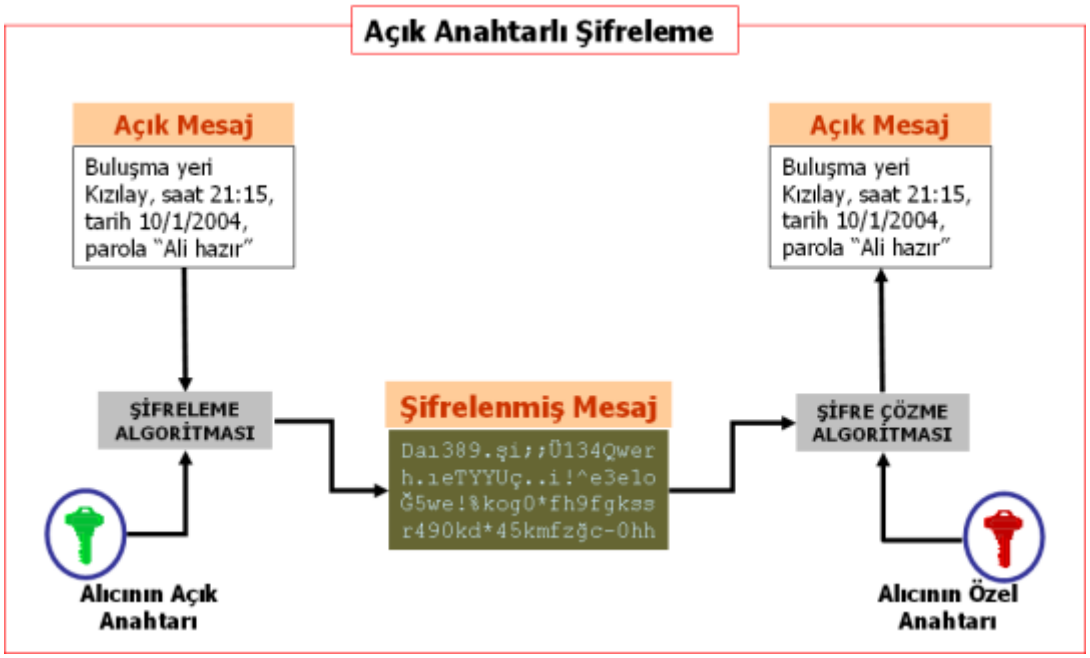
- Şifreleme hızı yaklaşık olarak Megabyte/sn seviyesindedir.

### 1.9.3.2. Asimetrik Kriptografi

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 gerekli kişilere verilebilir ve başka kişilerle paylaşılabilir. Bu özelliğinden dolayı asimetrik kriptografi, açık anahtarlı şifreleme adıyla da anılır. Açık anahtarlı şifreleme şekil 15'de gösterilmiştir.

Bu sistemi kullanarak haberleşen taraflar:

- Aynı şifreleme algoritmasını kullanırlar.
- Birbiriyle uyumlu gerçeklemeler kullanırlar.
- Gerekli anahtarlara erişebilirler.




Şekil 15. Açık anahtarlı şifreleme

#### 1.9.3.2.1. Asimetrik Kriptografi Anahtar Yönetimi

Asimetrik kriptografi için anahtar yönetimi çok önemlidir. Anahtar yönetimi için dikkat edilmesi gereken noktalar şöyle sıralanabilir:

- Açık anahtarlar kontrollü olarak bir otorite tarafından yayınlanmalı ve değiştirilmeleri önlenmelidir.
- Anahtar çiftleri merkezi bir otorite tarafından üretilebilir veya her kullanıcı kendi anahtar çiftini üretebilir.
- Şifreleme ve imzalama için ayrı ayrı anahtar çiftleri olmalıdır. Çok özel durumlar için imzalama ve şifreleme anahtar çiftlerinin aynı olmasına izin verilebilir.
- Anahtar iptalleri kontrollü bir şekilde yapılmalı ve duyurulmalıdır.

Asimetrik kriptografi için anahtar yönetimi simetrik kriptografiye göre daha kolaydır çünkü bir kullanıcıyla şifreli haberleşmek isteyen kişi karşı tarafın açık anahtarına ihtiyaç duyar. Bu açık anahtar kamuya açık olarak yayınlandığı için sisteme giren bir kişi için sadece bir anahtar çifti üretmek yeterli olmaktadır. Anahtar sayısının kullanıcı sayısına bağlı olarak artışı tablo 8'de verilmiştir.

Tablo 8. Asimetrik kriptografide anahtar sayısının kullanıcı sayısına bağlı olarak artışı

| **Kullanıcı Sayısı** | **Anahtar Çifti Sayısı** |
|---|---|
| 3 | 3 |
| 10 | 10 |
| 100 | 100 |
| 1000 | 1000 |
| 10000 | 10000 |
| N | N |

#### 1.9.3.2.2. Asimetrik Kriptografi Artıları Eksileri

Asimetrik kriptografinin kuvvetli yönleri aşağıdaki gibi özetlenebilir:

- Anahtar yönetimi ölçeklenebilir.
- Kripto-analize karşı dirençli (Kırılması zor).
- Bütünlük, kimlik doğrulama ve inkâr edememezlik güvenlik hizmetleri sağlanabilir.

Asimetrik kriptografinin zayıf yönleri ise aşağıdaki gibidir:

- Algoritmalar genel olarak yavaş çalışırlar. Simetrik kriptografi algoritmalarına göre yaklaşık 1500 kat daha yavaştırlar.

- Anahtar uzunluğu bazı durumlar için kullanışlı değildir. Mobil cihazlar için klasik algoritma anahtar uzunlukları sorunlu olabilir.

#### 1.9.3.2.3. Asimetrik (Açık Anahtarlı) Kriptografi Algoritmaları

Başlıca asimetrik kriptografi algoritmaları RSA, Eliptik Eğri Sistemleri, El Gamal ve Diffie-Hellman anahtar belirleme olarak sıralanabilir. Asimetrik kriptografi algoritmaları, simetrik algoritmalardan farklı olarak çözülmesi zor olan matematiksel problemlere dayanır.

##### 1.9.3.2.3.1. RSA Algoritması

En yaygın olarak kullanılan asimetrik algoritmadır. R. Rivest, A. Shamir, L. Adleman tarafından 1977 yılında bulunmuş ve 1978 yılında yayınlanmıştır. Adını mucitlerinin isimlerinin ilk harflerinden almıştır. Aşağıdaki özelliklere sahiptir:

- Açık anahtar kriptografik sistemi ve sayısal imzalama yöntemi olarak kullanılır.
- Çarpanlarına ayırma problemi üzerine inşa edilmiştir.
- Bileşik tam sayı olan n'i oluşturan, asal sayılar p ve q bulunur, öyleki n=pq 'dir.
- Yeterince büyük bir n için kırılması çok zordur.
- Ayrıca kök bulma problemine de dayanır.
- Çok güvenlidir fakat fazla hızlı değildir.

Algoritmanın kullandığı parametreler aşağıda verilmiştir;

Açık anahtar : n, e

Özel anahtar : d

n bileşik bir tamsayıdır ("modulus").

e bir tamsayıdır ("açık üs ifadesi").

d bir tamsayıdır ("gizli üs ifadesi").

öyleki

$$ed \equiv 1(\mathrm{mod}(p-1)(q-1)) \tag{2}$$

ve p, q sayıları n'nin asal çarpanlarıdır.

Algoritmanın kullanımı ile ilgili aşağıda bir örnek verilmiştir.

Ayşe, Bora'ya m mesajını şifreli göndermek için:

m'nin e'inci üssünü alır, yani m'yi Bora'nın açık anahtarı ile şifreler:

$$c = me(\mathrm{mod}\, n) \tag{3}$$

c ("şifreli mesajı")' yi Bora'ya gönderir.

Bora c sayısının d'nci üssünü alır, yani c'nin şifresini kendi özel anahtarını kullanarak çözer:

$$m = cd(\mathrm{mod}\, n) \tag{4}$$

Algoritmayı inceleyecek olursak;

- Ayşe'nin işi kolaydır, sadece iki tane modüler çarpma işlemi yapar.
- Bora'nın işi kolaydır, 1.5logn tane modüler çarpma yapar.
- Eğer asal sayılar p, q bilinirse işlem daha hızlı yapılabilir.
- Düşmanın işi zordur çünkü kök bulma ya da çarpanlarına ayırma problemini çözmelidir.
- Etkili bir çözümü bulunmamıştır.
- Modulus n sayısı arttıkça algoritmanın güvenliği artar.

## 1.10. Kripto Sistemlerinin Karşılaştırılması

Asimetrik ve simetrik kriptografi sistemlerinin özellikleri tablo 9'da verilmiştir.

Tablo 9. Asimetrik ve simetrik kriptografi sistemlerinin karşılaştırılması

| **Konu** | **Simetrik Kriptografi** | **Asimetrik Kriptografi** |
|---|---|---|
| Gizlilik | Sağlar | Sağlar |
| Bütünlük | - | Sağlar |
| Kimlik doğrulama | - | Sağlar |
| İnkâr Edememezlik | - | Sağlar |
| Performans | Hızlı | Yavaş |
| Güvenlik | Anahtar uzunluğuna bağlı | Anahtar uzunluğuna bağlı |

## 1.11. Kriptografik Algoritmaların Gücü

Kriptografik bir algoritma bir anahtar kullanarak çalışıyorsa, teorik olarak olası tüm anahtarlar denenerek çözülebilir. Olası anahtarların denenmesindeki zorluk anahtarın uzunluğu ile üstel olarak doğru orantılıdır. Örneğin 16 bitlik bir anahtar ile en çok 216 tane yani 65536 farklı anahtar oluşturulabilir. Bugünün 40, 56, 64 veya 128 bitlik anahtarlı sistemler büyük şirketlerin veya devletlerin yapabilecekleri yatırımlarla kırılabilecekleri gibi bunu, organize olmuş suçlular da yapabilir. Bunun düşünülebilecek en uç örneği; SETI projesinin son zamanlarında olduğu gibi; bireysel internet kullanıcılarının mikro bilgisayarlarının dahi, farkında olunmadan yüklenen programların yardımı ile paralel şifre çözme işleminin bir parçası olabilmeleridir. On milyon dolarlık bir yatırımla, saniyede 400 trilyon anahtarı deneyebilecek bir makine tasarlanabilir. Böyle bir makine 128 bitlik bir anahtar kullanarak oluşturulmuş bir şifreyi 5.000.000.000.000.000 yılda kırabilir.

Simetrik bir şifrenin çözülmesi için anahtar değerlerini teker teker deneme yöntemine, İngilizce'de 'Kaba Kuvvet Araması (Brute Force Search)', Fransızca'da 'Recherche Exhaustive' denir. Bu yöntem ilk zamanlarından günümüze değin, satranç programlarının algoritmalarında da, olası hamlelerin ağaç diyagramına uyarlanan alfa-beta taraması ile güçlendirilerek kullanılmaktadır. Türkçe'de Deneme-Yanılma denilen bu yöntem ile aranan n değerli bir anahtarın bulunması için ortalama n / 2 değer denemesi gerekir. Anahtar uzunluğu (n) bir bit arttıkça olası anahtar sayısı ikiye katlanır. 40 bitlik bir anahtar alanı için olası anahtar sayısı n = 240 = 1.099.511.627.776 olur. 1995 yılında yapılan bir denemede 40 bitle şifrelenmiş bir kredi kartı numarası basit bir bilgisayar sistemi ile 3,5 saatte bulunmuştur [6].

250 bitlik anahtarla şifreleme yapan bir algoritmanın kırılabilmesi için gerekli çaba termodinamik yasaları kullanılarak tahmin edilebilir. 250 bitlik bir anahtarı bulana dek sistemimizin yıldızı güneşin ömrü boyunca açığa çıkardığı kadar enerji gereklidir. Hala kullanılabilen 56 ve 80 bitlik eski anahtar boyutları ise böyle bir araçla sırasıyla 14 saniye ve yaklaşık 6 ayda kırabilir. Teknoloji geliştikçe bu süreler azalacağı gibi daha az maliyetle daha yüksek dereceden şifrelerin kırılabileceği açıktır. Teorik olarak kırılabilecek şifrelerin uygulamada kırılması anahtarın büyüklüğü arttıkça imkânsıza gider. Anahtar bulma süreleri tablo 10'da verilmiştir.

Tablo 10. Anahtar bulma süreleri

| ANAHTAR BULMA SÜRELERİ | | | | |
|---|---|---|---|---|
| Anahtar uzunluğu (n) | Olası anahtar sayısı ($2^n$) | O.Ç.S. 1 | O.Ç.S. 2 | O.Ç.S. 3 |
| 32 | 4294967296 | 11 sa 55 dk 12 sn | ~ 4.3 sn | ~ 1/250.000 sn |
| 40 | 1099511627776 | ~ 127 gün | ~ 18 dk 20 sn | ~ 1/1000 sn |
| 56 | 72057594037927936 | ~ 22849 yıl | ~ 834 gün | ~ 1 dk 12 sn |
| 64 | 18446744073709551616 | ~5.85 milyon yıl | ~ 213 bin 504 yıl | 5 sa 7 dk 27 sn |
| 128 | 3,4028236692093846346x1050 | 3.4x1032 yıl | 3.4x1028 yıl | 10.9x1015 yıl |

**O.Ç.S 1** (Ortalama Çözüm Süresi)**:** $10^5$ şifre/saniye deneme hızında,

**O.Ç.S 2:** $10^9$ şifre/saniye deneme hızında ve

**O.Ç.S 3:** $10^{15}$ şifre/saniye deneme hızında (Kişisel bilgisayarlar için yaklaşık değer, 2000 yılı standartları için)

Bir zincirin dayanabileceği en yüksek çekiş kuvvetinin en zayıf halkasına bağlı olması gibi bir kriptosistemin de gücü en zayıf noktasına eşittir. Kriptosistemi oluşturan halkalar ise; algoritması, anahtarlar ve kullanılan aygıtlardır.

Açık anahtar kriptografisi doğru anahtar tahmin edilerek değil ancak açık anahtardan buna uygun gizli anahtar bulunarak kırılabilir. Açık ve gizli anahtarlı şifreleme işlemlerinde bu düşünce ile açık-anahtarlı kriptografi çok ilginç hale gelmiştir.

### 1.12. Anahtar Dağıtma Problemi

Tek anahtarlı (simetrik anahtarlı) kriptografinin pratik kullanımındaki bir esas problem anahtar dağıtma problemidir. Bu problem temel olarak gönderici ve alıcının her ikisinin de anahtarın bir kopyasına sahip olmalarından kaynaklanır, ancak başkalarının anahtarın bir kopyasını elde etmelerini de önlemelidirler.

Varsayalım ki iki kişi O ve L, bilgiyi güvenlice değişmek istemekte ama gönderinin güvenliğini garanti edememektedirler. Mesajın içeriğine dair gizliliği sağlamak için büyük olasılıkla bir çeşit şifreleme kullanırlardı. Bu işlem için her ikisi de verinin şifrelenmesinde kullanılacak bir gizli anahtarı bilmelidir. Bununla birlikte, iletişim ortamı güvenilir

olmadığından anahtarın verileceği kişiyle görüşmelidirler. Bir kez bu yapılabilirse, bu gizli anahtarla şifrelenmiş anahtar olmadan başka birine sadece anlamsız gibi görünen bilgiyi mutlulukla değişebilirler. O ve L kendilerine ait olan anahtarın güvenliğini bir C kriptanalizcisinin ele geçirip O ve L'den gelebilecek mesajları okuyabilmesine karşı korumalıdır.

Bu, hemen ortaya çıkan bir problem dışında mükemmel bir iş olarak görünüyor. Varsayalım ki O ve L başka biriyle, T ile yazışmak istesin. T'ye anahtarı verirlerse onunla tam bir uzlaşma içinde olmalıdırlar çünkü C anahtarı ele geçirebileceği yeni bir kaynağa sahip olmuştur. Tarafların birbirlerine gönderdiği her bir mesajın çözümlenmediğinden emin olmak için O ve L, T ile iletişimde farklı anahtarlara sahip olmalıdırlar. Böylece her birinde iki anahtar bulunur. O, T'nin mesajını başka şekilde alır, L'ye başka türlü iletir ve böyle sürer.

Şimdi 1000 üyeli bir sistem düşünelim, bunların tümü bir diğeri ile gizli bir iletişim kurmak istesin. Bu halde her bireyin iletişim kurduğu herkes için bir anahtara ihtiyacı olacaktır. Diğer bir deyişle diğer herkes için 999 anahtar olacaktır. Her birey de bu 999 anahtarı korumak zorundadır.

Bu şartlarda sisteme üye olanlara göre verilecek anahtarlar sayısını hesaplamak mümkündür. Gerekli anahtar sayısı, n üye sayısı olmak üzere şöyle hesaplanır:

$$AnahtarSayısı = \left[n \times (n-1)\right]/2 \tag{5}$$

Saklanması gereken çok sayıda anahtar olacağından çoklu kullanıcılı ortamlarda açık-anahtarlı kripto sistemleri uygun çözümdür.

### 1.13. Bir Açık-Anahtarlı Kriptosistemin Özellikleri

Bir kriptosistemi için mümkün olan iki anahtarlı kriptografi aşağıdaki özelliklere sahip olmalıdır:

Özel ve açık anahtarlar hesaplanması, kriptograflar için kolay ama anahtarı ele geçirebilecek kriptanalistler için şifremetnin ne kadarı alınmış olursa olsun hemen hemen imkânsız olmalıdır.

Şifreleme ve deşifreleme işlemleri kullanıcı bilgisayarlarının yapabileceği kadar basit olmalıdır.

En az sayıda anahtar, kriptanaliz için birçok düzmetin ve şifremetin parçasının ele geçirilmesi durumunda bile çözümün neredeyse imkânsızlığını sağlamalıdır.

Bütün bu koşulları sağlayan bir kriptosistemi yoktur. Bununla beraber, kriptograflar bu şartları sağlayan kriptosistemleri kullanmaya güç bir matematik problemini çözerek başlamıştır. Bu denli güvenli bir sistem olabilmesinin altında yatan neden açık anahtarlı kriptosistemler için ortak olarak kullanılan temel bir sayı probleminin çözümünün oldukça güç olmasına dayanır. Bu Knapsack Problemi olarak bilinir.

### 1.14. Mevcut Uygulamalar

Yapılan araştırmalarda; VHF/UHF bandında çalışan analog telsizler için şifreleme yapan bazı ürünlere rastlanmıştır. Bu ürünlerden;

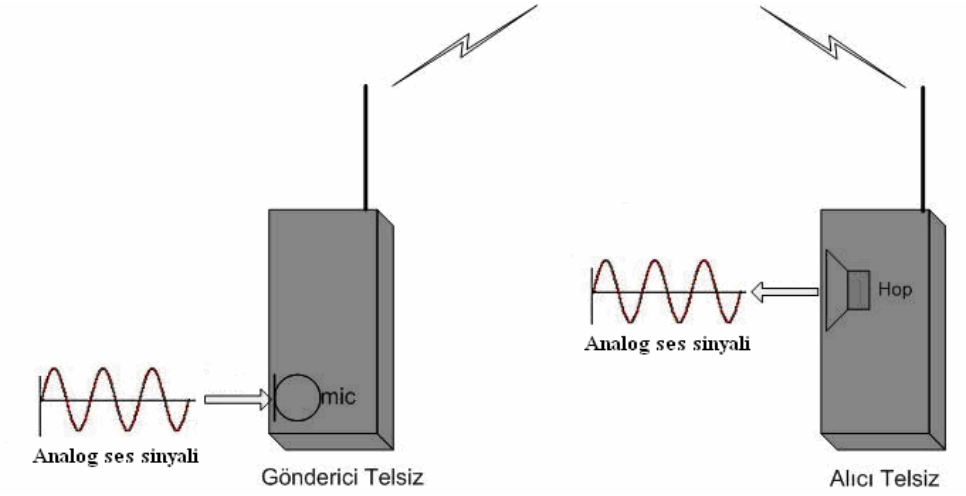
Hindistan firmasının ürününde, ara taşıyıcı frekansı 1800 Hz, kanaldaki veri hızı 4800 bps ve frekans bandı 200–3400 Hz olan bir QPSK modem kullanılmıştır. Şifreleme algoritması olarak Sovyetler Birliği ve Rusya'ya özgü simetrik kriptografi algoritmalarından blok şifreleme algoritması olan GOST kullanılmıştır [7].

Amerika Birleşik Devletleri'nde ise DES gibi algoritmalar kullanan karıştırıcılara (scrambler) ve tescilli 128-bit şifreleme yöntemi kullanan sayısal şifreleme birimlerine rastlanmıştır [8].

### 1.15. Tez Çalışmasının Amacı, Kapsamı ve Yöntemi

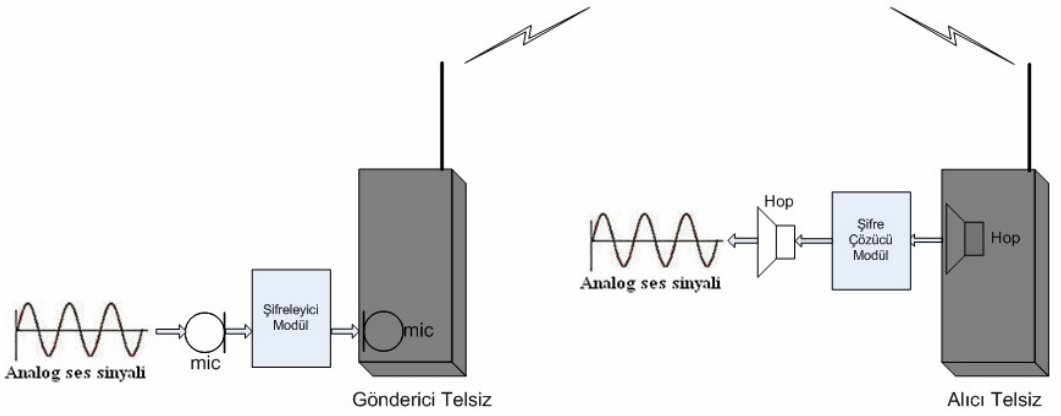
Burada amaç, sayısal şifrelemenin analog el telsizlerine uygulanabilirliğini araştırmak ve el telsizleri üzerinde bir uygulama yapmaktır.

Normal telsiz iletişimi şekil 16'da verilmiştir. Uygulama için tasarlanan şifreleme biriminin, VHF ya da UHF bandında kullanılmakta olan iki adet el telsizine dışarıdan monte edilebilecek bir arayüz ile test edilmesi planlanmıştır. Verici telsizde iletilecek olan ses (konuşma) sinyali mikrofon girişine uygulanarak şifreleme birimi ile şifrelenecek ve normal telsiz vericisi ile şifrelenmiş olarak gönderilecektir.




Şekil 16. Normal telsiz iletişimi

Alıcı telsizde ise alınan bu şifrelenmiş ses sinyali, alıcı telsiz hoparlör çıkışına bağlanan şifre çözücü birim ile orijinal ses sinyali elde edilecektir. Bu ses sinyali elde edildikten sonra hoparlöre verilecektir. Önerilen telsiz şifreleme sistemi şekil 17'de verilmiştir.




Şekil 17. Önerilen telsiz şifreleme sistemi

# 2. YAPILAN ÇALIŞMALAR, BULGULAR VE İRDELEME

## 2.1. Giriş

Bu çalışmada, analog el telsizleri ile yapılan görüşmelerin güvenli hale getirilmesi için sayısal bir şifreleme biriminin tasarlanması amaçlanmaktadır. Tasarlanacak birim analog el telsizinin mikrofon ve hoparlör girişlerine takılabilecek yapıda olacaktır. Verici konumundaki telsiz şifreleme biriminde, ses sinyali telsiz mikrofonuna verilmeden önce, sayısallaştırılıp şifrelendikten sonra tekrar analog işaret haline getirilecektir. Alıcı konumundaki telsiz şifreleme biriminde ise, alınan analog şifreli ses sinyali hoparlör çıkışına verilmeden önce denkleştirici devresi yardımı ile lojik–0 ve lojik–1 sinyallerine atanan taşıyıcı sinüsoidal işaretlerin genlik seviyeleri ayarlanıp sayısallaştırılacak ve şifre çözme işlemi gerçekleştirildikten sonra tekrar analog şifresiz ses sinyaline dönüştürülecektir.

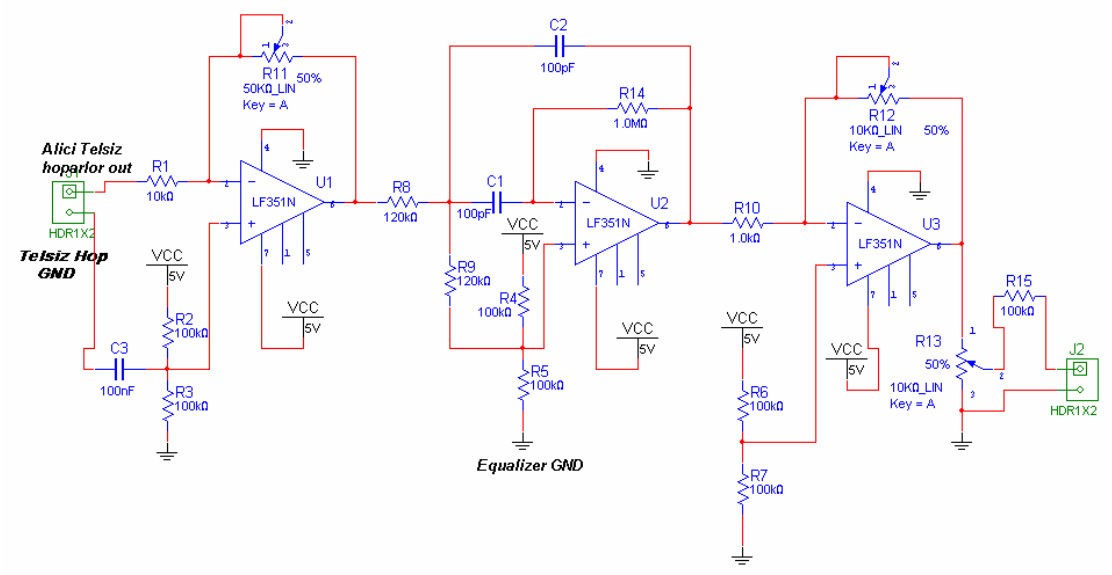
## 2.2. Sistemin Teknik Özellikleri

Sistem tasarım çalışmasının yapılacağı ses frekans bandının belirlenmesi amacıyla kullanılacak analog el telsizinin ses frekans karakteristiği elde edilmiştir.

Tasarımda kullanılacak modülasyon türünün belirlenebilmesi için sayısal modülasyon yöntemleri incelenmiştir.

İnsan kulağının algıladığı frekanslar 20Hz ile 20kHz arasındadır. Ancak burada belirtilen sınırlar kulakları olağanüstü duyarlı genç insanlarda ölçülmüş uç değerlerdir. İnsanların büyük bölümünün kulakları bu derece duyarlı değildir. Bu sebepten kaliteli müzik dinletisi için ses bandının üst sınırının 15kHz olması yeterlidir. Ses bandı FM radyo vericilerinde 15kHz, genlik modüleli (AM) radyo vericilerinde 5kHz ve telefonda da 3.4kHz'dir [9].

Sistemde, analog el telsizinin ses band genişliği (300-3000Hz) ve kullanılan modülasyon türü nedeniyle ses dönüştürme hızı (voice transformation rate) 4800bps (bit per second) olacaktır. Tasarlanan birimde 4800bps ses dönüştürme hızına ulaşabilmek için denkleştirici devresi kullanılmıştır (Şekil 18).




Şekil 18. Denkleştirici devresi

Tasarım için uygun olan ses kodlayıcı (vocoder) ve modem entegreleri mikroişlemci ile ayrı ayrı programlandıktan sonra testleri yapılmıştır. Yapılan testlerin ardından pcb tasarımına geçilmiştir. Vocoder ve modem entegrelerinin aynı anda programlanması amacı ile bu iki program düzenlenerek tek bir program haline getirilmiştir. Tasarlanan pcb üzerinde yer alan vocoder ve modem entegreleri programlanarak öncelikle ayrı ayrı daha sonra birlikte test edilmiştir. Ayrıca uygun ses seviyesinin sağlanabilmesi amacı ile denkleştirici devresi (lojik–1 ve lojik–0 sinyallerine atanan işaretlerin genlik değerlerinin ayarlanması için) tasarlanmıştır.

### 2.2.1. Analog El Telsizi Ses Frekans Karakteristiğinin Elde Edilmesi

Analog el telsizi ses frekans karakteristiğinin elde edilmesi için;

Sinyal üretecinden alınan 1Vpp genlikli sinüsoidal işaret, stereo kabloya bağlı jack yardımıyla verici olarak kullanılacak el telsizinin mikrofon girişine uygulanmıştır. Alıcı olarak kullanılacak el telsizinin hoparlör çıkışına stereo kabloya bağlı jack takılarak osiloskopa bağlanmıştır.

El telsizi Push-to-Talk (PTT) butonuna basılarak verici durumuna getirilmiştir. Verici telsizin anteninden gönderilen işaret, alıcı konumundaki el telsizinin hoparlör çıkışına bağlı osiloskop üzerinden gözlemlenmiş ve işaretin genlik değeri kaydedilmiştir.

Yukarıdaki işlemler gönderilen işaretin frekansı değiştirilerek (300-5100Hz bandı boyunca) tekrarlanarak osiloskop üzerinde görülen işaretin genlik değerleri kaydedilmiştir.

Ölçüm sonuçları tablo 11'de verilmiştir.

Tablo 11. Analog el telsizinin ses frekans karakteristiği

| **Analog El Telsizinin Ses Frekans Karakteristiği Ölçüm Sonuçları** | | | |
|---|---|---|---|
| **Frekans (Hz)** | **Ölçülen Çıkış Gerilimi ($mV_{p-p}$)** | **Ölçülen Çıkış Gerilimi (mV)** | **Ölçülen Çıkış Gerilmi (dBmV)** |
| 300 | 360 | 127.2792 | 42.0952 |
| 400 | 700 | 247.4874 | 47.8711 |
| 500 | 960 | 339.4113 | 50.6145 |
| 600 | 1120 | 395.9798 | 51.9535 |
| 700 | 1160 | 410.1219 | 52.2583 |
| 800 | 1160 | 410.1219 | 52.2583 |
| 900 | 1160 | 410.1219 | 52.2583 |
| 1000 | 1160 | 410.1219 | 52.2583 |
| 1100 | 1160 | 410.1219 | 52.2583 |
| 1200 | 1160 | 410.1219 | 52.2583 |
| 1500 | 1240 | 438.4062 | 52.8375 |
| 1700 | 1400 | 494.9747 | 53.8917 |
| 2000 | 1520 | 537.4012 | 54.6060 |
| 2200 | 1720 | 608.1118 | 55.6797 |
| 2500 | 1760 | 622.2540 | 55.8794 |
| 2800 | 1760 | 622.2540 | 55.8794 |
| 3000 | 1760 | 622.2540 | 55.8794 |
| 3200 | 1600 | 565.6854 | 55.0515 |
| 3500 | 1440 | 509.1169 | 54.1363 |
| 3600 | 1360 | 480.8326 | 53.6399 |
| 3700 | 1360 | 480.8326 | 53.6399 |
| 3800 | 1240 | 438.4062 | 52.8375 |
| 3900 | 1080 | 381.8377 | 51.6376 |
| 4000 | 1040 | 367.6955 | 51.3098 |
| 4100 | 1000 | 353.5534 | 50.9691 |
| 4200 | 1000 | 353.5534 | 50.9691 |
| 4300 | 800 | 282.8427 | 49.0309 |
| 4400 | 760 | 268.7006 | 48.5854 |
| 4500 | 720 | 254.5584 | 48.1158 |
| 4600 | 680 | 240.4163 | 47.6193 |
| 4700 | 680 | 240.4163 | 47.6193 |
| 4800 | 520 | 183.8478 | 45.2892 |
| 4900 | 480 | 169.7056 | 44.5939 |
| 5000 | 480 | 169.7056 | 44.5939 |
| 5100 | 320 | 113.1371 | 41.0721 |

### 2.2.2. Modülasyon

Modülasyon, veriyi iletime uygun hale getirmek için yapılan kodlama işlemidir.

Modülasyonun amaçları;

- Anten boyutlarını küçültmek,
- Tüm frekans bölgesinden yararlanmak,
- Aynı anda birden çok sinyalin iletilmesine olanak tanımak (çoğullama yapmak),
- İletim ortamına uymak,
- Bozucu etkileri azaltmak,
- Gönderilen sinyaller arasındaki etkileşimi (interference) azaltmak,
- Verici ve alıcı yapımını kolaylaştırmak olarak sıralanabilir.

Bir dalganın değişik parametrelerini (örneğin genlik, frekans, faz gibi) kontrollü olarak değiştirerek bilgi yükleme işlemi olan modülasyon eğer dalganın;

- Genliği değiştirilerek yapılıyor ise Genlik Modülasyonu (Amplitude Modulation-AM),
- Frekansı değiştirilerek yapılıyor ise Frekans Modülasyonu (Frequency Modulation-FM),
- Faz açısı değiştirilerek yapılıyor ise Faz Modülasyonu (Phase Modulation-PM) denir.

Bu modülasyon yöntemleri analog-analog çevirme yöntemleri olarak bilinir. Sayısal analog çevirme ise analog sinyalin karakteristik özelliklerden birisinin sayısal veriye göre değiştirilmesi işlemidir.

Sayısal analog çevirme yöntemleri; ASK (Amplitude Shift Keying), FSK (Frequency Shift Keying), PSK (Phase Shift Keying) ve QAM (Quadrature Amplitude Keying) modülasyon yöntemleridir.

Sayısal haberleşmenin avantajları;

- Sayısal iletimin en önemli avantajı, gürültüden fazla etkilenmemesidir. Analog sinyaller, sayısal darbelere oranla arzu edilmeyen genlik, frekans ve faz değişimlerine daha yatkındır.
- Sayısal sinyallere parazit ve karıştırıcı sinyal etkilerinden korunabilmek için güvenlik ve kriptolama gibi sinyal işleme teknikleri uygulanabilir.

- Sayısal darbeler, işleme ve çoğullama için analog sinyallerden daha uygundur. Sayısal darbeler kolayca saklanabilir, ancak analog sinyalleri saklamak kolay değildir.
- Sayısal bir sistemin iletim hızı, değişik ortamlara uyum gösterecek ya da değişik tür donanımlara, arabirim üzerinden bağlanacak şekilde kolayca değiştirilebilir.
- Hata sezme (error detection) ve düzeltme (correction) teknikleri sayesinde az hata oranlı sinyal iletimi yapılabilir.
- Sayısal devreler analog devrelere göre daha esnek, daha dayanıklı ve daha az maliyetli olarak tasarlanabilir.

Sayısal haberleşmenin dezavantajları;

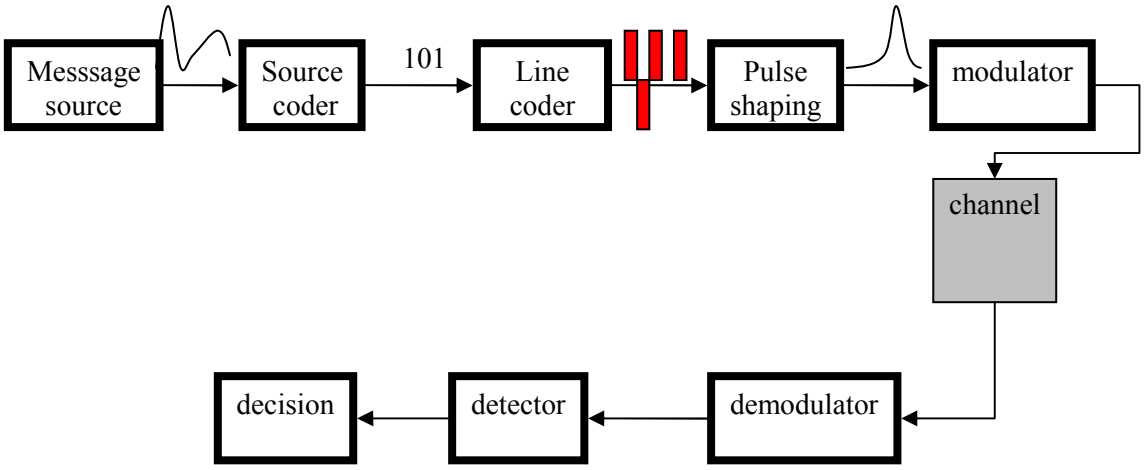
- Sayısal olarak kodlanmış analog sinyallerin iletimi, analog sinyalleri oldukları gibi iletmeye oranla daha fazla bant genişliği gerektirir.
- Analog sinyaller, iletimden önce sayısal kodlara, alıcıda ise tekrar analog biçime dönüştürülmelidir.
- Sayısal haberleşmede, verici ile alıcının saat darbeleri (cp) arasında duyarlıklı senkronizasyon gerektirir.
- Sayısal haberleşme sistemleri, günümüzde kullanılmakta olan analog sistem (TV ekranı gibi) donanımı ile uyumlu değildir.

Sayısal haberleşmenin yaygınlaşmasının nedenleri;

- Tümleşik devre teknolojisindeki son gelişmelerin, sayısal devre tasarımını kolaylaştırması.
- Sayısal işaret işleme (DSP) tekniklerindeki ilerlemelerin, sayısal işaretlerin daha verimli bir şekilde kullanımına neden olması.
- Sayısal bilgisayarların çok yaygın kullanımı.
- Gürültü ve girişim açısından sayısal haberleşme sistemlerinin, analog haberleşme sistemlerine göre daha güvenilir olması.
- Zaman çoklamalı sistemlere elverişli olması.

#### 2.2.2.1. Sayısal Modülasyonlar ve Demodülasyonlar

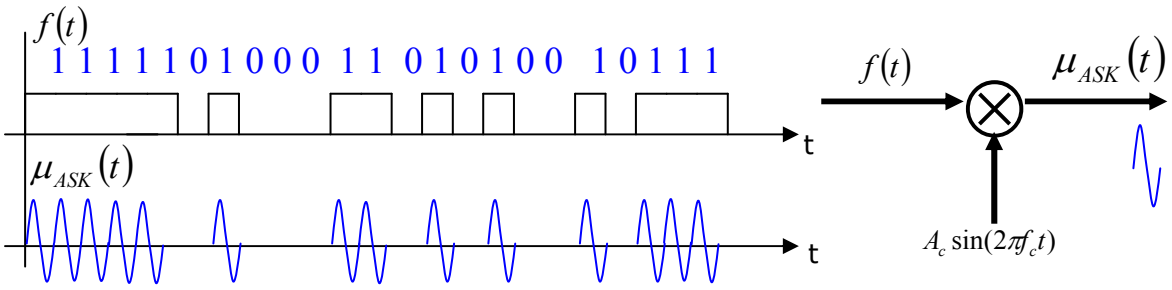
Tasarımda, yukarıda verilen avantajlarından dolayı sayısal modülasyon tercih edilmiştir. Sayısal modülasyon blok şeması şekil 19'da gösterilmiştir.




Şekil 19. Sayısal modülasyon blok şema

#### 2.2.2.1.1. Genlik Kaydırmalı Anahtarlama (ASK)

- Taşıyıcı sinyalin genliği değiştirilir. Birçok genlik seviyesi oluşturulabilir.
- İkili değerlerden (binary digit) birisi taşıyıcı sinyalin (carrier signal) varlığı ile ifade edilir.
- Diğer binary digit ise taşıyıcı sinyalin yokluğu ile ifade edilir.
- Genellikle birisi 0 olmak üzere iki seviyeli değişim yapılır (On-off keying).
- Genlik kaydırmalı anahtarlama şekil 20'de verilmiştir.




Şekil 20. Genlik kaydırmalı anahtarlama (ASK)

$A_c \sin \omega_c t$ : Taşıyıcı sinyal olmak üzere;

$$\omega_c = 2\pi f_c \tag{6}$$

$$f(t)=\sum_n a_n rect\left[\frac{t-nT}{T}\right] \qquad Burada \qquad a_n=\begin{cases}1\\0\end{cases} \tag{7}$$

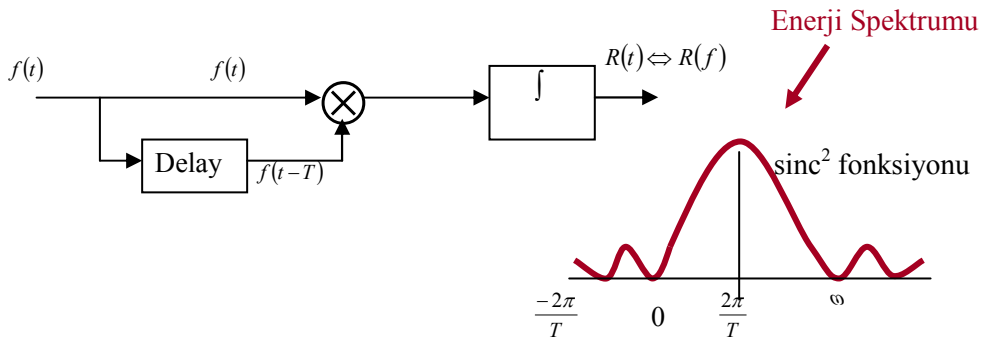
$$\mu_{ASK}(t)=f(t)\cdot A_c \sin \omega_c t \tag{8}$$

$$\mu_{ASK}(t)=\begin{cases}A_c \sin \omega_c t & \text{(lojik–1)}\\ 0 & \text{(lojik–0)}\end{cases} \tag{9}$$

Bir peryot için ASK modüleli sinyal;

$$\mu_{ASK}(t)=\begin{cases}A_C \sin \omega_C t & 0\le t\le T\\ 0 & digeryerlerde\end{cases} \tag{10}$$

ASK modüleli sinyalin enerji spektrumu şekil 21'de verilmiştir.

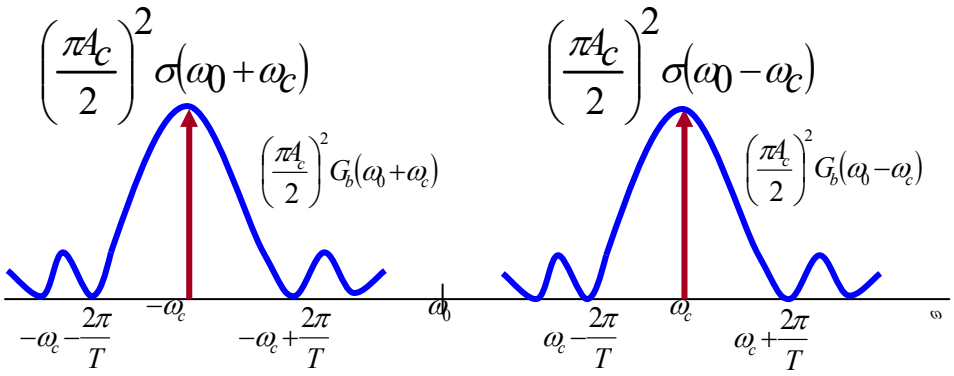



Şekil 21. ASK modüleli sinyalin enerji spektrumu

ASK modüleli işaretin spektral güç dağılımı;

$$G_{ASK}(\omega)=\left(\frac{\pi A_c}{2}\right)^2\left[\{G_b(\omega_0-\omega_c)+G_b(\omega_0+\omega_c)\}+\sigma(\omega_0-\omega_c)+\sigma(\omega_0+\omega_c)\right] \tag{11}$$

ile ifade edilir (Şekil 22).



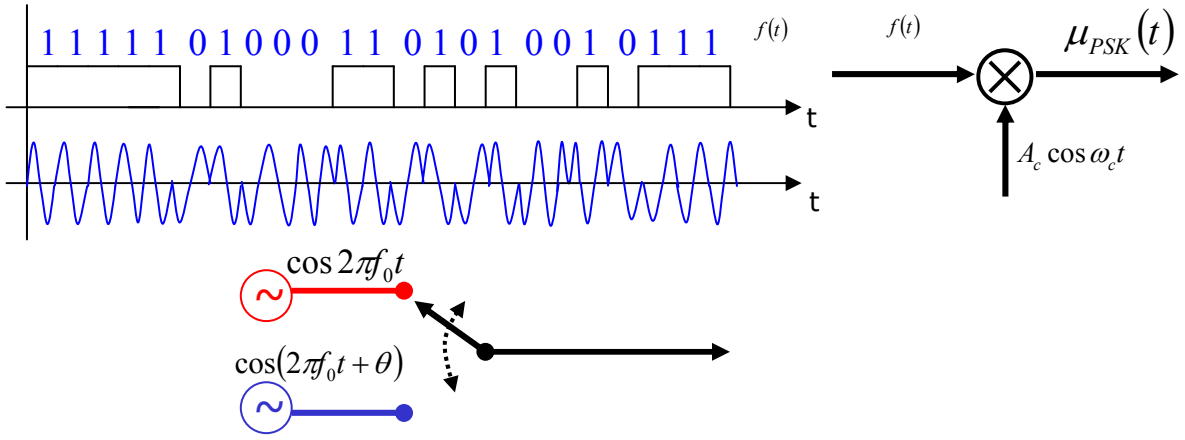

Şekil 22. ASK modüleli sinyalin spektral güç dağılımı

ASK modüleli sinyalde bildiri işaretinin tekrar elde edilmesi yani demodülasyonu, taşıyıcı sinyalin varlığı lojik–1 ve yokluğu lojik–0 ile ifade edilir.

#### 2.2.2.1.2. Faz Kaydırmalı Anahtarlama (PSK)

- Taşıyıcı sinyalin fazı değiştirilir.
- BPSK (Binary Phase Shift Keying)'da 0° ve 180° faz farklı iki sinyal kullanılır.
- PSK gürültüden ASK'ya göre daha az etkilenir.
- PSK sadece bir tane taşıyıcı frekans gerektirir, FSK seviye sayısı kadar gerektirir.

Faz kaydırmalı anahtarlama şekil 23'de verilmiştir.




Şekil 23. Faz kaydırmalı anahtarlama (PSK)

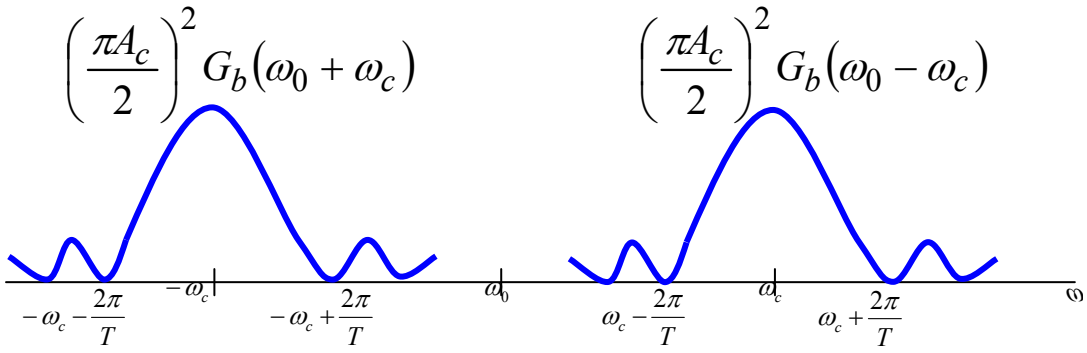
$$f(t)=\sum_n a_n rect\left[\frac{t-nT}{T}\right] \qquad Burada \qquad a_n=\begin{cases}1\\0\end{cases} \tag{12}$$

$$\mu_{PSK}(t)=f(t)\cdot A_c\cos\omega_c t \tag{13}$$

PSK modüleli işaretin spektral güç dağılımı;

$$G_{PSK}(\omega)=\left(\frac{\pi A_c}{2}\right)^2\left[G_b\left(\omega_0-\omega_c\right)+G_b\left(\omega_0+\omega_c\right)\right] \tag{14}$$

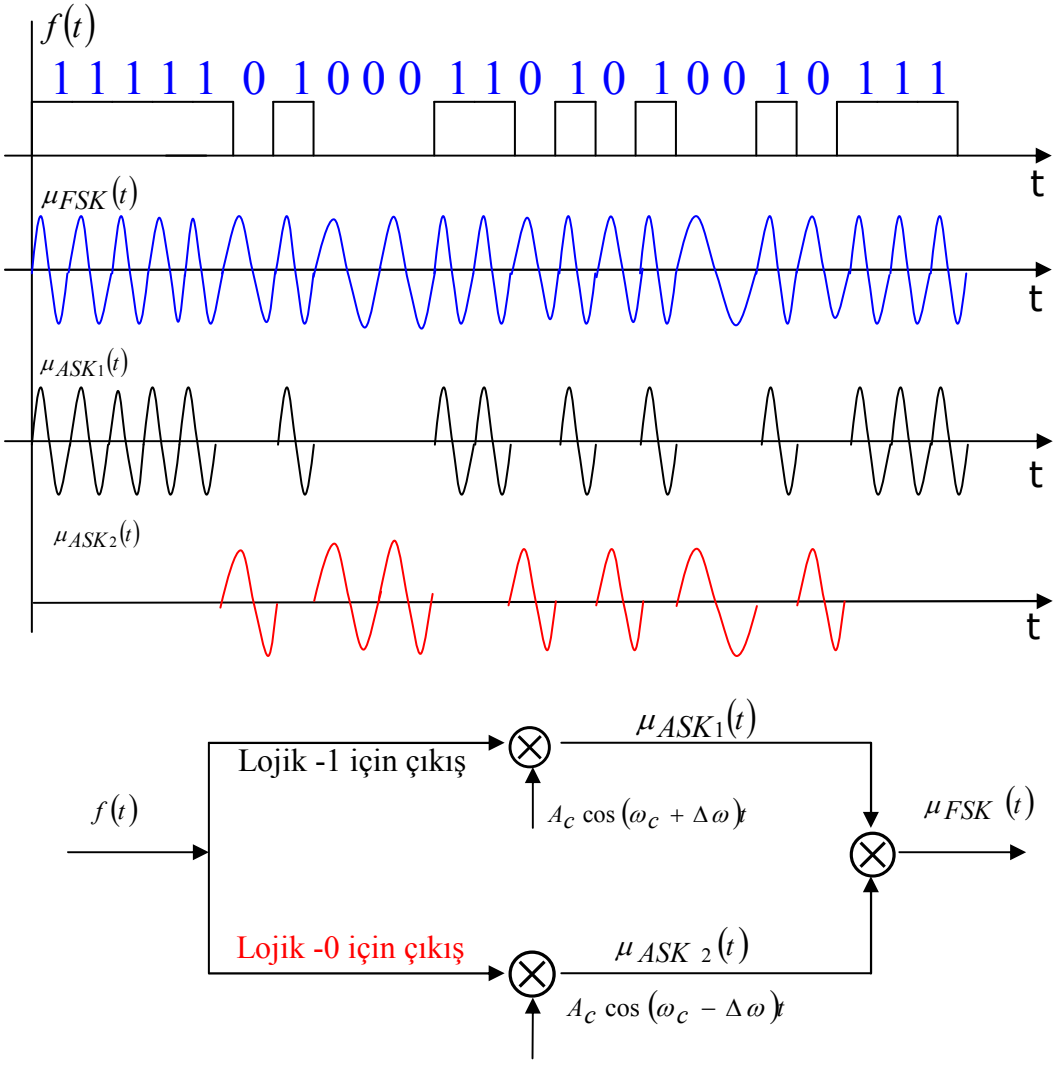
ile ifade edilir (Şekil 24).



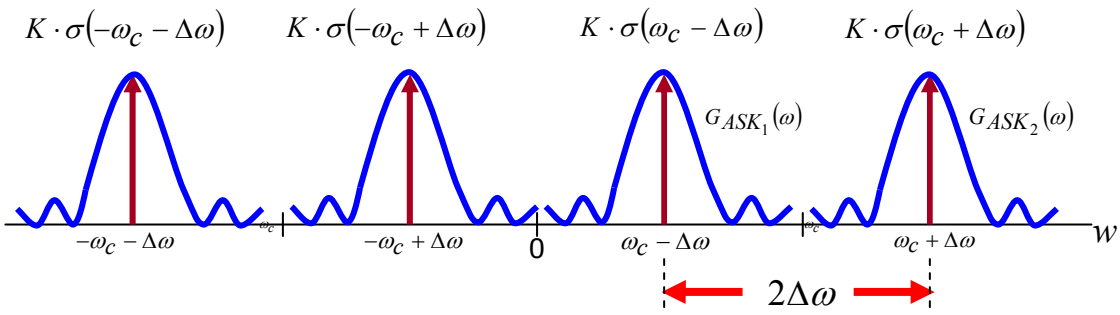

Şekil 24. PSK modüleli sinyalin spektral güç dağılımı

**2.2.2.1.3. Frekans Kaydırmalı Anahtarlama (FSK)**

- FSK'da genliği değişmeyen bir taşıyıcı frekansı ikili işaret düzeylerine (PCM) göre 2 frekans değerinden birisini alabilir. Sayısal ikili işaret modülasyonu iki farklı frekansa sahip osilatör arasında bir anahtarlama olarak düşünülebilir.
- FSK'da taşıyıcının frekansı değiştirilir.
- BFSK (Binary Frequency Shift Keying)'da iki farklı frekansta taşıyıcı sinyal (Lojik–1 ve lojik–0 için) kullanılır.
- Frekans kaydırmalı anahtarlamada seviye sayısı kadar farklı frekansta taşıyıcı sinyal gerektirir (Şekil 25).
- FSK modüleli sinyalin spektral güç dağılımı şekil 26'da verilmiştir.



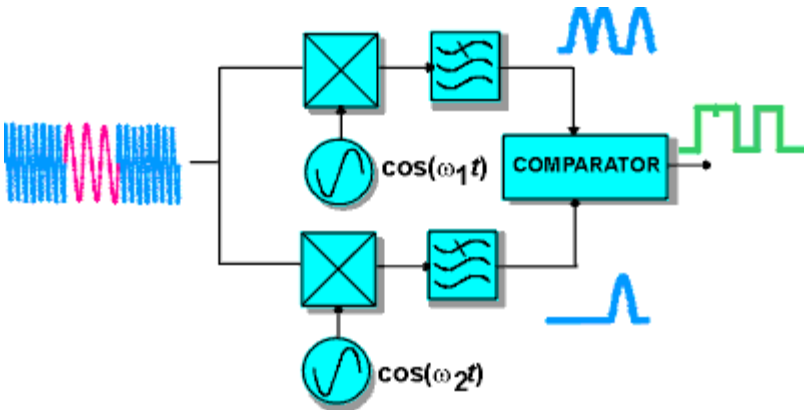

Şekil 25. Frekans kaydırmalı anahtarlama (FSK)



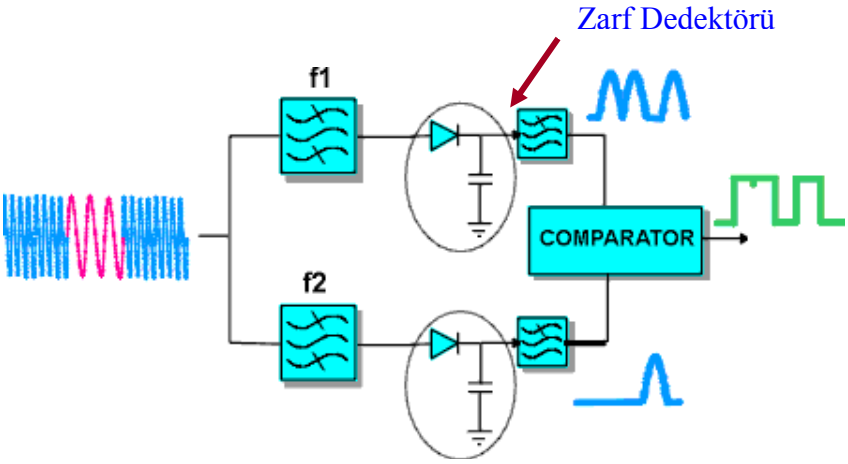

Şekil 26. FSK modüleli sinyalin spektral güç dağılımı

FSK modüleli işaretin demodüle edilmesi, alıcıda taşıyıcı işaretin bilindiği bağdaşık dedeksiyon (coherent detection) ya da taşıyıcı işaretin bilinmediği zarf dedektörünün

kullanıldığı bağdaşık olmayan dedeksiyon (non-coherent detection) yöntemi ile yapılabilir. Bağdaşık dedeksiyon şekil 27'de, bağdaşık olmayan dedeksiyon ise şekil 28'de verilmiştir.




Şekil 27. Bağdaşık dedeksiyon




Şekil 28. Bağdaşık olmayan dedeksiyon

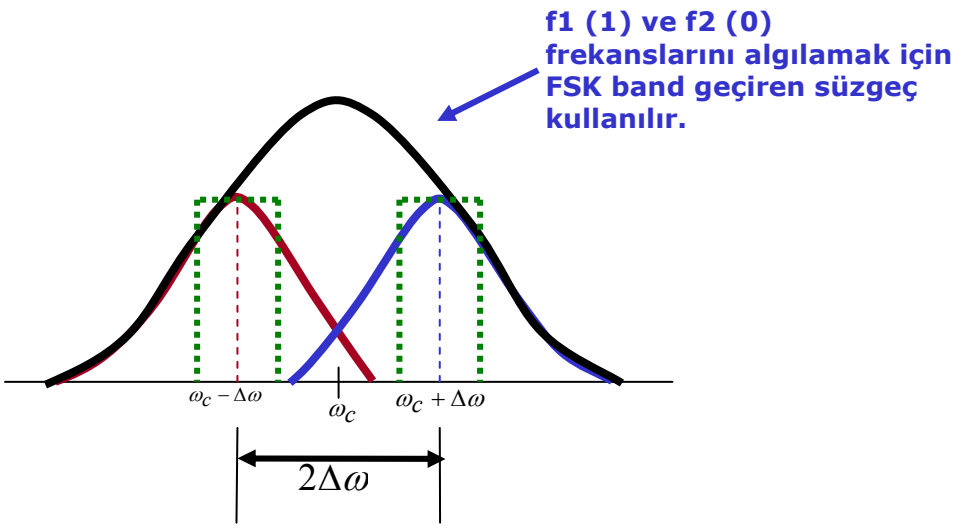
Genel olarak frekans dağılımı;

$$2\Delta\omega \geq DataRate \tag{15}$$

$$2\Delta f = \frac{1}{T} \qquad 2\Delta\omega = \frac{2\pi}{T} \tag{16}$$

$$\omega = 2\pi f \quad \text{veya} \quad \frac{m}{T} \tag{17}$$

Frekans kaydırmalı anahtarlamada frekans dağılımı şekil 29'da verilmiştir.




Şekil 29. Frekans kaydırmalı anahtarlamada frekans dağılımı

#### 2.2.2.1.4. Hızlı Frekans Kaydırmalı Anahtarlama (MSK)

Hızlı frekans kaydırmalı anahtarlama (Minimum Shift Keying, MSK) modülasyonu, sürekli faz modülasyonunun özel bir biçimi olarak sabit zarf, band verimliliği gibi özellikleri nedeniyle band ve/veya güç sınırlı iletişim ortamları için oldukça uygun bir modülasyon tekniğidir. Yapısında barındırdığı doğal kodlamaya [10] ek olarak band verimliliğinden bir miktar özveride bulunularak güç verimliliğinin kodlama işlemi yardımıyla daha da artırılabiliyor olması, bu modülasyon tekniğini söz konusu iletişim ortamları için daha da çekici duruma getirmektedir. Son yıllarda yaygın olarak incelenen ve sistemin kodlama kazancını artıran bu tür yöntemler genellikle kafes kodlamalı modülasyon (trellis coded modulation, TCM) tekniğine dayanır. MSK modülasyonu, toplamsal beyaz Gauss gürültülü kanalların yanısıra özellikle gezgin iletişim sistemlerinde karşılaşılan sönümlemeli (fading) kanallar için de çok uygun bir modülasyon tekniğidir [11].

## 2.3. Sistemin Özellikleri

Analog telsiz sistemleri ile yapılan görüşmeleri güvenli hale getirmek için yapılan bu çalışmada dört temel bloktan oluşan bir devre tasarlanmış ve programlanmıştır. Bu temel bloklar;

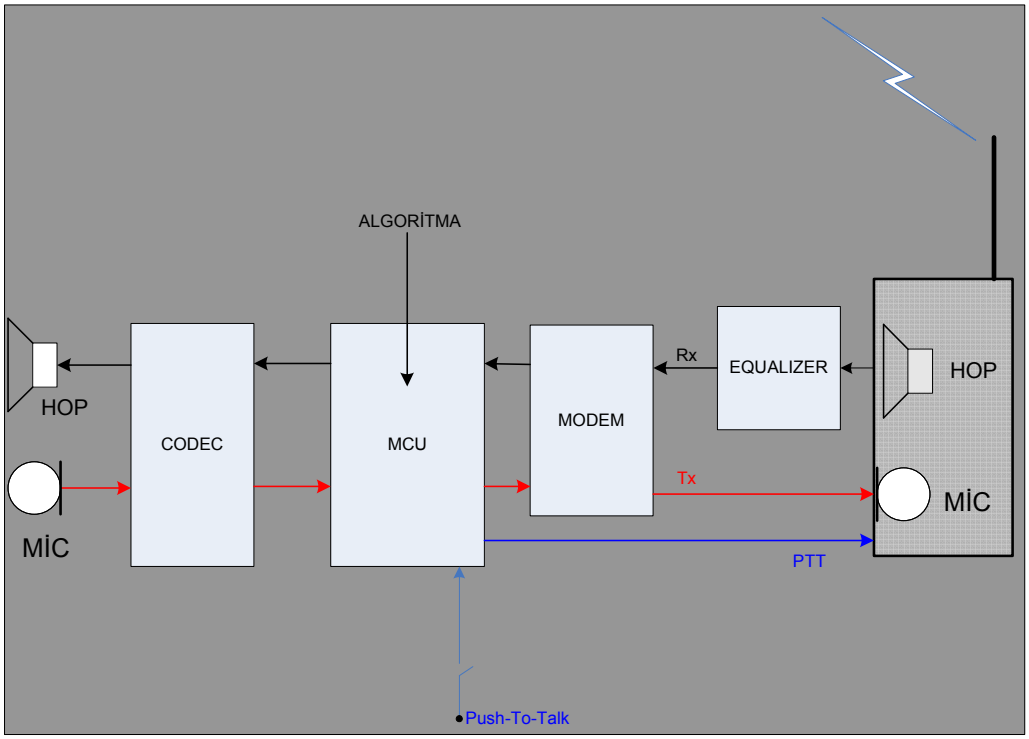
- Vocoder
- Modem
- Mikroişlemci
- Denkleştirici devresidir.

Analog ses sinyali verici konumundaki analog telsiz (Tx) mikrofon girişine uygulanmadan önce ses kodlayıcı (vocoder) ile kodlanıp MSK (Minimum Shift Keying) modem ile modüle edilir**.**

Verici konumundaki (Tx) analog telsiz mikrofon girişine verilen analog ses sinyali, alıcı konumundaki analog telsiz (Rx) ile alındıktan sonra denkleştirici devresi yardımı ile lojik–0 sinyaline atanan taşıyıcı sinüsoidal işaretin seviyesi artırılıp MSK modem ile demodüle edilip vocoder entegresi ile kodu çözüldükten sonra hoparlör çıkışından tekrar elde edilir.

Tasarlanan birimde modem ve vocoder entegreleri mikroişlemci ile kontrol edilmiştir. Programlama dili olarak ise C programlama tercih edilmiştir. Önerilen sistemin blok şeması şekil 30‘da verilmiştir.

Sistemde, MSK modem kullanılmıştır. Bu çalışmada kullanılan telsiz, lojik–0 sinyaline atanan taşıyıcı sinüsoidal işareti, lojik–1 sinyaline atanan taşıyıcı sinüsoidal işarete göre daha düşük genlikte geçirdiği için alıcı konumundaki telsiz hoparlör çıkışındaki sinyal, denkleştirici devresinin girişine uygulanmış ve denkleştirici devresi ile lojik–0 sinyaline atanan taşıyıcı sinüsoidal işaretin genliği arttırılarak lojik–1 sinyaline atanan taşıyıcı sinüsoidal işaretin genliği ile eşitlenmiştir. Böylece bit hatası minimuma indirilmiş ve 3kHz’lik band genişliğinde 4800bps veri hızına ulaşılmıştır.




Şekil 30. Önerilen sistemin blok şeması

a. Ses Kodlayıcının Programlanması:

Vocoder, ses dönüştürme hızı 2400bps+1200bps FEC olacak şekilde programlanmıştır. Öncelikle kaydediciler (register), kullanılacak pinler, değişkenler, bayraklar (flag) fonksiyonlar, kesme fonksiyonları tanımlanır. Temel (main) fonksiyonda; ilk olarak mikroişlemci ve vocoder initialize (başlangıç durumuna getirmek) edildikten sonra ses şifreleyici kod ve şifre çözücü kod yazılarak program tamamlanır.

b. MSK (Minimum Shift Keying) Modemin Programlanması:

Modem, gönderme ve alma fonksiyonu olmak üzere iki alt fonksiyon kullanılarak programlanmıştır. Vocoder ile kodlanan sayısal veri mikroişlemci yardımıyla modem girişine uygulanır. Modemde gönderme alt fonksiyonu ile modüle edildikten sonra telsiz mikrofon girişine verilir. Alıcı telsiz ile alınan şifreli ses sinyali modeme uygulandıktan sonra alma alt fonksiyonu ile demodüle edilip mikroişlemciye verilir.

## 2.4. Sistem Donanımının Tasarlanması

Bu çalışmada yapılan tasarım; vocoder, modem, mikroişlemci ve denkleştirici donanımlarından oluşan ve gömülü yazılım içeren bir donanım tasarımıdır.

Sistemin ilk parçası olan vocoder entegresi, ön yükselteç ve yükselteç içerdiği için sistemin girişinde ve çıkışında başka bir yükselteç devresi tasarlanmasına gerek duyulmamıştır. Vocoder entegresinin yapısında, analog ses sinyalinin sayısallaştırılması için gereken analog-sayısal dönüştürücü (ADC) ve sayısal ses sinyalinin analog ses sinyaline dönüştürülmesi için gereken sayısal-analog dönüştürücü (DAC)'de yer almaktadır.

Analog ses sinyali ilk olarak vocoder entegresinin girişine uygulanır ve vocoder entegresinde bulunan ön yükselteç ile yükseltilir. Daha sonra yükselteç ile tekrar yükseltildikten sonra ADC ile sayısal ses sinyaline dönüştürülüp filtrelenir. Filtrelenmiş sayısal ses sinyali mikroişlemci yardımıyla şifrelenir.

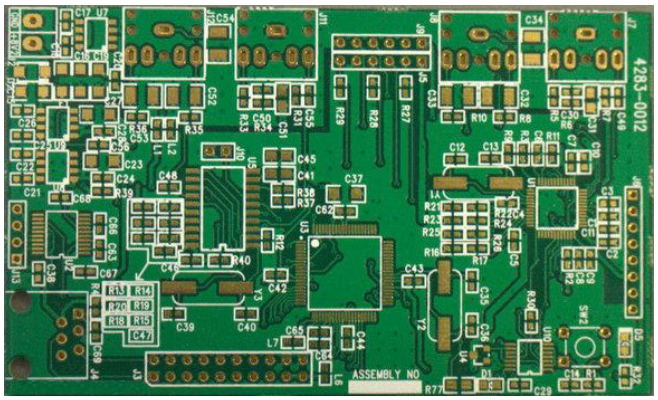
Vocoder çıkışından elde edilen şifreli sayısal ses sinyali analog telsiz ile gönderebilmek için MSK modem entegresinin girişine uygulanır. MSK modem ile sayısal ses sinyali modüle edildikten sonra telsiz mikrofon girişine uygulanır.

Alıcı konumundaki telsiz anteninden gelen analog ses sinyali hoparlöre verilmeden önce denkleştirici devresi ile lojik–0 sinyaline atanan taşıyıcı sinüsoidal işaretin seviyesi artırılıp MSK modem ile demodüle edilip vocoder entegresine uygulanır. Sayısal hale dönüştürülmüş olan ses sinyali vocoder entegresinde decode edilip filtrelendikten sonra sayısal-analog dönüştürücü ile analog ses sinyaline dönüştürülür ve hoparlör çıkışından elde edilir.

Tasarlanan birimde mikroişlemci olarak dspic kullanılmıştır.

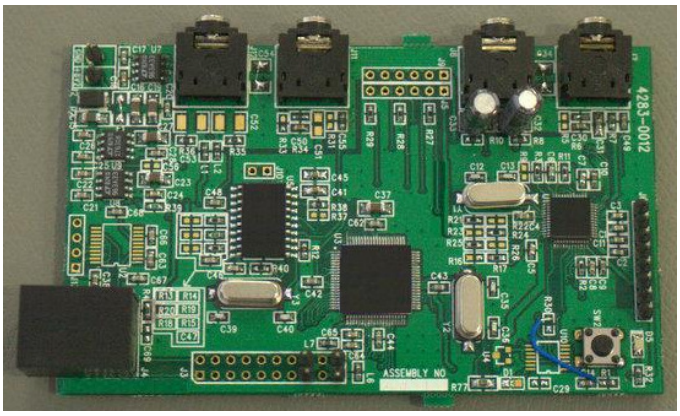
## 2.5. Sistemin Gerçeklenmesi ve Test Edilmesi

PCB kart tasarımı için Mentor Graphics şema ve pcb tasarım programı kullanılmıştır. Tasarlanan birimde yüzey montajlı (SMD) malzemeler tercih edilmiştir. Kartın PCB görünümü şekil 31'de gösterilmiştir.



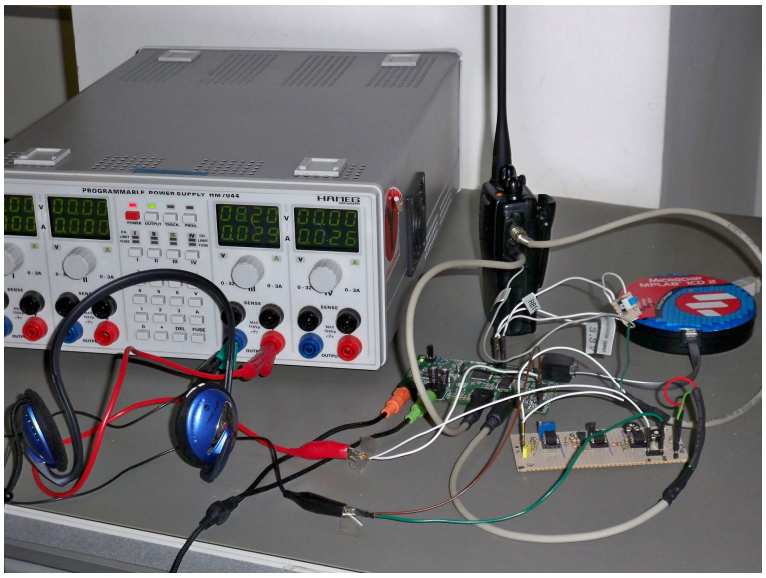

Şekil 31. Kartın PCB görünümü

Tasarlanan birimin küçük boyutlu olması amacıyla SMD malzeme kullanılmasından kaynaklanan malzeme dizilimi ve lehimlenmesi konusunda zorluklar yaşanmıştır. Soğuk lehim (cold soldering) olmasından dolayı iletim sorunu olan yollar oluşmuş ve hangi sinyal yolunda sorun olduğunun tespit edilmesi için sinyal takibi yapılması gerekmiştir. Kartın montajlı hali şekil 32'de verilmiştir.



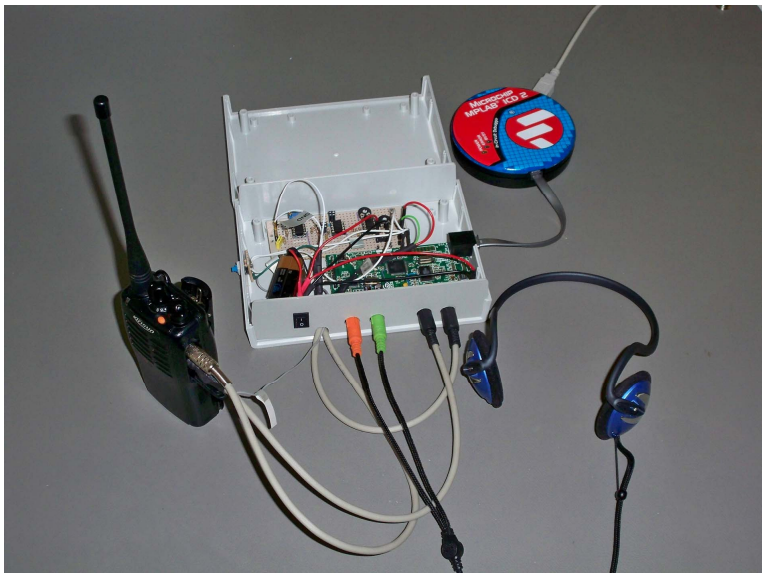

Şekil 32. Kartın montajlı hali

Şifreleme birimi, öncelikle güç kaynağı ile birlikte test edilmiştir. Şifreleme birimi ve güç kaynağı ile yapılan test ortamının görünümü şekil 33'de verilmiştir.



Şekil 33. Şifreleme birimi ve güç kaynağı ile yapılan test ortamı

Şifreleme birimi kutulandıktan sonra batarya ile birlikte tekrar test edilmiştir. Şifreleme birimi ve batarya ile yapılan test ortamının görünümü şekil 34'de verilmiştir.



Şekil 34. Şifreleme birimi ve batarya ile yapılan test ortamı

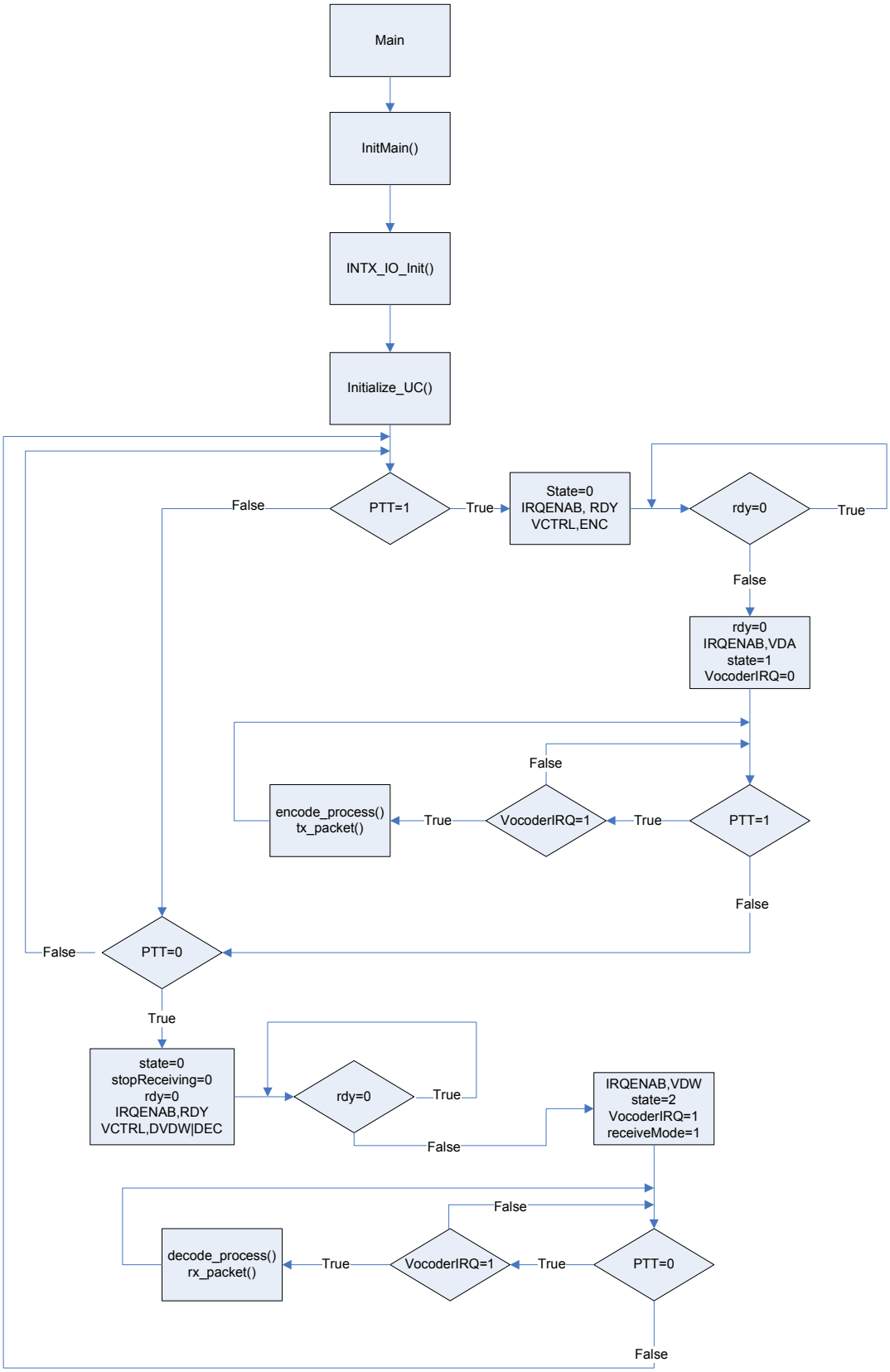
Tasarlanan şifreleme birimi gömülü yazılım içermektedir. Sistemin program akış şeması şekil 35'de gösterilmiştir. Şifreleme birimi için yazılan programın akış şeması kısaca aşağıda ifade edilmiştir:

Temel (main) fonksiyonda; öncelikle mikroişlemci ve vocoder initialize (başlangıç durumuna getirmek) edildikten sonra PTT değişkeninin durumuna göre, tasarlanan birimin alıcı ya da verici kısımlarından hangisinin çalışacağı belirlenir. PTT değişkeni bir ise verici kısmı, sıfır ise alıcı kısmı çalışacaktır.

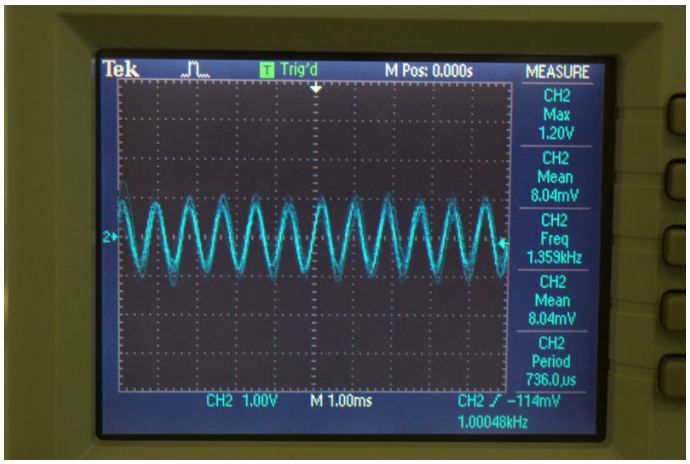
PTT değişkeni bir ise; şifreleme için vocoder ayarları yapılır ve telsiz ptt (push-to-talk) butonuna basılana kadar beklenir. Butona basıldığında şifreleme ve modem gönderme alt fonksiyonları çağrılır. Vocoder ile kodlanan sayısal ses verisi mikroişlemci yardımıyla modem girişine uygulanır. Modem gönderme alt fonksiyonu ile modüle edildikten sonra telsiz mikrofon girişine verilir.

PTT değişkeni sıfır ise; şifre çözme işlemi için vocoder ayarları yapılır ve telsiz ptt butonuna basılı olmadığı bilgisi mikroişlemciye iletilene kadar beklenir. Telsiz ptt butonuna basılı değil ise ve PTT değişkeni sıfır ise; modem alma ve şifre çözme alt fonksiyonları çağrılır. Alıcı telsiz ile alınan şifreli ses sinyali modeme uygulanarak alma alt fonksiyonu ile demodüle edilip mikroişlemciye verilir. Mikroişlemci yardımıyla vocoder girişine verilerek ses şifre çözücü kodu yardımıyla şifresi çözülür.

Verici konumundaki analog el telsizi ile gönderilen bir ses sinyalinin, alıcı konumundaki analog el telsiz hoparlör çıkışındaki osiloskop görüntüsü şekil 36'da verilmiştir.



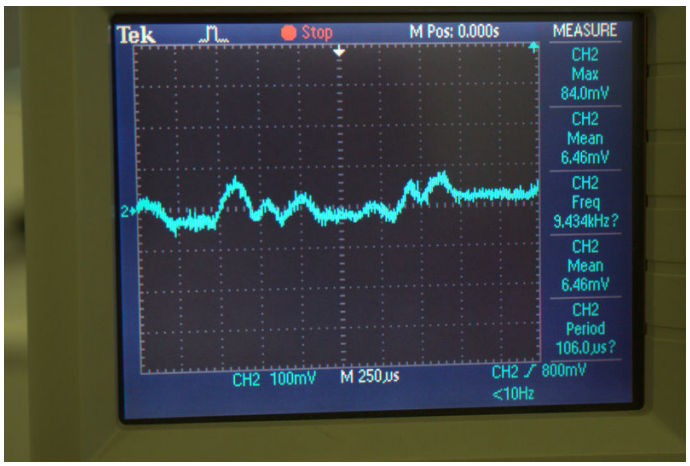

Şekil 35. Program akış şeması



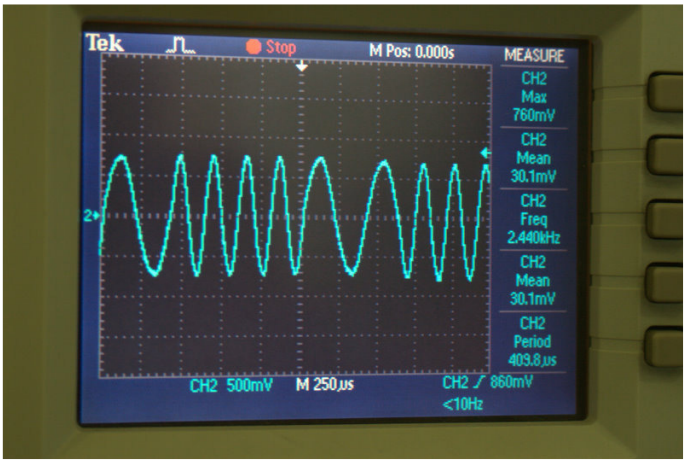

Şekil 36. Alıcı telsiz hoparlör çıkışındaki ses sinyali

Verici konumundaki (Tx) telsize takılan birimin girişine uygulanan ses sinyalinin osiloskop görüntüsü şekil 37'de verilmiştir. Ayrıca bu birimde, modem çıkışındaki modüleli sinyal şekil 38'de gösterilmiştir.

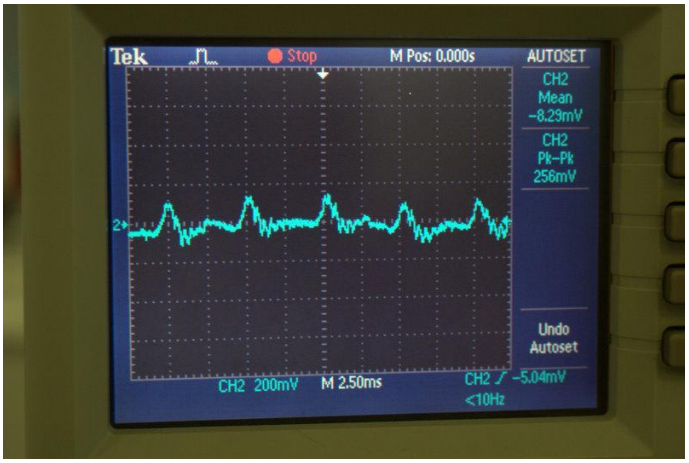
Bir verici ve bir alıcı birimin birbirine kablo ile bağlanması durumunda, alıcı konumundaki (Rx) birimin çıkışındaki ses sinyalinin osiloskop görüntüsü şekil 39'da verilmiştir.




Şekil 37. Verici konumundaki birimin mikrofon girişine uygulanan ses sinyali

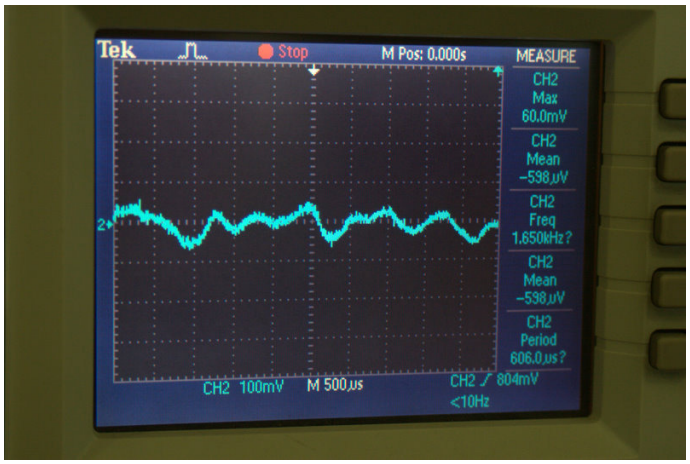



Şekil 38. Verici konumundaki birim çıkışındaki modüleli sinyal



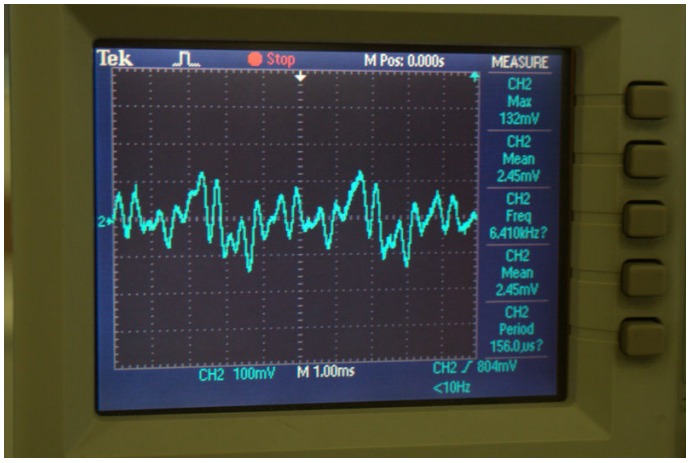

Şekil 39. Alıcı birim hoparlör çıkışındaki ses sinyali (kablolu iletişim durumunda)

Verici konumundaki (Tx) telsize takılan birimin mikrofon girişine uygulanan ses sinyalinin osiloskop görüntüsü şekil 40'da verilmiştir.



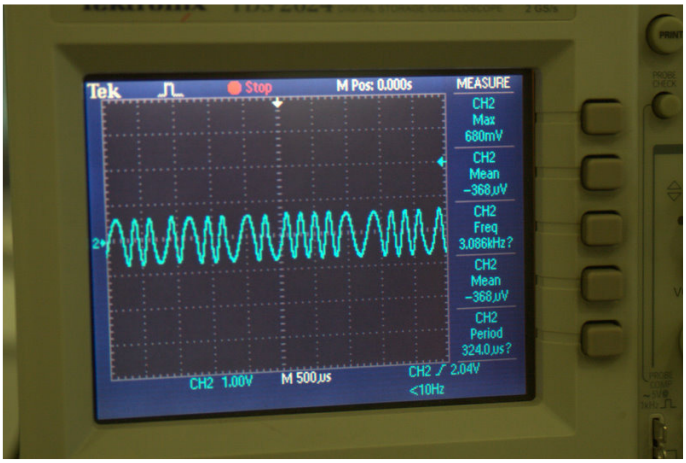

Şekil 40. Verici birim mikrofon girişine uygulanan ses sinyali

Alıcı konumundaki (Rx) telsize takılan birimin hoparlör çıkışındaki ses sinyalinin osiloskop görüntüsü şekil 41'de verilmiştir.



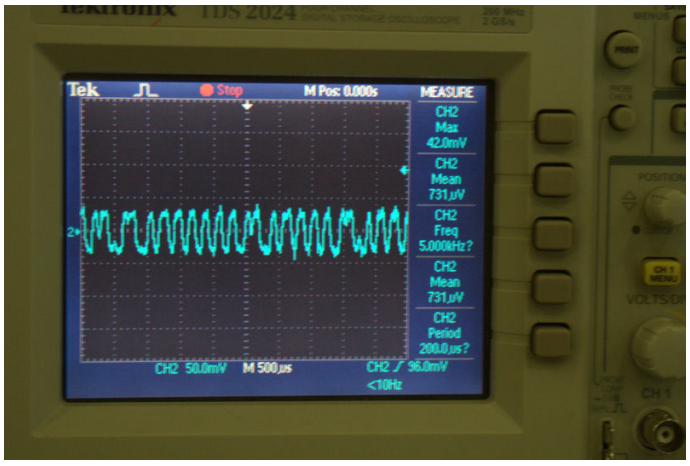

Şekil 41. Alıcı birim hoparlör çıkışındaki ses sinyali (Telsiz iletişim durumunda)

PTT butonuna basılarak telsiz ve birim verici (Tx) konumuna getirilmiştir. Verici konumundaki (Tx) telsize takılan birimin modem çıkışındaki MSK modüleli sinyal telsiz mikrofon girişine uygulanmıştır (Şekil 42).

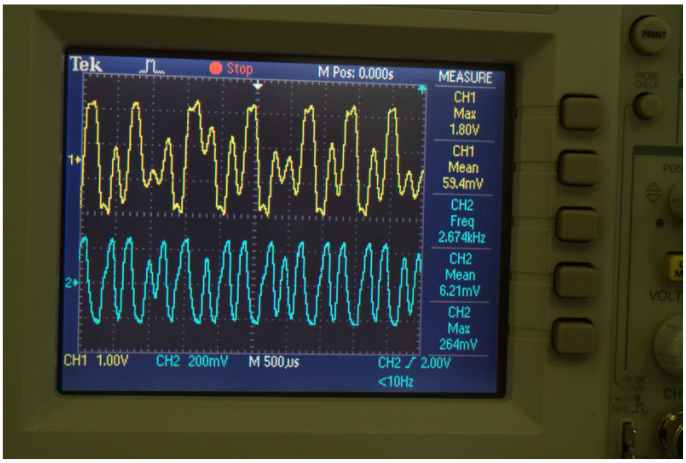



Şekil 42. Verici konumundaki telsizin mikrofon girişine uygulanan sinyal

Alıcı konumundaki telsiz hoparlör çıkışında gözlenen şifreli ve modüleli sinyal şekil 43'de verilmiştir. Alıcı telsiz ile alınan şifreli sinyal denkleştirici devresinin girişine uygulanır. Denkleştirici devresinde lojik–1 ve lojik–0 için atanan sinüsoidal işaretlerin genlikleri ayarlanarak alıcı birime verilir. Denkleştirici girişine verilen sinyal ile denkleştirici çıkışında elde edilen sinyal şekil 44'de gösterilmiştir.




Şekil 43. Alıcı konumundaki telsiz hoparlör çıkışında gözlenen modüleli sinyal




Şekil 44. Denkleştirici girişine verilen (sarı) ve çıkışında gözlenen sinyal (mavi)

Bu çalışmada, analog ses sinyalinin sayısallaştırılıp sıkıştırma algoritması ile şifrelenerek istenmeyen kişiler tarafından dinlenilmesinin engellenebildiği gözlenmiştir.

Tasarlanan birimin telsiz ile birlikte test edilmesi sırasında gürültü oluştuğu görülmüştür. Gürültünün, PTT butonuna basıldığında telsiz toprağı (ground) ile denkleştirici devresinin toprağı arasındaki gerilim seviye farkından kaynaklandığı tespit edilmiştir. Gürültü oluşmasının önlenmesi için denkleştirici devresinin toprağının devredeki diğer topraklardan yalıtılması gerektiği anlaşılmıştır.

İstenilen veri hıza ulaşabilmek için gerekli band genişliğine sahip olunmadığı durumda, denkleştirici devresi tasarlanarak o frekanstaki işaretin genliğinin artırılabildiği ve böylece istenilen hıza ulaşılabildiği tespit edilmiştir.

Tasarlanan birimlerin test edilmesi kapsamında son olarak bir makale okunarak alıcı birim hoparlör çıkışındaki ses kaydedilmiştir. Bu testte; tasarlanan şifreleme birimi ile şifrelenen ses verici konumundaki telsiz ile gönderilmiş ve alıcı konumundaki telsiz ile alınan şifreli ses, tasarlanan denkleştirici devresi ile lojik–1 ve lojik–0 için atanan sinüsoidal işaretlerin genlik değerleri eşitlenerek tasarlanan birim ile şifresi çözülüp hoparlör çıkışından tekrar elde edilmiştir.

## 3. SONUÇLAR

Bu çalışmada, analog el telsizleri ile yapılan görüşmelerin istenmeyen unsurlar tarafından dinlenilmesinin engellenmesi amaçlanmıştır. Analog el telsizinin mikrofon ve hoparlör girişlerine takılabilecek yapıda, küçük boyutlu ve düşük maliyetli bir şifreleme birimi tasarlanmıştır.

Bu çalışmada elde edilen bazı önemli sonuçlar aşağıdaki gibi özetlenebilir:

1. İstenilen veri hızına ulaşabilmek için gerekli band genişliğine sahip olunmadığı durumda, denkleştirici devresi tasarlayarak band genişliğinin dışında kalan frekanstaki işaretin genliğinin ayarlanabildiği ve böylece o frekanstaki işarete yüklenmiş sayısal verinin taşınabildiği tespit edilmiştir.
2. Analog ses sinyalinin sayısal biçime donüştürülerek sayısal teknikler yardımıyla şifrelenebileceği ve güvenli iletişim sağlanabileceği görülmüştür.
3. Analog sistemlerde düşük maliyetli ve hacimli ek bir birim geliştirilerek şifreleme özelliğinin sisteme dahil edilebileceği sonucuna varılmıştır.
4. Buna benzer çözümler, analog telsiz dışındaki diğer ses iletimi yapılan analog sistemlere de uyarlanabilir.
5. Şifreleme yapılırken telsizin yapısına herhangi bir şekilde müdahale edilmediği için telsizin iletişim mesafesi ve diğer özelliklerinde herhangi bir değişiklik olmadığı gözlenmiştir.
6. Biri verici diğeri alıcı olarak kullanılarak yapılan testlerde; doğrudan kablo ile birbirine bağlandığında herhangi bir sorun olmadığı görülmüştür. Ancak birimler telsizlere takılarak test edildiğinde yani iletim ortamı hava olduğu durumda gürültü sorunu olduğu tespit edilmiştir. Tasarlanan denkleştirici devresi alıcı telsiz hoparlör çıkışına takılarak bu sorun çözülmüştür.
7. Bu tez çalışmasında ADC, DAC, sıkıştırma, gömülü donanım tasarımı ve yazılıma dayalı teorik ve pratik bir yöntem denenmiştir. Hedeflenen başarı düzeyine ulaşılmıştır.

# 4. ÖNERİLER

Günümüzde sayısal telsizlerin kullanımı gittikçe yaygınlaşmaktadır. Sayısal telsizlerde güvenlik amaçlı kriptolama veya şifreleme özellikleri ya mevcuttur ya da rahatlıkla tasarıma eklenebilmektedir. Ancak analog telsizlerde kriptolama veya şifreleme özelliğinin eklenmesi daha zordur. Bu çalışmada esasında dar bandlı bir analog iletişim kanalında ses sinyalinin güvenlik amaçlı şifrelenmesi birimi donanım ve yazılım olarak gerçeklenmiştir. İletişim kanalı olarak analog el telsizi seçilmiştir. Çalışmadan elde edilen sonuçlar bu tür uygulamaların ses iletimi yapılan diğer haberleşme sistemlerine de (örneğin sabit telefon) uyarlanabileceğini göstermektedir. Literatürde çok fazla çalışmaya rastlanmamıştır. Bunun nedenlerinden biri, bu konunun ticari bir boyutunun olabileceğidir. Nitekim bu tezde verilen [7] ve [8] nolu kaynaklar bunu doğrulamaktadır.

Ses iletişimi insanlığın varlığından beri önemini hep korumuştur. Günümüz teknolojisinin geldiği nokta dikkate alındığında şifreli ses iletişimi için farklı yöntemler geliştirilebilme olanağı mevcuttur. Teorik ve uygulama açısından araştırma yapılmaya uygun ve kapsamlı bir konudur.

Bu konuda çalışma yapmayı hedefleyen araştırmacıların, daha yüksek hıza sahip mikroişlemciler kullanarak DES, AES gibi kripto algoritmaları denemeleri önerilir.

## 5. KAYNAKLAR


1. http://www.telsizamator.com/default.asp?islem=teknikbilgi&syf=3 Teknik Bilgiler. 30 Temmuz 2009.

2. http://www.telsan.com/FAQ.htm Sık Sorulan Sorular. 30 Temmuz 2009.

3. http://en.wikipedia.org/wiki/Selcall Selcall. 30 Temmuz 2009.

4. http://www.kamusm.gov.tr/tr/Bilgideposu/Belgeler/teknik/aaa/index.html Tübitak UEKAE Açık Anahtar Altyapısı Eğitim Kitabı. 30 Temmuz 2009.

5. Sakallı, M.T. ve Buluş, E., DES'in TMS320C6711 DSP Cihazı Üzerindeki Uygulaması, Performansı ve Karşılaştırılması, Elektrik Elektronik Bilgisayar Mühendisliği Sempozyumu (ELECO), Aralık, Bursa. http://www.emo.org.tr/ekler/f9e3767ef3b10a0_ek.pdf. 30 Temmuz 2009.

6. Eskici, A., Kriptografi. http://www.alieskici.com/matematik 30 Temmuz 2009.

7. http://www.shoghi.co.in/vhf_uhf_radio_encryption.html VHF/UHF Radio Encryption. 30 Temmuz 2009.

8. http://www.efjohnsontechnologies.com/products/encryption Encryption Modules. 30 Temmuz 2009.

9. http://tr.wikipedia.org/wiki/Ses_sinyali Ses Sinyali. 30 Temmuz 2009

10. Leib H. ve Pasupathy S., Error-Control Properties of Minimum Shift Keying, IEEE Communications Magazine, 31, 1 (1993) 52-61.

11. Pusane, A. ve Aygölü, Ü., Uzay-Zaman Kodlamalı Çoklu MSK Modülasyonu, 9. Sinyal İşleme ve Uygulamaları (SİU) Kurultayı, Nisan 2001, Gazi Mağusa, K.K.T.C., Bildiriler Kitabı, 312-317.

12. Türkoğlu, İ., Haberleşme Sistemleri-II Ders Notları, Fırat Üniversitesi, Elazığ, 2007.

13. Ertekin, Ö., Telsiz Haberleşme Sistemleri. http://www.qsl.net/ta1kb/aselsan/telsizhaberlesmesistemleri.htm 30 Temmuz 2009.

14. Menezes, A.J., Oorschot, P.C.V. ve Vanstone, S.A., "Handbook of Applied Cryptography", 1. Baskı, CRC Press, USA, 1996.

15. Zimmermann P., An Introduction to Cryptography, PGP Corporation, U.S., 2004.

16. Altan, K., Kaşkaloğlu K., Saygı, Z., Yıldırım, E. ve Yıldırım, M., "Kriptolojiye Giriş Ders Notları", ODTÜ Uygulamalı Matematik Enstitüsü, Ankara, 2004.

17. Pell, O., Cryptology. http://www.ridex.co.uk/cryptology/#_Toc439908850. 30 Temmuz 2009.

18. Çimen, C., Akleylek, S. ve Akyıldız, E., "Şifrelerin Matematiği : Kriptografi", 1.Baskı, ODTÜ Yayıncılık, Ankara, 2007.

## 6. EKLER

**Ek 1.** Kriptolojinin Tarihçesi

Kriptoloji çok eski çağlardan beri insanoğlu tarafından kullanılmaktadır. Bu tarihçeye kısaca bakacak olursak [4]:

- MÖ 1900 dolaylarında bir Mısırlı kâtip yazdığı kitabelerde standart dışı hiyeroglif işaretleri kullandı.
- MÖ 60–50 Julius Caesar (MÖ 100–44) normal alfabedeki harflerin yerini değiştirerek oluşturduğu şifreleme yöntemini devlet haberleşmesinde kullandı. Bu yöntem açık metindeki her harfin alfabede kendisinden 3 harf sonraki harfle değiştirilmesine dayanıyordu.
- 725–790 Abu Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi, kriptografi hakkında bir kitap yazdı (Bu kitap kayıp durumdadır). Kitabı yazmasına ilham kaynağı olan, Bizans imparatoru için Yunanca yazılmış bir şifreli metni çözmesidir. Abu Abd al-Rahman, bu metni çözmek için ele geçirdiği şifreli mesajın başındaki açık metni tahmin etme yöntemini kullanmıştır.
- 1000–1200 Gaznelilerden günümüze kalan bazı dokümanlarda şifreli metinlere rastlanmıştır. Bir tarihçinin dönemle ilgili yazdıklarına göre yüksek makamlardaki devlet görevlilerine yeni görev yerlerine giderken şahsa özel şifreleme bilgileri (belki şifreleme anahtarları) veriliyordu.
- 1586 Blaise de Vigenère (1523-1596) şifreleme hakkında bir kitap yazdı. İlk kez bu kitapta açık metin ve şifreli metin için otomatik anahtarlama yönteminden bahsedildi. Günümüzde bu yöntem hala DES CBC ve CFB kiplerinde kullanılmaktadır.
- 1623'de Sir Francis Bacon, 5-bit ikili kodlamayla karakter tipi değişikliğine dayanan stenografı buldu.
- 1790'da Thomas Jefferson, Strip Cipher makinesini geliştirdi. Bu makineyi temel alan M-138-A, ABD donanmasının 2.Dünya savaşında da kullandı.
- 1917'de Joseph Mauborgne ve Gilbert Vernam mükemmel şifreleme sistemi olan "one-time pad"'i buldular.

**Ek 1.'in devamı**

- 1920 ve 1930'larda FBI içki kaçakçılarının haberleşmesini çözebilmek bir araştırma ofisi kurdu.
- William Frederick Friedman, Riverbank Laboratuarlarını kurdu, ABD için kriptoanaliz yaptı, 2. Dünya savaşında Japonlar'ın Purple Machine şifreleme sistemini çözdü.
- 2. Dünya savaşında Almanlar Arthur Scherbius tarafından icat edilmiş olan Enigma makinasını kullandılar. Bu makine Alan Turing ve ekibi tarafından çözüldü.
- 1970'lerde Horst Feistel (IBM) DES'in temelini oluşturan Lucifer algoritmasını geliştirdi.
- 1976'da DES (Data Encryption Standard), ABD tarafından FIPS 46 (Federal Information Processing Standard) standardı olarak açıklandı.
- 1976 Whitfield Diffie ve Martin Hellman Açık Anahtar sistemini anlattıkları makaleyi yayınladılar.
- 1978'de Ronald L. Rivest, Adi Shamir ve Leonard M. Adleman: RSA algoritmasını buldular.
- 1985'de Neal Koblitz ve Victor S.Miller ayrı yaptıkları çalışmalarda eliptik eğri kriptografik (ECC) sistemlerini tarif ettiler.
- 1990'da Xuejia Lai ve James Massey: IDEA algoritmasını buldular.
- 1991'de Phil Zimmerman: PGP sistemini geliştirdi ve yayınladı.
- 1995'de SHA–1 (Secure Hash Algorithm) özet algortiması NIST tarafından standart olarak yayınlandı.
- 1997'de ABD'nin NIST (National Institute of Standards and Technology) kurumu DES'in yerini alacak bir simetrik algoritma için yarışma açtı.
- 2001'de NIST'in yarışmasını kazanan Belçikalı Joan Daemen ve Vincent Rijmen'e ait Rijndael algoritması, AES (Advanced Encryption Standard) adıyla standart haline getirildi.

# ÖZGEÇMİŞ

Sibel ARSLAN, 1983 yılında Ankara'nın Polatlı ilçesinde doğdu. İlköğrenimini Sakarya İlkokulu'nda, ortaokul öğrenimini Polatlı Lisesi Ortaokul kısmı ile İstiklal İlköğretim Okulu'nda ve lise öğrenimini Polatlı Yabancı Dil Ağırlıklı Lise'de yaptı. 2001 yılında Mühendislik Mimarlık Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü'nde lisans programına başladı ve 2005 yılında bu bölümden mezun oldu. 2006 yılında Karadeniz Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik-Elektronik Mühendisliği Anabilim Dalı'nda yüksek lisans programına başladı. 2006–2008 yılları arasında Emniyet Genel Müdürlüğü, Haberleşme Dairesi Başkanlığı, Mühendislik Hizmetleri Şube Müdürlüğü'nde mühendis olarak görev yaptı. 2008 yılından beri GATE Elektronik San. ve Tic. A.Ş. şirketi AR-GE bölümünde AR-GE mühendisi olarak çalışmaktadır. İyi derecede İngilizce bilmektedir.