İLETİŞİM DÜNYASINDA KULLANILAN MOBİL HABERLEŞME SİSTEMLERİNDEKİ ŞİFRELEME ALGORİTMALARI ARASINDAKİ GÜVENLİK FARKLARI

Fatma AKGÜN*, Ercan BULUŞ **

**) Trakya Üniversitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, EDİRNE, fatmaakgun@trakya.edu.tr Tel: + 90 284 212 08 08; Fax: + 90 284 215 00 75*

***) Namık Kemal Üniversitesi Çorlu Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, Çorlu / TEKİRDAĞ, ercanbulus@nku.edu.tr Tel: + 90 282 652 94 75 - 76 ; Fax: + 90 282 652 93 72*

ÖZET

İletişim sistemleri teknolojik olarak günden güne büyük oranda gelişim göstermektedir. Ilk haberleşme sistemi olan Analog haberleşme sisteminde sayısal bir iletim olmadığından herhangi bir şifreleme ya da kimlik doğrulama işlemi yapılmamış ve yeterli güvenlik sağlanamamıştır, fakat daha sonra yapılan çalışmalar ile dijital haberleşme sistemi ortaya çıkarılmış, bu sayede kimlik doğrulama işlemi ve konuşmaların şifreli iletimi gerçekleştirilmiştir. Tüm bu yenilikler ile iletişim dünyasında güvenli haberleşmenin adımı atılmıştır. Günümüzde birçok ülkede 2G olarak adlandırılan ikinci nesil haberleşme sistemi kullanılmaktadır. Fakat kullanılan bu sistemin bant genişliğinin yetersizliğinden dolayı, sesin yanı sıra video görüntülerinin ve büyük verilerin aktarımında bağlantıda çok fazla yavaşlık yaşandığı ve şifreleme işlemlerinde çeşitli güvenlik açıkları ortaya çıktığı için üçüncü nesil olarak adlandırılan 3G sistemi ortaya çıkarılmıştır. Ülkemizde de bu sisteme geçiş çalışmaları yoğun biçimde yapılmaktadır.

Çalışmamızda ikinci nesil ve üçüncü nesil mobil iletişim sistemlerinde kullanılan şifreleme algoritmaları ve bunlar arasındaki güvenlik farkları üzerinde durulmuştur.

Anahtar Kelimeler: mobil haberleşme, 2G, 3G, şifreleme, güvenlik.

1. GİRİŞ

İletişim dünyası, gün geçtikçe yenilikler ile insanlığa büyük hizmetler sunmaktadır. Verilerin şifreli iletiminden tutunda görüntülü konuşmaya kadar yeni yeni gelişmeleri, bilim dünyasında ilgi uyandırmaktadır. Artık istediğimiz an istediğimiz kişiyle konuşup aynı anda görüşebiliriz. Fakat bu esnada güvenlik kavramının da ihmal edilmemesi gerekir. Güvenlik; kullanıcının ve baz istasyonunun kimlik doğrulamasından başlanarak, verilerin şifreli, eksiksiz ve değişmeksizin iletimini de kapsayan bir kavram olarak karşımıza çıkar. Şifreleme, Sezar'dan başlayarak gelişmekte, verinin her türlü iletiminde verinin gizlenmesi ve güvenli bir şekilde iletilmesi için kullanılmaktadır. Şifreleme işlemini sağlayan şifreleme algoritmaları bir kripto sistemin temel öğesidir. Bir kripto sistem; şifreleme algoritması, anahtar, açık metin ve şifreli metinden oluşmaktadır. İletişim dünyasında da sayısal haberleşme tekniklerinin kullanılması ile verilerin şifrelenmesi işlemi gerçekleşmiş ve her bir yeni haberleşme tekniğinde daha yeni daha güvenilir şifreleme algoritmaları kullanmıştır.

2. GSM

2.1. Genel Mobil İletişim Sistemi (Global System for Mobile Communication)

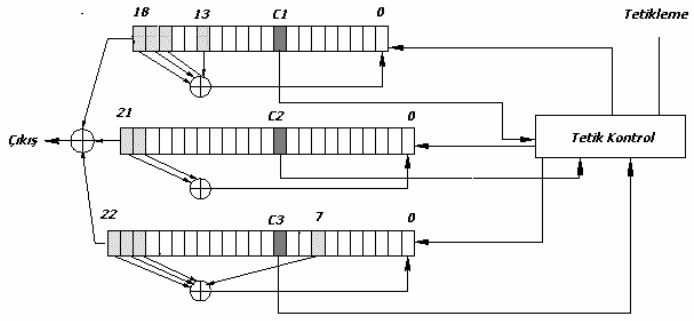
GSM bugün dünyada yoğun olarak kullanılan ve ikinci nesil (2G) haberleşme sistemi olarak adlandırılan bir mobil telefon sistemidir. Avrupa'da 1982 yılında 900 Mhz frekans hızında, "European Conference of Postal and Telecomunications-CEPT" konferansı tarafından mobil haberleşme sağlayabilen, çok güçlü hücresel bir teknoloji hayata geçirilmiştir. Bu konferansın ardından GSM[1][2] haberleşme standartlarını belirlemek üzere 1989 yılında "European Telecommunications Standarts Institute-ETSI" kurulmuş ve bu kuruluş GSM haberleşme standardı olarak kabul edilmiştir. Geliştirilen bu yeni mobil haberleşme sisteminde iletişim sayısal olarak yapılabildiğinden, haberleşmede çeşitli kriptografik algoritmalar da uygulanabilmiştir.

2.2. GSM Haberleşme Sisteminde Güvenlik

Şifrelemede akış (stream) şifreleme yani A5 algoritması kullanır. A5, hava kanalı üzerinden ses şifrelemede kullanılan güçlü bir şifreleme algoritmasıdır. Şifreleme işlemi, A8 (HASH Algoritması) anahtar üretme algoritmasından elde edilen 64 bitlik oturum anahtarı (K) ve 22 bitlik çerçeve numarası (F_n) ile başlatılır. Akış şifre, her bir çerçeve (frame) gönderildiğinde tekrar başlangıç

durumuna getirilir. Aynı K arama süresince kullanılır, fakat 22 bit çerçeve numarası (Fn) arama süresince değişir, böylece her bir çerçeve için benzersiz bir ***keystream*** kullanılır.

A5 algoritması üç farklı uzunlukta kayıtçıdan (LFSR) oluşmaktadır. Bu üç kayıtçının toplam uzunluğu 64 bittir. Her bir kayıtçı sırasıyla R1, R2, R3 olarak ifade edilen ve 19, 22 ve 23 bit uzunluğunda geri beslemeli polinomlara dağılmıştır. R1 kayıtçısındaki 13, 16, 17, 18 nolu bit pozisyonları, R2'deki 20,21. bit pozisyonları, R3'deki 7,20,21,22. bit pozisyonları önemli bit gruplarıdır. Bu bit grupları **tap** olarak isimlendirilir. Kayıtçılar her tetiklendiğinde her bir kayıtçıya ait taplar kendi aralarında XOR'lanır ve sonuç sola kaydırmalı kayıtçının en sağ bitinde depolanır. Major kuralına göre bu bitler tetiklenir. Her bir kayıtçıda tek bir tetikleme tapı vardır. R1 için 8, R2 için 10 ve R3 için 10 numaralı taplar. Her bir saat çevriminde tetiklenen tapların major fonksiyonu hesaplanır ve sadece majority biti ile uyuşan bu taplar tetiklenir. Örneğin kayıtçıların bitleri 1,1 ve 0 ise ilk iki kayıtçı tetiklenir veya kayıtçının bitleri 0,1 ve 0 ise ilk ve üçüncü kayıtçı tetiklenir. Böylece her bir çevrimde en az iki kayıtçı tetiklenmiş olur.



Şekil 1. A5 Algoritması LFSR Yapısı

Oturum anahtarı K ve çerçeve sayıcısı (frame number) Fn ile pseudo random bitlerinin üretim işlemi 4 adımda gerçekleşir.

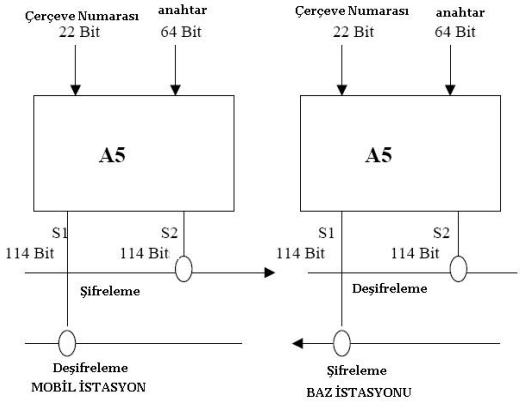
1-) 3 register'da sıfırlanır ve 64 döngü için saatlenir. (stop/go saat kontrolü görmezden gelinerek) bu periyod boyunca K'nın her bir biti, üç registerın lsb's içinde paralel olarak XOR'lanır. (lsb'den msb'ye-en önemsiz bitlerden en önemli bitlere doğru hareketlenme olur.)

2-) 3 register 22 ek döngü için saatlenir. Bu periyot boyunca Fn'in bitleri ardışık olarak, 3 registerın lsb'sinin içinde paralel olaraktekrar tekrar XOR'lanır. Bu adımın sonunda bu üç registerın içeriği, çerçevenin başlangıç durumu olarak adlandırılır.

3-) Herhangi bir çıkış üretmeksizin stop/go saat kontrolü ile bu üç register ek olarak 100 saat döngüsü için zamanlanır.

4-) Sonunda da 228 çıkış biti üretmek için stop/go saat kontrolü ile bu üç register 228 ilave saat döngüsü için zamanlanır. Her bir saat döngüsü bir çıkış biti, üç registerın msb'sinin XOR'lanması ile üretilir

Elde edilen bu 228 bitlik keystream değerinin 114 biti giden verileri şifrelemek diğer 114 biti ise gelen verileri deşifrelemek için kullanılır. Bu işlemlerin aynısı aynı anda hem alıcı hem de gönderici tarafta yapılır[3][4]. Bu şekilde şifreli konuşma yada şifreli veri aktarımı işlemleri gerçekleşmiş olur.



Şekil 2. A5 Şifreleme Algoritması[12]

3. CDMA

3.1. Kod Bölmeli Çoklu Erişim (Code Division Multiple Access System) Sistemi

Kimlik doğrulama ve güvenlik hem Amerika da hem de Avrupa da sürmekte olan önemli konudur. Amerika'da 2G Mobil haberleşme sistemi olarak iki rakip standart kullanır. TDMA ve CDMA (Zaman ve Kod Bölmeli Çoklu Erişim) teknolojileri. TDMA kavramı GSM'e benzerdir fakat detayda bazı farklılıklar vardır, CDMA ise temelden farklı bir yapıdır.

Birinci nesil hücresel sistemlerde, çoklu erişim tekniği olarak sadece Frekans Bölmeli Çoklu Erişim kullanılırken, 2G sistemlerde FDMA'in yanı sıra Zaman Bölmeli Çoklu Erişim ve Kod Bölmeli Çoklu Erişim de kullanılmaktadır. CDMA'in ilk versiyonunda (IS-95a) data transfer hızı 14,4 Kbit/s seviyesinde iken, sağlanan gelişmelerle yeni versiyonda (IS-95b) bu hız 115 Kbit/s'a ulaşmıştır. Günümüzde sesten daha çok data talebinin arttığı dikkate alınırsa, data transfer hızının artırılmış olması, CDMA teknolojisinin avantajlı hale gelmesi anlamını taşımaktadır[5].

3.2. CDMA Sisteminde Güvenlik

CDMA ağındaki başlıca güvenlik 64 bitlik gizli anahtar olan "A-key" ve Elektronik Seri Numarası (ESN) bağlıdır. A-key hem mobil hem de kimlik doğrulama merkezi (Authentication Center) içinde saklıdır. Mobil ve ağın her ikisi de giriş olarak, Elektronik Seri Numarası (ESN), operatör ve ağ tarafından sağlanan A-key ve RAND değerlerini giriş olarak alır ve bu değerleri CAVE (Cellular Authentication and Voice Encryption) algoritması ile işleme alarak SSD değerini yani ikinci anahtarı üretir[6]. Üretilen 128 bitlik SSD değeri;

- ✓ SSD-A (64 bit) , kimlik hesabı için kullanılır.
- ✓ SSD-B (64 bit) , ses ve sinyal mesajlarını şifrelemede kullanılır.

SSD-A, bazı mobil aboneler için 18 bitlik kimlik tanıma imzası üretir ve mobil bunu baz istasyonuna gönderir. Bu imza, baz istasyonu tarafından sahte erişimleri engellemek üzere mobil kullanıcıyı tanımlamak için kullanılır. Diğer işlem olarak yine CAVE Algoritması, SSD_B, RAND ve ESN değerlerini giriş olarak alır ve Voice Privacy Mask, Data Key ve CMEA Key değerlerini üretir[7]. Elde edilen bu Data Key değeri ORYX algoritması ile birlikte hava kanalı üzerinden iletilen verileri şifrelemek için kullanılır[8]. ORYX, LFSR tabanlı bir tür ikili (binary) akım şifreleyicisidir. ORYX uzunlukları 32 bit olan, $LFSR_A$, $LFSR_B$ ve $LFSR_K$ seklinde gösterilen 3 LFSR'in birleşmesinden oluşmuştur. Sistem ayrıca 0-255 arasında permütasyon işlemlerinden sorumlu olan bir S kutusuna da sahiptir. $LFSR_K$ 'nın ilkel geri besleme çokterimlisi aşağıdaki gibidir:

$LFSR_K$:
$x^{32} + x^{28} + x^{19} + x^{18} + x^{16} + x^{14} + x^{11} + x^{10} + x^9 + x^6 + x^5 + x + 1$

$LFSR_K$'nın içeriğine bağlı olarak, $LFSR_A$ aşağıda belirtilen iki ilkel çokterimlisinden birisini kullanarak her çevrimde kendini güncellemektedir.

$LFSR_A$:
$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

ve

$x^{32} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{17} + x^{13} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^2 + x + 1$

Son olarak $LFSR_B$, aşağıdaki geri besleme çok terimlisine sahiptir.

$LFSR_B$:
$x^{32} + x^{31} + x^{21} + x^{20} + x^{16} + x^{15} + x^6 + x^3 + x + 1$

ORYX anahtar akım dizilerini byte byte oluşturmaktadır. Her byte ise su şekilde üretilmektedir: $LFSR_K$ bir defa saatlenir, $LFSR_A$ ise $LFSR_K$ 'nın içeriğine bağlı olarak iki geri besleme çokterimlisinden biriyle saatlenir. Hangi geri çokterimlinin seçileceği LFSRK'nın son sekiz bitine bağlıdır. $LFSR_B$ ise yine $LFSR_K$'nın son sekiz bitine bağlı olarak bir defa veya iki defa saatlenir. Daha sonra, $LFSR_A$'nın ve $LFSR_B$'nin son sekiz bitleri permütasyon işlevine sokulur ve $LFSR_K$'nın son sekiz biti ile XOR'lanırlar. Permütasyon *L,* konuşma boyunca değişmemektedir ve arama işlemi boyunca açık olarak aktarılan bir değer ile başlatılan, bilinen bir algoritmadan oluşturulur. Bu durum aşağıdaki şekilde ifade edilebilir.

Anahtar akım dizisi = (Yüksek8K + *L*[Yüksek8A] + *L*[Yüksek8B]) mod 256

Şifreleme işlemi, veri bitleri ile anahtar akım dizisinin XOR'lanması ile elde edilir.

4. UMTS

4.1. Uluslar arası Mobil Haberleşme Sistemi (Universal Mobile Telecommunication System)

UMTS, GSM'in gelişmiş bir halidir. 3.nesil (3G) haberleşme sistemidir ve genellikle Avrupa'da yoğun olarak kullanılır. Geniş bandlı çoklu ortam (ses, resim ve video aktarımı) servislerinin kullanılmasına olanak sağlayarak yüksekbit hızlarını desteklemektedir. Aktarım hızı yakın lokasyonlarda saniyede 2 Mb/s bulurken uzak lokasyonlarda 384 Kb/sseviyelerinde işlem göstermektedir. UMTS içindeki güvenlik 128 bit şifreleme anahtar uzunluğu ile daha güçlü şifreleme ve karşılıklı kimlik doğrulaması gibi artı işlemleri kapsar[9].

4.2. UMTS Sisteminde Güvenlik

Mitsuru Matsui, lineer ve diferansiyel kriptanalizin her ikisine de karşı güvenilirliği tam olan MISTY1 adında bir blok şifreleme algoritmasını tasarlamıştır. MISTY1, 128 bit anahtar uzunluğu ve 64 bit data bloğunda işlem yapan bir blok şifreleme işlemidir. Güvenilirliği oldukça yüksek bir algoritmadır. Bu sebepten dolayı Avrupa İletişim Şirketlerinin tüm üyeleri bir karar alarak MISTY1 yapısının 3G nesil haberleşme sisteminde büyük ölçüde güvenlik sağlayacaklarını ortaya çıkarmışlardır. Bu sebeple MISTY1'in değiştirilmiş versiyonu olarak KASUMI algoritması ortayaçıkarılmıştır. KASUMI, 8 döngülü bir Feistel şifrelemedir. 128 bitlik K anahtarını kullanarak 64 bit girişten 64 bit

çıkış üretir. I giriş değeri 32 bitlik iki stringe ayrılmıştır[10][11][12][13].

$I=L_0||R_0$ yani $L_0= I[63:32]$ ve $R_0=I[31:0]$

Her bir i döngü değeri $1\leq j\leq 8$ arasındadır. Kısaca;
$R_i=L_{i-1}$, $L_i=R_{i-1}$ XOR $f_i(L_{i-1},RK_i)$
şeklinde ifade edebiliriz.

KASUMI, FL, FO ve FI adı verilen, Feistel yapısında da içeren KL, KO ve KI alt anahtarlarını kullanan, alt fonksiyonları kullanır. Alt anahtar değerler şu şekilde elde edilir; KASUMI 128 bitlik K anahtarına sahiptir. Her bir KASUMI döngüsü bu K'dan elde edilen 128 bit yeni anahtar değerini kullanır. Döngü anahtarlarından önce 16 bitlik K_j ve K_j^I (j=1 to 8) dizileri elde edilip hesaplanır. 128 bit anahtar 16 bitlik 8 alt değere bölünür. $K_1,\ldots K_8$

K=K1 || K2 || K3 || K4 || K5 || K6 || K7 || K8
K_j^I dizisi K_j den elde edilir. Her bir j integer değeri için $1\leq j\leq 8$

$K_j^I= K_j$ XOR C_j ifadesi ile elde edilir.

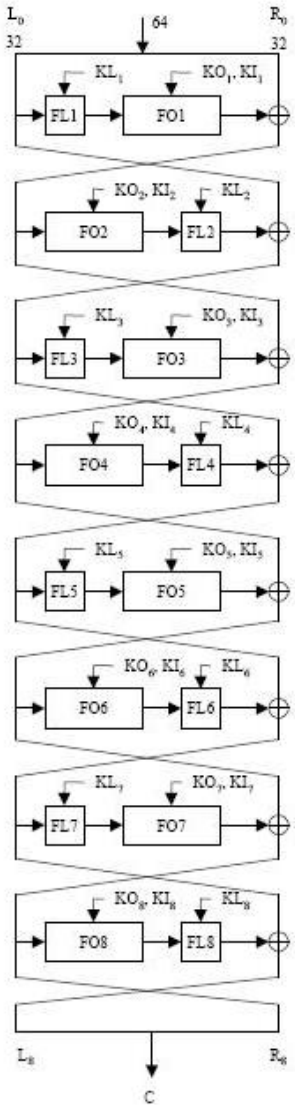
Alt Anahtarlar	i. döngü çıkışı	C_i Değerleri
KL_{i1}	K_i <<< 1	C_1 0x0123
KL_{i2}	$K^I_{i+2\ (mod\ 8)}$	C_2 0x4567
KO_{i1}	$K_{i+1\ (mod\ 8)}$ <<< 5	C_3 0x89AB
KO_{i2}	$K_{i+5\ (mod\ 8)}$ <<< 8	C_4 0xCDEF
KO_{i3}	$K_{i+6\ (mod\ 8)}$ <<< 13	C_5 0xFEDC
KI_{i1}	$K^I_{i+4\ (mod\ 8)}$	C_6 0xAB98
KI_{i2}	$K^I_{i+3\ (mod\ 8)}$	C_7 0x7654
KI_{i3}	$K^I_{i+7\ (mod\ 8)}$	C_8 0x3210

Tablo1. Döngü alt anahtarları ve C_i sabitleri

F_i fonksiyonu 64 bit I giriş değerini, RK_i döngü anahtarı (döngü anahtarı KL_i, KO_i ve KI_i üçlü anahtar grubu olarak) kontrollüğünün altında 64 bitlik O çıkış değerine dönüştürür. Fonksiyon yapı olarak iki alt fonksiyondan elde edilir. FL ve FO fonksiyonları KL_i (FL ile kullanılan) ve KO_i-KI_i (FO ile kullanılan) alt anahtar ile birleştirilmiştir. F_i fonksiyonu tek ve çift döngülere bağlı olarak iki biçimde oluşturulmuştur.

1,3,5 ve 7 döngü sayıları için;
$f_i(I,RK_i)=FO(FL(I,KL_i),KO_i,KI_i)$
2,4,6 ve 8 döngü sayıları için;
$f_i(I,RK_i)=FL(FO(I,KO_i,KI_i),KL_i)$

Konuşma esnasında 64 bitlik uygun verilerin, oturum anahtarı ile KASUMI algoritmasına girmesi ile 64 bitlik şifreli veri elde edilmiş olur. UMTS sisteminde ses ve verilerin şifrelenmesi bu şekilde gerçekleşir.



Şekil 3. KASUMI Şifreleme Algoritması

5. CDMA2000

5.1. Code Division Multiple Access 2000 (Kod Bölmeli Çoklu Erişim Sistemi)

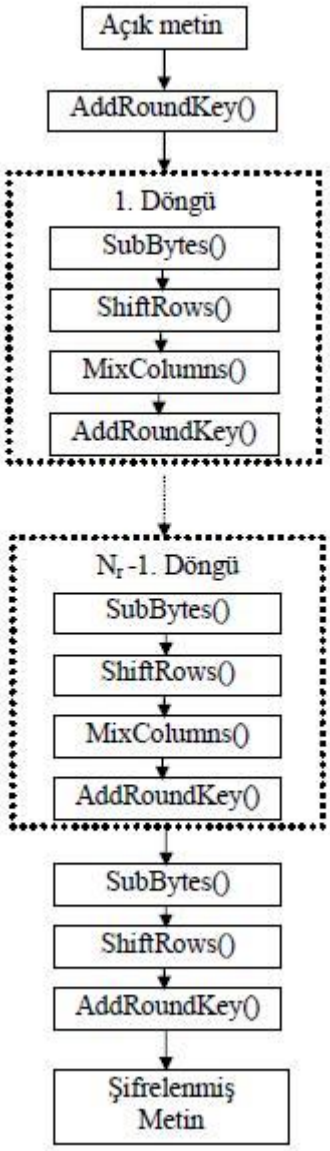
CDMA2000 (Kod Bölmeli Çoklu Erişim) mimarisi, IMT-2000'den elde edilir ve 3GPP2 tarafından belirlenmiştir. Bu sistem önceki 2G/2.5G'yi temel alan ve Amerika'da yoğunlukla kullanılan 3G mobil haberleşme sisteminin bir versiyonudur. Cdma2000, cdmaOne sisteminin gelişmiş halidir. Sistem hareketli halde 144 kb/s hızında, kentsel alanda 384 kb/s ve hareketsiz olarak 2 mb/s hızlarına ulaşabilmektedir. İnternet ve diğer data servislerine hızlı ulaşım sağlar. CDMA2000 ayrıca, sorunsuz global dolaşıma da büyük yarar sağlamıştır. UMTS gibi CDMA2000 'da devre ve paket anahtarlamalı yapıyı desteklemektedir [14][15][16].

5.2. CDMA2000 Sisteminde Güvenlik

CDMA2000 içerisinde, güvenilirlik için Advanced Encryption Standard (AES) algoritması kullanılmaktadır. AES, RIJNDAEL algoritması olarak bilinir. Bu blok şifreleme algoritması, 128 bit anahtar uzunluğu ve 128 bit data bloğunu kullanır. 128 bitlik bu şifreleme anahtarı, f3 tek yönlü SHA-1 algoritmasından elde edilir. Ve CK olarak adlandırılır. Algoritmadan elde edilen sonuç, veriyi şifrelemek veya deşifrelemek için stream cipher içerisinde kullanılır.

AES (Rijndael-Gelişmiş Şifreleme Standardı) algoritması 128 bit veri bloklarını 128, 192, 256 bit anahtar seçenekleri ile şifreleyen bir algoritmadır. SPN algoritmasının geniş bir çeşididir. Döngü sayısı anahtar genişliğine göre değişmektedir. 128 bit anahtar için 10 döngüde şifreleme yaparken 192 ve 256 bit anahtarlar için sırasıyla 12 ve 14 döngüde şifreleme yapmaktadır. AES algoritmasında her döngü dört katmandan oluşur. İlk olarak 128 bit veri 4×4 byte matrisine dönüştürülür. Daha sonra her döngüde sırasıyla byte'ların yerdeğiştirmesi, satırların ötelenmesi, sütunların karıştırılması ve anahtar planlamadan gelen o döngü için belirlenen anahtar ile XOR'lama işlemleri yapılır[17].

Byte'ların yerdeğiştirilmesinde 16 byte değerinin her biri 8 bit girişli ve 8 bit çıkışlı S kutusuna sokulur. Satırların ötelenmesi işleminde 4×4 byte matrisinde satırlar ötelenir ve sütunların karıştırılması işleminde herhangi bir sütun için o sütundaki değerler karıştırılır. Döngünün son katmanında ise o döngüye ait anahtar ile XOR'lama yapılmaktadır.[41] [42] [3] [4] . Bu şekilde şifrelenmiş veri elde edilmiş olur.



Şekil 4 AES Algoritması Ana Akış Şeması[62]

6. ŞİFRELEME ALGORİTMALARI ARASINDAKİ GÜVENLİK FARKLARI

Mobil haberleşme sistemlerinde ses, data, görüntü, mesaj vs. bilgilerin iletiminde şifreleme işlemi mutlaka yapılmaktadır. GSM haberleşme sisteminde anahtar uzunluğu 64 bit olması ve akış şifreleme kullanılması bir zafiyet oluşturmuş ve A5 şifreleme algoritması çok kısa bir zaman içerisinde kırılmıştır[18][19][20]. Bu işlem sonucunda güvenilirliği olmayan bu algoritma yerine yeni algoritmaların arayışı içerisine gidilmiştir. Diğer 2G sistemi olan CDMA haberleşme sisteminde de kimlik doğrulama için CAVE[21][22], sinyal şifreleme için CMEA[23] ve veri şifrelemek için 32 bitlik şifreleme anahtarı ve yine LFSR tabanlı akış şifreleme algoritması olan ORYX[24] kullanılmasına rağmen bu algoritmaya da yapılan saldırılar başarılı olmuş ve algoritma kolayca çözümlenebilmiştir. Bu sistem üzerinde de güvenilir bir iletişim sağlanamamıştır. Bu sebepten yeni nesil sistemler olan UMTS ve CDMA2000 sistemlerinde 128 bit anahtar uzunluğu ve blok şifreleme algoritmalarının kullanılması diğer sistemlere oranla daha güçlü güvenlik sağlanmasına neden olmuştur. Bu sistemlerde kullanılan KASUMI ve AES şifreleme algoritmalarına henüz tamamen bir kriptanaliz işlemi yapılamamıştır. KASUMI algoritması 8 döngülü olmasına rağmen kriptanaliz çalışmalarında henüz 5 döngüde bir sonuç bulunabilmiştir[25][26]. AES şifreleme algoritmasında ise henüz tamamıyla çözümlenememiştir[17]. Her iki sistemde şuan en güvenilir sistem olarak kabul edilmiştir. Ayrıca bu sistemler hız, güvenlik, kapsama alanı olarak tüm dünyada sorunsuz olarak çalışabilmektedir.

7. SONUÇ

Çalışmamızda, mobil haberleşme teknolojilerinden ve bu teknolojilerin ses ve dataları şifrelemek için kullandığı güvenlik algoritmalarından bahsettik. Her bir haberleşme sistemini birbirinden farklı şifreleme algoritmaları kullanmaktadır. Bazı mobil sistemler, veri şifrelemenin hızlı yapılabilmesi için fazla donanım gerektirmeyen şifreleme algoritmaları kullanmaktadır. Fakat bu algoritmalar arasında çeşitli güvenlik farkları vardır. Şifrelemede, blok şifrelemelerin kullandıkları yapı itibari ile (S-kutuları, permutasyon, alt fonksiyonlar vs.) akış şifrelemelere oranla daha güvenilir bir yapı oluşturmaktadır. Yaptığımız araştırmalarda bazı mobil haberleşme sistemlerinin gerçekten güvenilir algoritmalar kullandığını fakat bazılarında ise güvenliklerinde açıklar olduğunu ve bu açıklardan yararlanarak saldırganların algoritmaları kolayca kırabildiklerini gördük.

KAYNAKLAR

[1] Martin Sauter, "Communication Systems for the Mobile Information Society", 2006.

[2] Praphul Chandra, Bulletproof Wireless Security, Communications Engineering Series, Elsevier, 2005.

[3] Lauri Tarkkala, "Attacks against A5", Seminar on Network Security, 2000.

[4] Elad Barkan, Eli Biham, Nathan Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", 2004.

[5] Nihal Çetinkaya, "Kablosuz Haberleşmede Kod Bölmeli Çoklu Erişim", Gazi Üniversitesi Fen Bilimleri Enstitüsü Elektrik-Elektronik Mühendisliği, Yükseklisans Tezi 2007.

[6] Keonwoo Kim, Dowon Hong, and Kyoil Chung, "Application of ESA in the CAVE Mode Authentication", Procedings Of World Academy Of Science, Engineering and Technology Volume 18 December 2006.

[7] Debdeep Mukhopadhyay and Dipanwita RoyChowdhury, "Customizing Cellular Message Encryption Algorithm", International Journal of Network Security, Vol.7, No.2, PP.194{202, Sept. 2008

[8] İmran Ergüler, Emin Anarım, "Hücresel İletişim Sistemleri İçin Yeni Bir Akım Şifreleme Modeli", IEEE 2005

[9] Geir M. Kqien, Telenor R&D and Agder University College, "An Introduction To Access Security In UMTS", IEEE Wireless Communications, February 2004.

[10] Specification of the 3GPP Confidentiality and Integrity Algorithms, Document1: f8 and f9 Specifications, 2000.

[11] Specification of the 3GPP Confidentiality and Integrity Algorithms, Document2: KASUMI Specifications, 1999.

[12]Kaisa Nyberg, Cryptographic Algorithms For UMTS, ECCOMAS, 2004.

[13] Sedat Akleylek, "On The Avalanche Properties Of Misty1, Kasumi and Kasumi-R", Middle East Technical Universty, 2008.

Cdma2000

[14] Ai-Chun Pang, Jyh-Cheng Chen,Yuan-Kai Chen, Prathima Agrawal, "Mobility and Session Management: UMTS vs. cdma2000", IEEE Wireless Communications, February 2004.

[15]Greg Rose,Geir M. Kqien, "Access Security In Cdma2000, Including A Comparison With UMTS Access Security", IEEE Wireless Communications, February 2004.

[16]Minho Shin, Justin Ma, Arunesh Mishra and William A. Arbaugh, "Wireless Network Security and Interworking", Proceeding of the IEEE, Vol. 94, No.2, February 2006.

[17] Tolga Sakallı, "Modern şifreler ve bu şifrelere karşı yapılan başlıca önemli saldırı teknikleri", Doktora Tezi, T.Ü Fen Bilimleri Enstitüsü, 2006.

[18] Eli Biham, Orr Dunkelman, "Cryptanalysis of the A5/1 GSM Stream Cipher NES/DOC/TEC/WP3/005/a", European Union fund IST-1999-12324- NESSIE and by the Technions's Chais Excellence Program, 2001.

[19] Alex Biryukov, Adi Shamir, David Wagner, "Real Time Cryptanalysis of A5/1 on a PC", 1999.

[20] Jovan Dj. Golic, Cryptanalysis of Alleged A5 Stream Cipher, School of Electrical Engineering, University of Belgrade, Beograd Yugoslavia, 1997.

[21] William Millan, Praveen Gauravaran, Cryptanalysis of the Cellular Authentication and Voice Encryption Algorithm, Information Security, 17-26 Feb, 2005.

[22] Praveen S.S Gauravaram and William L. Millan, "Improved Attack on the Cellular Authentication and Voice Encryption Algorithm", Information Security Research Centre, Queensland University of Technology, Australia, 2005

[23] David Wagner, Bruce Schneier, John Kelsey, "Cryptanalysis of the Cellular Message Encryption Algorithm", 1999

[24] D. Wagner L. Simpson, E. Dawson, J. Kelsey, W. Millian, B. Schneir, "Cryptanalysis of ORYX", 2000.

[25] Issam W. Damaj, "igher Level Hardware Synthesis of the KASUMI Algorithm" 2007.

[26] Eli Biham, Orr Dunkelman, Nathan Keller, "A Related-key Regtangle Attack on the Full Kasumi", 2006.