Mobil Ağlarda Güvenlik Doğrulaması Hakkında Bir İnceleme

Fatma AKGÜN

İçerik

- Giriş
- Doğru ve Güvenilir Bir Sistem Temeli
- Kimlik Doğrulama Nedir?
- Mobil İletişim Teknolojileri
- Mobil Haberleşme Teknolojilerinde Kimlik Doğrulama İşlemi
- Sonuç ve Öneriler

Giriş

Bilimin uygulamacı yönü olarak bilinen **teknoloji** durmak tükenmek bilmeyen bir hızla ilerlemektedir. Yapılan bu tür yeniliklerin amacı insan hayatını kolaylaştırmak ve hep daha iyisini sunmaktır. Teknolojinin sağladığı büyük kolaylıklar ve yeniliklerle birlikte çeşitli güvenlik riskleri de ortaya çıkarılmıştır.

Asıl metin stillerini düzenlemek için tıklatın

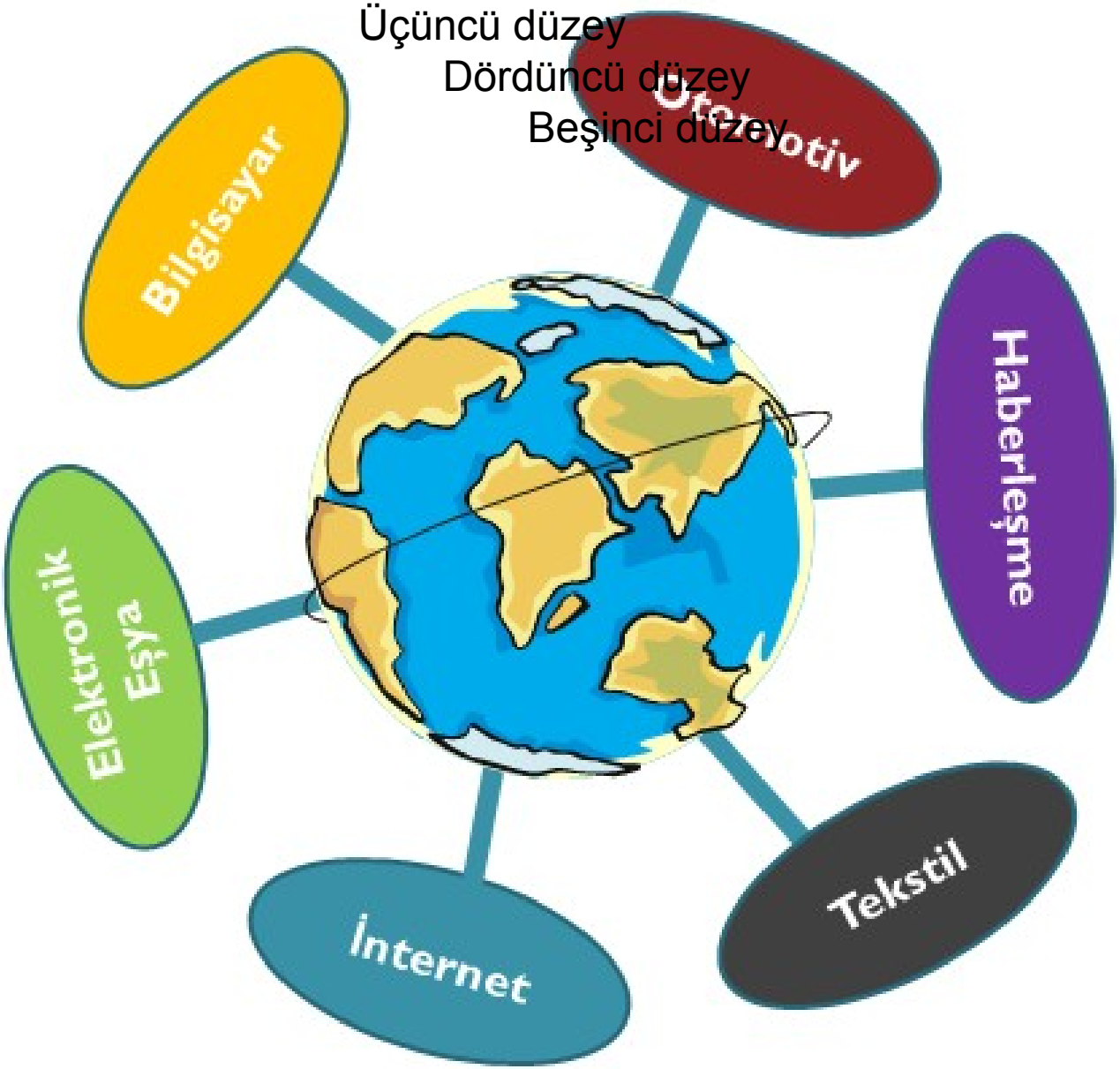
İkinci düzey

Üçüncü düzey

Dördüncü düzey

Beşinci düzey

TEKNOLOJİ ve YENİLİKLERİ

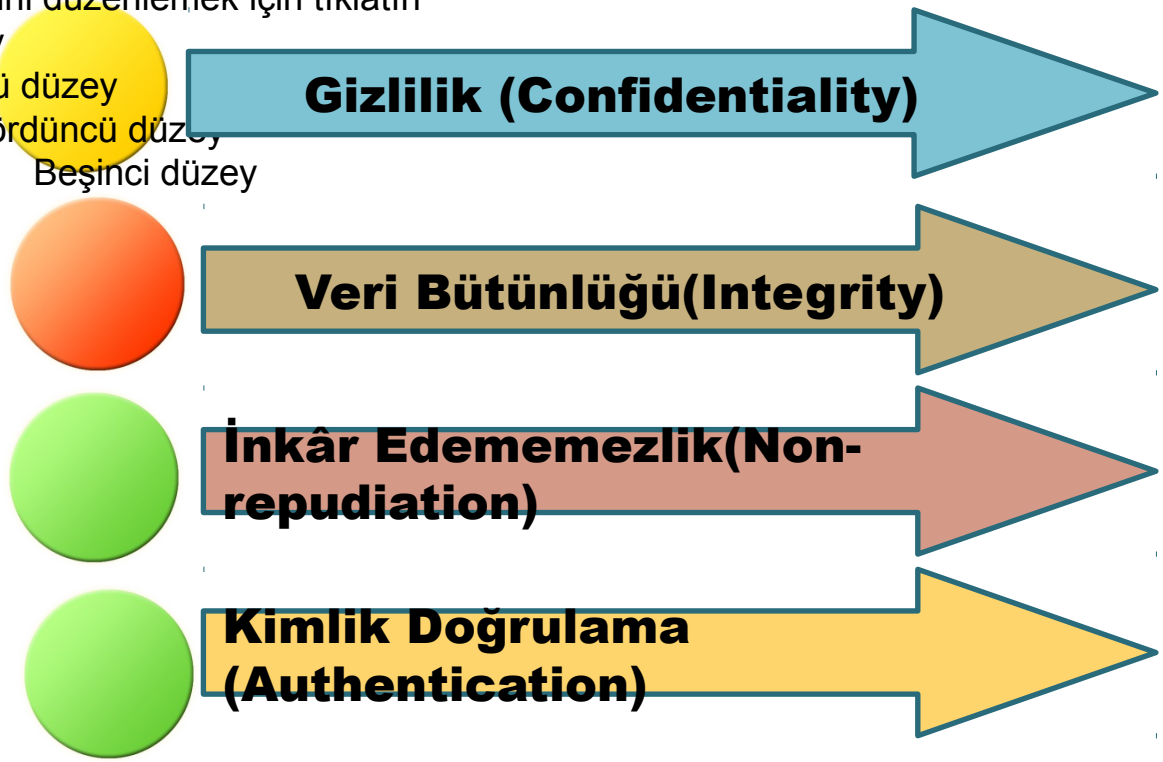


İnternet Kullanımı

Bankacılık Sistemleri
Eğitim
Hastane
Kamu Kurum ve Kuruluş
Özel Şirketler
Yurtlar
Mobil Haberleşme

Doğru ve Güvenilir Bir Sistem Temeli

Asıl metin stillerini düzenlemek için tıklatın
İkinci düzey
Üçüncü düzey
Dördüncü düzey
Beşinci düzey



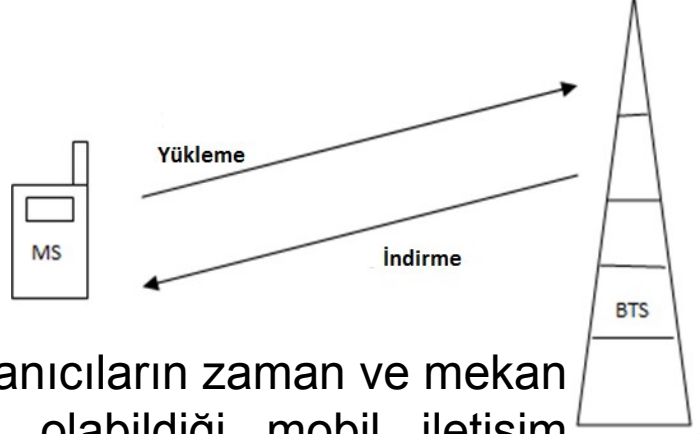
Kimlik Doğrulama Nedir?

Asıl metin stillerini düzenlemek
İkinci düzey
Üçüncü düzey
Dördüncü düzey
Beşinci düzey

Kullanıcıların uzak veya yakındaki herhangi bir sisteme giriş yapıp o sistemi kullanabilmesi yada herhangi bir kişi ile iletişim sağlayabilmesi için kendini o sisteme veya o kişiye tanıtması gerekir. Bu olaya kimlik doğrulaması (authenticaiton) denmektedir.

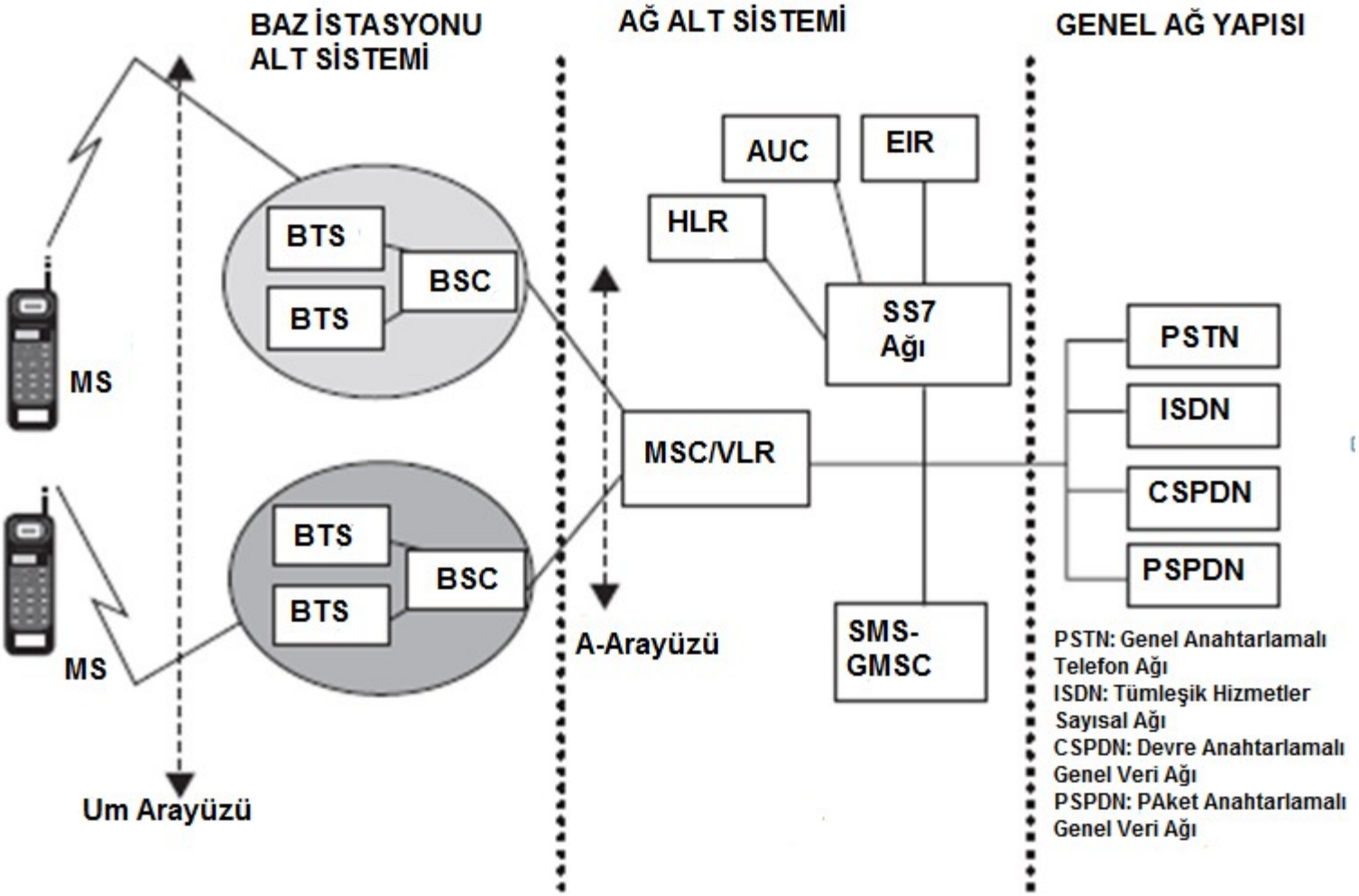
Kimlik Doğrulama İşlemi Çeşitli Şekillerde Olabilir.

Mobil Haberleşme Teknolojisi



Bilim ve teknolojide yapılan gelişmeler ile, kullanıcıların zaman ve mekan bağımsız olarak hareket özgürlüklerine sahip olabildiği mobil iletişim sistemleri ortaya çıkarılmıştır.

Kablolu iletişim sisteminin yarattığı sıkıntı ve kısıtlamalar, insanlar arasında kablosuz iletişim sağlayan mobil haberleşme sistemine geçişi hızlandırmıştır. Mobil iletişim teknolojisinde, kullanıcıların güvenli haberleşmesini sağlamak üzere sistem üzerinde kimlik doğrulama algoritmaları ve bunun yanı sıra veri şifreleme algoritmaları kullanılmıştır.


BAZ İSTASYONU
ALT SİSTEMİ
AĞ ALT SİSTEMİ
GENEL AĞ YAPISI
AUC
EIR
HLR
SS7
Ağı
BTS
BTS
BSC
MS
MSC/VLR
PSTN
ISDN
CSPDN
PSPDN
BTS
BTS
BSC
MS
A-Arayüzü
SMS-
GMSC
Um Arayüzü
PSTN: Genel Anahtarlamalı
Telefon Ağı
ISDN: Tümleşik Hizmetler
Sayısal Ağı
CSPDN: Devre Anahtarlamalı
Genel Veri Ağı
PSPDN: PAket Anahtarlamalı
Genel Veri Ağı

SIM(Subscriber Identity Module-Abone Kimlik Modülü)

Asıl metin stillerini düzenlemek için tıklatın
İkinci düzey
Üçüncü düzey
Dördüncü düzey
Beşinci düzey

2.Nesil Haberleşme Sistemi

GSM(Global System for Mobile Communication)

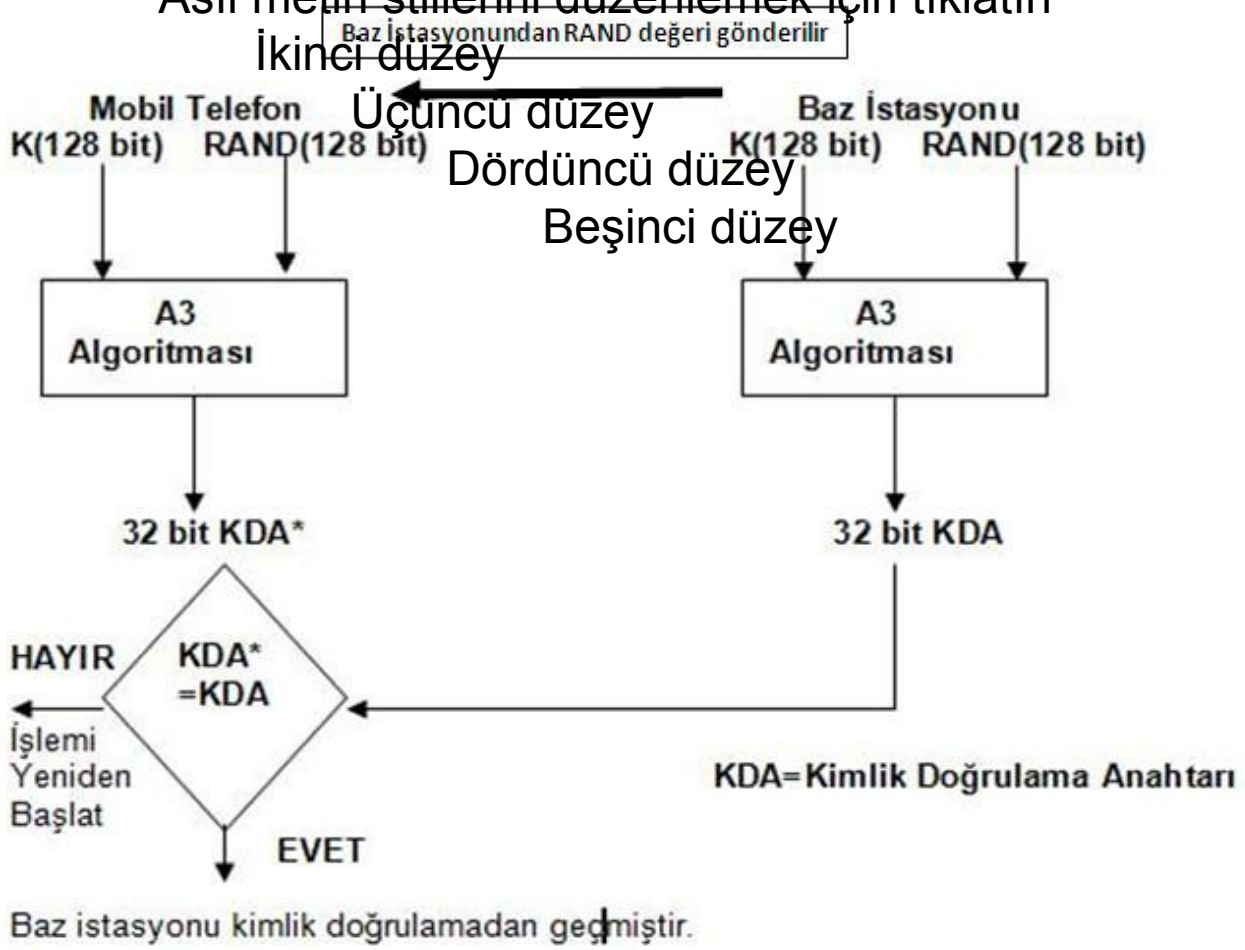
Asıl metin stillerini düzenlemek için tıklatın

İkinci düzey

Üçüncü düzey

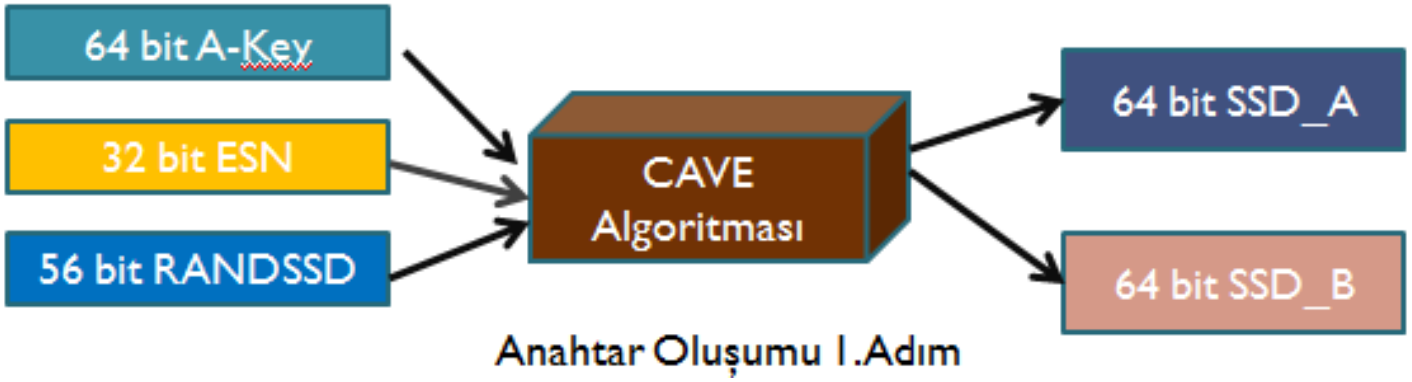
Dördüncü düzey

Beşinci düzey

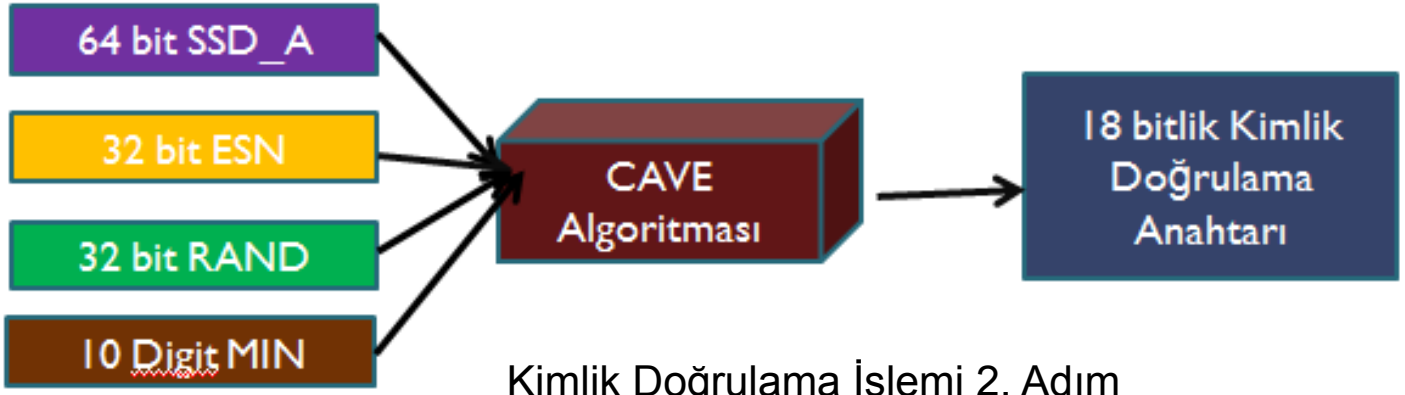


2.Nesil Haberleşme Sistemi

CdmaOne(Code Division Multiple Access)



Anahtar Oluşumu 1.Adım



Kimlik Doğrulama İşlemi 2. Adım

HASH Algoritmaları

HASH fonksiyonlarının;

- Bilginin özetini oluşturmak,
- Bilgiyi sıkıştırmak,
- Veri bütünlüğünü sağlamak
- Sayısal imza yani kimlik doğrulama işlemlerinde

kullanılmak üzere çeşitli uygulama alanları vardır.

Hash fonksiyonları tek yönlü yani one-way fonksiyonlardır. Yani bir fonksiyon yardımı ile verinin özeti kolayca hesaplanabilir fakat özetten verinin elde edilmesi çok zordur. Herhangi bir hash fonksiyonunda giriş verisinin uzunluk değeri değişken olmasına karşın elde edilen sonuç değerinde veri uzunluğu değişmez yani sabittir. Genelde elde edilen hash sonuç değeri, girdiye göre çok daha ufak boyuttadır.

Geleneksel olarak hash fonksiyonlarının iki önemli özelliği vardır. Bunlar;

Tanım 1: Ön görüntü direnci (Preimage resistance-tek yönlülük özelliği **):** özetleme fonksiyonunun tek yönlülük özelliğidir, yani özeti kullanarak özeti alınan mesaja ulaşmak kolay olmamalıdır. Mesaj kümesi özet kümesinden çok daha büyük olduğu için veri kaybı olur, dolayısıyla geri dönülemezler. Mesaj özetinden algoritmayı geriye doğru çalıştırıp 2n' den daha az işlemde mesaj elde edilebildiği takdirde özet fonksiyonunun tek yönlülük özelliği kırılmış olur.

Tanım 2: Çakışma direnci (Collision resistance-güçlü çakışma direnci **):** Verilen herhangi bir mesaj M için, M'den farklı ve aynı özete sahip başka bir mesaj bulunması zor olmalıdır.

Özetlenecek mesaj (girdi) herhangi bir boyutta olabilir.
Mesaj özeti (çıktı) sabit bir uzunluktadır.
Verilen herhangi bir mesaj için özetin hesaplanması kolay olmalıdır.
H(x) tek yönlü olmalıdır.
H(x) çakışmalara dayanıklı olmalıdır.

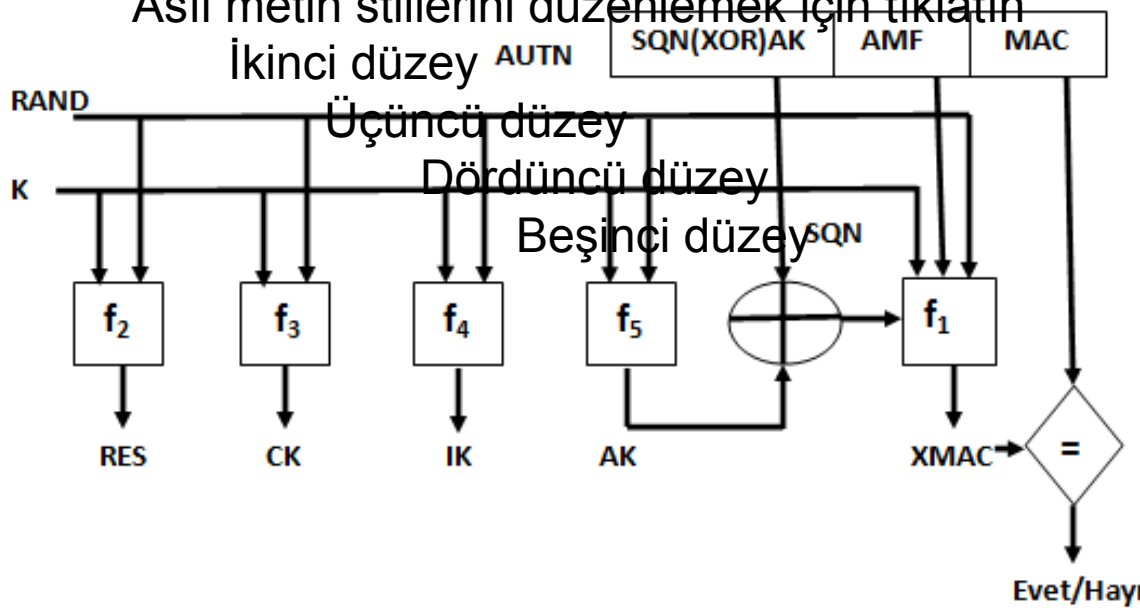
3.Nesil Haberleşme Sistemi

UMTS(Universal Mobile Telecommunications System)

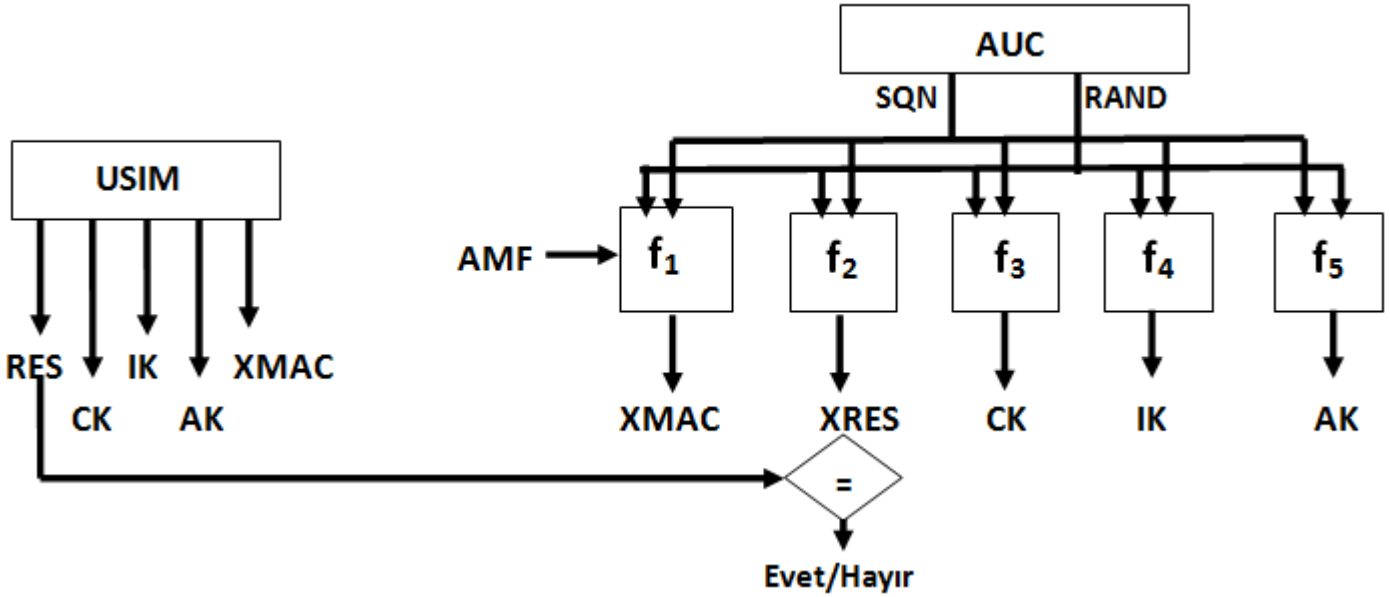
Asıl metin stillerini düzenlemek için tıklatın
İkinci düzey
Üçüncü düzey
Dördüncü düzey
Beşinci düzey

Sim kart ve kimlik doğrulama merkezi (AUC), içerisinde gerçekleşen AKA işleminde (f0-f5) kriptografik fonksiyonlar kullanılır. UMTS, AKA işlemini gerçekleştirmek için MILENAGE algoritmasını kullanır.

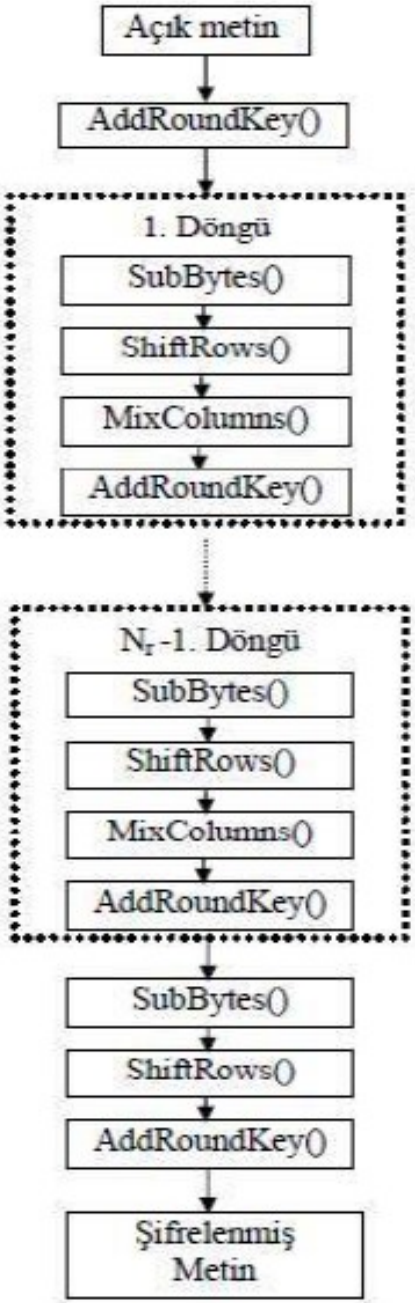
MILENAGE, simetrik blok şifreleme olan RIJNDAEL algoritması üzerine inşa edilmiştir. AKA prosedürü içinde yer alan farklı fonksiyonlar, RAND değerini ve USIM/AUC içerisinde bulunan 128 bitlik master K anahtarını kullanarak, kimlik tanımlama bilgilerini üretirler.



USIM içerisinde baz istasyonunun kimliğinin tanımlanması



Baz İstasyonu Tarafından Kullanıcının Doğrulanması



AES Algoritması Ana Akış Şeması

3.Nesil Haberleşme Sistemi

CDMA2000(Code Division Multiple Access-2000)

Bu haberleşme tekniğinde SIM kart kullanılabilir yada kullanılmaz. Eğer SIM kart taşınabiliyor ise (GSM ve UMTS sistemlerinde de bu şekildedir) K değeri USIM içerisine gömülür, eğer USIM kart taşınamaz ise sadece telefona özgü ise bu durumda K değeri telefon içerisinde varolan hafızaya gömülür.

K değerinin önemi büyüktür çünkü bu değer sayesinde AKA algoritması içerisinde mobil ve servis ağı arasında oturum anahtarları oluşturulur ve veriler güvenilir bir şekilde gönderilir.

CDMA2000 sisteminde UMTS'e göre bazı yeni kriptografik fonksiyonlar eklenmiştir. F11 ve UMAC gibi. F11, AV içerisinde yer alan UIM Kimlik Anahtarı (UAK-USIM Authentication Key) üretmek için kullanılır.

UMAC veya MAC fonksiyonları ise sinyal verisinin bütünlüğünü korumak için kullanılır. UMAC fonksiyonu, IK (Integrity Key-Bütünlük Anahtarı) ve UAK değerlerinin her ikisine de bağlıdır. Ama bazı zamanlar sadece IK değerine bağlı kalabilir.

SHA-1, cdma2000 içerisinde bazı durumlarda kullanılan tek yönlü bir çekirdek fonksiyondur. Kullanıcı kimlik tanımlaması, anahtar elde edilmesi ve mesaj kimlik tanımlaması gibi durumlar için kullanılırken bazı durumlarda da, bu işlemler için CDMA2000, SHA-1 Core Compression fonksiyonu nu kullanır. Ayrıca sistem kullanıcı ve servis ağı arasında gizlilik ve bütünlük koruma için çözüm olarak SS7 protokolünü kullanan IPSec tüneli sayesinde veri aktarımı sağlanır ve bu güvenilir tünel 3. şahısların veriye erişimini engeller.

Sonuç

2G sistemlerde kimlik doğrulamanın tek taraflı yapılması,
Sahte baz istasyonlarına maruz kalınması,
Kimlik doğrulamanın sadece mobil istasyon ve baz istasyonu arasında yapılması,
Kimlik anahtar değer uzunluğunun yeterli güvenliği sağlayacak biçimde olmaması nedeniyle yeni sistem arayışlarına gidilmiştir ve 3G sistemleri geliştirilmiştir.
3G sistemleri ile tüm bu sıkıntılar giderilmesi ile beraber hem veri şifreleme hem de kimlik doğrulama işlemlerinde daha güvenilir algoritmalar kullanılmış ve veri aktarım hızı arttırılmıştır. Gelecek yıllarda ise bunun üzerine IP üzerinden iletişim imkanı sağlanacak 4G sistemler ile daha da hızlı ve güveniliri iletişim olanağı sağlanacaktır.

Kaynaklar

[1] SAĞIROĞLU, S., MOHAMMMED, M., “Mobil Ortamlar Üzerine Yapılan Saldırılar Üzerinde Bir Ġnceleme”, TUBAV, Yıl: 2009, Cilt:2, Sayı:2, Sayfa:138-147.
[2] ÖZKOÇ, E., “Akıllı Kart Tabanlı Uzaktan Kimlik Doğrulama Sistemi Tasarımı”, Yüksek lisans Tezi, Gebze Ġleri teknoloji Enstitüsü, 2008.
[3] ALAZEIB, A., “An Ontology for Generic Wireless Authentication”, Thesis, Stuttgart, 07.October.2005.
[4] VEDDER , K., “Smart Cards”, Chairman ETSI TC SCP, Group Senior VP, Giesecke & Devrient, 2nd ETSI Security Workshop, 1997.
[5] REDL, S. M., WEBER, M. K., OLIPHANT, M. W.,” GSM and Personel Communaticon Handbook”, Artech House, Boston LONDON,1998.
[6] Martin SAUTER,” Communications Systems for the Mobile Information Society”, Nortel Networks, Germany,2006.
[7] ERGÜLER, Ġ., KARAHĠSAR, A., ANARIM, E., “GSM ĠletiÇim Sistemindeki Zayıflıklar ve Olasıl Saldırılar”, SAVTEK 2004, 24-25 Haziran, ODTU, Ankara.
[8] BUDAK, B., “ Güvenli Özet Algoritması”, Yükseklisans tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Temmuz 2010.
[9] MEYER, U., WETZEL, S., “On The Impact of GSM Encryption and Man-In-The-Middle Attacks On The Security of Interoperating GSM/UMTS Networks”, 2004 IEEE.
[10] ROSE, G., “Authentication and Security in Mobile Phones”, QUALCOMM Australia.
[11] BALANI, A., “Authentication and Encryption in CDMA Systems”, LG Soft India Private Limited Mumbai-India.
[12] BOCAN, V., CRETU, V., “Threats and Countermeasures in GSM Networks”, Journal of Networks, Vol. 1, No. 6, 2006.
[13] CHEN, J. C., ZHANG, T., “IP-Based Next-Generation Wireless Networks, Chapter 5: Security”, 2004.
[14] “Advanced Encryption Standard (AES)”, Federal Information Processing Standards Publication 197, November 26, 2001
[15] NYBERG, K., “Cryptographic Algorithms for UMTS”, European Congress on Computational Methods in Applied Sciences and Engineering, ECCOMAS 2004
[16] KQIEN, G., TELENOR R&D and AGDER UNIVERSITY COLLEGE, “An Introduction to Access Security in UMTS”, IEEE Wireless Communications, 2004.
[17] ROSE, G., KQIEN, G., TELENOR R&D and AGDER UNIVERSITY COLLEGE, “Access Security in CDMA2000, Including a Comparison with UMTS Access Security”, IEEE Wireless Communications, 2004.
[18] ALTUN, M., “Yeni Nesil Kablosuz Mobil Ağlar Ġçin Bir Sanal USIM Uygulaması”, Yükseklisans Tezi, Ege Üniversitesi Fen Bilimleri E nstitüsü, 2009.

TEŞEKKÜRLER...