**Gebze Technical University**

Computer Engineering

Cryptography and Computer Security

BİL 470

MIDTERM

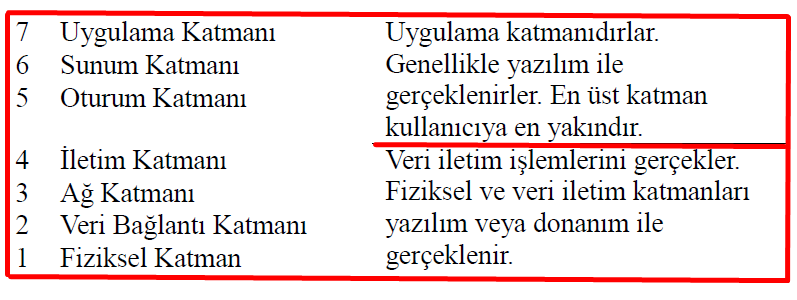
Değer MANDAL

161044096

**ARAŞTIRMA:**

OSI modeli, aynı veya farklı bilgisayar üreticileri tarafından üretilen cihazların arasındaki haberleşmeyi standartlaştırmak için önerilmiştir. OSI farklı donanım ve ağ uygulamalarına göre değişiklik göstermez, belli bir ürün ailesine özgü bir standart değildir. Sadece her katmanın görevlerini ayrıntısıyla açıklar. Bunu bir gemi planına benzetebiliriz….

OSI modelinde, iki bilgisayar arasındaki iletişim problemini çözmek için 7 katman bulunmaktadır. OSI sadece her katmanın görevlerini tüm detaylarıyla tanımlar.



**Uygulama Katmanı (katman 7):**

• Uygulama katmanı, kullanıcıların gerçekte bilgisayarla iletişime geçtiği yerdir.

• Diğer katmanlarda olduğu gibi bir üst katmanı olmadığı için o katmana servis sağlaması gibi bir durum söz konusu değildir.

• Sisteminizden ağ bileşenlerinin (ağ kartı vs.) tümünü kaldırsanız dahi yerel HTML dökümanlarına göz atmak için bir Chrome veya Firefox gibi bir tarayıcıyı kullanabilirsiniz. Ancak HTTP ile bir web sayfasına erişmek istediğinizde tarayıcınız uygulama katmanı ile iletişime geçerek bu isteğinize cevap verecektir.

• OSI modelinde en üst katmandan yola çıkan ham veri, her katmanda o katmanla ilgili bazı ek bilgiler eklenerek bir alt katmana aktarılır.

FTP (File Transfer Protocol)

SNMPvX (Simple Network Management Protocol, versions 1-3)

POP3 (Post Office Protocol, version 3)

SMTP (Simple Mail Transfer Protocol)

Telnet

DHCP (Dynamic Host Configuration Protocol)

HTTP (HyperText Transfer Protocol)

Others…

**Pretty Good Privacy (PGP) =>**

E-postaların ve diğer iletişim biçimlerinin şifrelenmesi, herkesin güvenliği, gizliliği ve mahremiyeti için hayati önem taşır. Burası PGP'nin devreye girdiği yerdir ve bu nedenle bugün PGP bu kadar popülerdir. Aslında, şu anda PGP, kişisel iletişimde popüler şifreleme ve dijital imza şemalarından biridir. Phil Zimmermann tarafından geliştirilen Pretty Good Privacy (PGP), açık anahtarlı bir şifreleme sistemidir. Açık anahtar şifrelemede, bir anahtar gizli tutulur ve diğer anahtar kamuya açık hale getirilir. Alıcı tarafla güvenli iletişim (gizli bir anahtarla), gönderilecek mesajın alıcının açık anahtarı kullanılarak şifrelenmesiyle sağlanır. Bu mesajın şifresi yalnızca alıcının gizli anahtarı kullanılarak çözülebilir. PGP, kullanıcıları arasında bir güven çemberi oluşturarak çalışır. Güven çemberinde, kullanıcılar iki ile başlayarak, her kullanıcı tarafından tutulan ortak anahtar / isim çiftlerinden oluşan bir anahtarlık oluştururlar. Bu "güven kulübüne" katılmak, güvenmek ve birinin anahtarlığındaki anahtarları kullanmak anlamına gelir. Standart PKI altyapısının aksine, bu güven çemberi, bir davetsiz misafir tarafından delinebilecek yerleşik bir zayıflığa sahiptir. Bununla birlikte, PGP mesajları imzalamak için kullanılabildiğinden, dijital imzasının varlığı bir belge veya dosyanın gerçekliğini doğrulamak için kullanılır. Bu, İnternet'ten yeni indirilen bir e-posta mesajının veya dosyanın hem güvenli hem de değiştirilmemiş olmasını sağlamada uzun bir yol kat eder. PGP, öngörülebilir gelecekte kırılması imkansız olan sert şifreleme olarak kabul edilir. Gücü, kapsamlı bir kamu incelemesinden sonra hayatta kalan ve birçokları tarafından zaten güvenli olarak kabul edilen algoritmalara dayanmaktadır. Bu algoritmalar arasında, PGP'nin şifreleme için kullandığı RSA, DSS ve açık anahtar şifrelemesi için Diffie-Hellman;

Geleneksel şifreleme için CAST-128, IDEA ve 3DES;

ve hashing için SHA-1. PGP'nin fiili işleyişi beş hizmete dayanmaktadır:

kimlik doğrulama, gizlilik, sıkıştırma, e-posta uyumluluğu ve bölümleme (authentication, confidentiality, compression, e-mail compatibility, and segmentation).

*Kimlik Doğrulama*

PGP, bir dijital imza şeması aracılığıyla kimlik doğrulama sağlar. Karma kod (MAC), etkili bir dijital imza sağlamak için SHA-1 ve RSA'nın bir kombinasyonu kullanılarak oluşturulur. Ayrıca, DSS ve SHA-1 kullanarak alternatif bir imza oluşturabilir. İmzalar daha sonra gönderilmeden önce mesaja veya dosyaya eklenir. PGP, ek olarak, bağlanmamış dijital imzaları da destekler. Bu durumda imza mesajdan ayrı olarak gönderilebilir.

*Gizlilik*

PGP, iletileri iletimden önce şifreleyerek gizlilik sağlar. PGP, CAST-128, IDEA ve 3DES gibi geleneksel şifreleme şemalarını kullanarak iletimi ve depolanması için mesajları şifreler. Her durumda, 64 bitlik bir şifre geri besleme modu kullanılır. Tüm şifreleme durumlarında olduğu gibi, her zaman bir anahtar dağıtımı sorunu vardır; bu nedenle PGP bir kez geleneksel bir anahtar kullanır. Bu, gönderilecek her mesaj için, gönderenin mesaj için yepyeni bir 128 bitlik oturum anahtarı oluşturması anlamına gelir. Oturum anahtarı, alıcının genel anahtarı kullanılarak RSA veya Diffie-Hallman ile şifrelenir; mesaj, oturum anahtarıyla birlikte CAST-128 veya IDEA veya 3DES kullanılarak şifrelenir. Kombo alıcıya iletilir. Alındıktan sonra alıcı, mesajı kurtarmak için kullanılan oturum anahtarını şifrelemek ve kurtarmak için kendi özel anahtarıyla RSA'yı kullanır.

*Sıkıştırma*

PGP, imzayı uyguladıktan sonra ve şifrelemeden önce mesajı sıkıştırır. Fikir, yerden tasarruf etmektir.

*E-posta Uyumluluğu*

Yukarıda gördüğümüz gibi, PGP bir mesajı imza ile birlikte (ayrı olarak gönderilmemişse) şifreleyerek rastgele 8 bitlik sekizli akışına neden olur. Ancak birçok e-posta sistemi yalnızca ASCII metninden oluşan blokların kullanımına izin verdiğinden, PGP bunu, ham 8-bit ikili akışları bir radix-64 dönüştürme şeması kullanarak yazdırılabilir ASCII karakter akışlarına dönüştürerek gerçekleştirir. Alındığında, blok radix-64 formatından ikiliye geri dönüştürülür. Mesaj şifrelenmişse, bir oturum anahtarı kurtarılır ve mesajın şifresini çözmek için kullanılır. Sonuç daha sonra açılır. İmza varsa, iletilen karma kodu kurtararak ve kabul etmeden önce alıcının hesaplanan karma değeri ile karşılaştırarak kurtarılması gerekir.

*Segmentation*

E-posta boyutu kısıtlamalarına uymak için PGP, çok uzun e-posta mesajlarını otomatik olarak bölümlere ayırır. Bununla birlikte, bölümleme, mesaj üzerinde tüm temizlik yapıldıktan sonra, iletilmeden hemen önce yapılır. Bu nedenle, oturum anahtarı ve imza, iletilen ilk bölümün başında yalnızca bir kez görünür. Alındığında, alan PGP tüm e-posta başlıklarını çıkarır ve orijinal postayı yeniden birleştirir. PGP’nin popülaritesi ve kullanımı iki nedenden dolayı şimdiye kadar beklenenden daha az çıktı: Birincisi, Zimmermann’ın Network Associates’e sattıktan sonra geliştirmesi ve ticari dağıtımı, daha sonra başka bir şirkete satması iyi sonuç vermedi; ikincisi, açık kaynak kuzeni OpenPGP, kullanım kolaylığı sorunu da dahil olmak üzere piyasa sorunları ile karşılaştı. Hem OpenPGP hem de ticari PGP'nin kullanımı zordur çünkü birçok e-posta istemcisinde yerleşik değildir. Bu, e-postalarını PGP kullanarak şifrelemek isteyen herhangi iki iletişim kuran kullanıcının PGP'yi manuel olarak indirmesi ve yüklemesi gerektiği anlamına gelir; bu, birçok kullanıcı için bir zorluk ve bir rahatsızlıktır.

**Secure/Multipurpose Internet Mail Extension (S/MIME) =>**

Çok Amaçlı İnternet Posta Uzantılarının (MIME) protokollerini dijital imzalar ve şifreleme ekleyerek genişletir. S / MIME'yi anlamak için önce kısa bir inceleme yapalım ve MIME'ye bakalım. MIME, resimler, ses ve video dahil olmak üzere multimedya verilerinin aktarımını açıklayan iletişim protokollerinin teknik bir özelliğidir. MIME protokol mesajları RFC 1521'de açıklanmaktadır; MIME ile daha fazla ilgilenen bir okuyucunun RFC 1521'e başvurması gerekir. Dosyalar gibi Web içerikleri, kendileri diğer hiperlinklere bağlanan hiper bağlantılardan oluştuğundan, herhangi bir e-posta bu tür bir ara bağlantıyı açıklamalıdır. Bir MIME sunucusu, bir istemci bir Web belgesi istediğinde bunu yapar. Web sunucusu istenen dosyayı istemcinin tarayıcısına gönderdiğinde, belgeye bir MIME başlığı ekler ve bunu iletir. Bu, bu nedenle, bu tür İnternet e-posta mesajlarının iki bölümden oluştuğu anlamına gelir: başlık ve gövde (the header and the body).

Başlık içinde, iki tür bilgi bulunur: MIME türü ve alt tür. MIME türü, görüntü, metin, ses, uygulama ve diğerleri gibi iletilen içerik türünün genel dosya türünü açıklar. Alt tür, jpeg veya gif, tiff vb. Gibi belirli dosya türünü taşır. MIME başlığının yapısı hakkında daha fazla bilgi için lütfen RFC 822'ye bakın. Gövde yapılandırılmamış olabilir veya bir e-posta mesajının gövdesinin nasıl yapılandırıldığını tanımlayan MIME biçiminde olabilir. Burada dikkate değer olan, MIME'nin herhangi bir güvenlik hizmeti sağlamamasıdır. Daha sonra eksik olan güvenlik hizmetlerini eklemek için S / MIME geliştirildi. İki kriptografik öğe ekler: şifreleme ve dijital imzalar.

*Şifreleme*

S / MIME, mesajla iletilmek üzere oturum anahtarlarını şifrelemek için üç genel anahtar algoritmasını destekler. Bunlar arasında tercih edilen algoritma olarak Diffie-Hallman, hem imza hem de oturum anahtarları için RSA ve Üçlü DES bulunur.

*Dijital İmzalar*

Dijital imza oluşturmak için S / MIME, mesaj özeti oluşturmak için 160 bitlik SHA-1 veya MD5'in bir karma işlevini kullanır. Mesaj özetlerini dijital bir imza oluşturmak üzere şifrelemek için DSS veya RSA kullanır.

**Güvenli HTTP (S-HTTP) =>**

Her S-HTTP dosyası ya şifrelenir, dijital bir sertifika içerir veya her ikisini birden içerir. S-HTTP tasarımı, bir HTTP istemcisi ile bir sunucu arasında öncelikle ticari işlemler olmak üzere güvenli iletişim sağlar. Bunu, politikayı mekanizmadan ayırırken gizlilik, kimlik doğrulama ve bütünlük sağlamak için çok çeşitli mekanizmalar aracılığıyla yapar. Sistem herhangi bir kriptografik sisteme, anahtar altyapısına veya kriptografik formata bağlı değildir. HTTP mesajları iki bölümden oluşur: mesajın başlığı ve gövdesi. Başlık, alıcılara (tarayıcı ve sunucu) iletinin gövdesinin nasıl işleneceği konusunda talimatlar içerir. Örneğin, mesaj gövdesi MIME, Metin veya HTML gibi türdeyse, bu mesajı uygun şekilde görüntülemek için talimatlar verilmelidir. Normal HTTP'de, bir istemcinin bir sunucudan bilgi (metin tabanlı mesaj) alması için, istemci tabanlı bir tarayıcı, sunucuya istenen kaynağı belirten bir istek mesajı göndermek için HTTP'yi kullanır. Sunucu yanıt olarak istemciye istenen mesajı içeren bir mesaj gönderir. Aktarım işlemi sırasında hem istemci tarayıcısı hem de sunucu, istenen bilgileri aktarmak için kullanacakları biçimleri görüşmek için HTTP başlığında bulunan bilgileri kullanır. Hem sunucu hem de istemci tarayıcısı, ihtiyaç duyulduğu sürece bağlantıyı koruyabilir: aksi takdirde, tarayıcı kapatmak için sunucuya mesaj gönderebilir. S-HTTP, istemci tarayıcısı ile sunucu arasındaki bu görüşmeyi, güvenlik konuları için görüşmeyi içerecek şekilde genişletir. Bu nedenle, S-HTTP, mesaj şifreleme, dijital sertifikalar ve mesaj gövdesinin şifresinin nasıl çözüleceğine ilişkin ek talimatlar içeren HTTP biçiminde kimlik doğrulama için ek başlıklar kullanır.

Esneklik sunmak için, istemci tarayıcısı ile sunucu arasındaki görüşme sırasında, kriptografik geliştirmelerin kullanılması için, istemci ve sunucunun dört kısımda anlaşması gerekir: özellik, değer, yön ve güç (property, value, direction, and strength). Agentlar ortak bir algoritma setini keşfedemezse, uygun eylemler alınır. Adam Shastack, görüşme line’ı olarak aşağıdaki örneği verir:

Bu, makine tarafından alınan mesajların anahtar değişimi için Kerberos 5 veya RSA şifrelemesini kullanması gerektiği anlamına gelir. (Recv-required) modları için seçenekler şunlardır: (recv || orig)-(optional || required || refused). Anahtar uzunluğu özelliklerinin değişken anahtar uzunluklu şifrelerde gerekli olduğu durumlarda, bu daha sonra özellikle şifre [length] veya şifre [L1-L2] olarak adlandırılır, burada anahtar uzunluğu uzunluktur veya L1-L2 durumunda, L1 ve L2 arasındadır.

S-HTTP görüşmelerindeki diğer başlıklar şunlar olabilir:

• S-HTTP-Privacy-Domains

• S-HTTP-Certificate-Types

• S-HTTP-Key-Exchange-Algorithms

• S-HTTP-Signature-Algorithms

• S-HTTP-Message-Digest-Algorithms

• S-HTTP-Symmetric-Content-Algorithms

• S-HTTP-Symmetric-Header-Algorithms

• S-HTTP-Privacy-Enhancements

• Your-Key-Pattern

**Taşıma katmanı (katman 4):**

• Veriyi, bir data akışına segmentler ve tekrar bir araya getirir.

• Bu katmanda bulunan servisler, üst-katman uygulamalarından gelen verileri böler, tekrar bir araya getirir ve onu aynı veri akışında birleştirir. Bu şekilde veri kaybı olması durumunda veriler daha küçük boyutlu olacağı için tekrar gönderilmesi daha kolay olur.

• Her bir parçaya bir sıra numarası vererek eksik parçaların alıcı tarafından belirlenip tamamlanmasını sağlar.

• TCP ve UDP protokolleri bu katmanda çalışır.

**Secure Socket Layer (SSL) =>**

SSL, iki büyük İnternet tarayıcısında kullanılan, yaygın olarak kullanılan genel amaçlı bir şifreleme sistemidir: Netscape ve Explorer. Platform veya işletim sisteminden bağımsız olarak bir istemci ile sunucu arasında şifreli bir uçtan uca veri yolu sağlamak üzere tasarlanmıştır. Güvenli ve kimliği doğrulanmış hizmetler, HTTP, LDAP veya POP3 uygulama katmanları aracılığıyla bir TCP bağlantısı için veri şifreleme, sunucu kimlik doğrulaması, ileti bütünlüğü ve istemci kimlik doğrulaması aracılığıyla sağlanır.

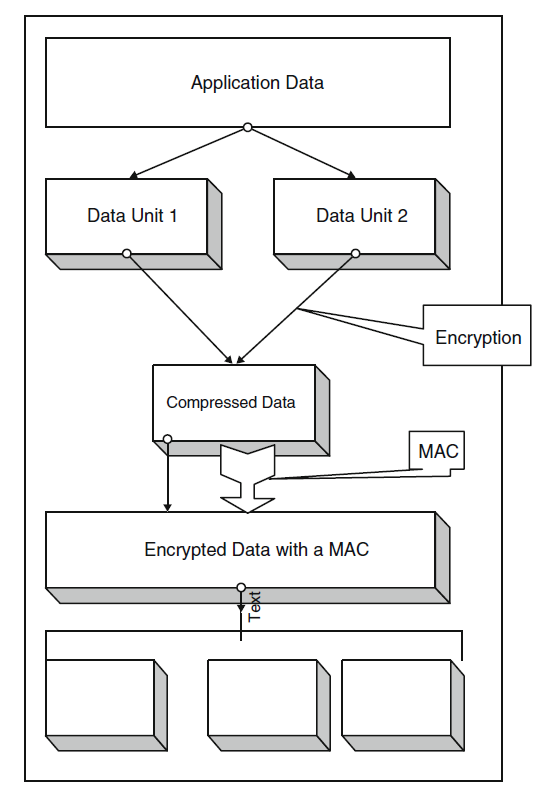
*SSL Hedefleri ve Mimarisi:*

SSL hedefleri, sunucular ve istemciler arasındaki veri yollarının güvenliğini sağlamak ve doğrulamaktı. Bu hedeflere, veri şifreleme, sunucu ve istemci kimlik doğrulaması ve mesaj bütünlüğünü içeren çeşitli hizmetler aracılığıyla ulaşılacaktı:

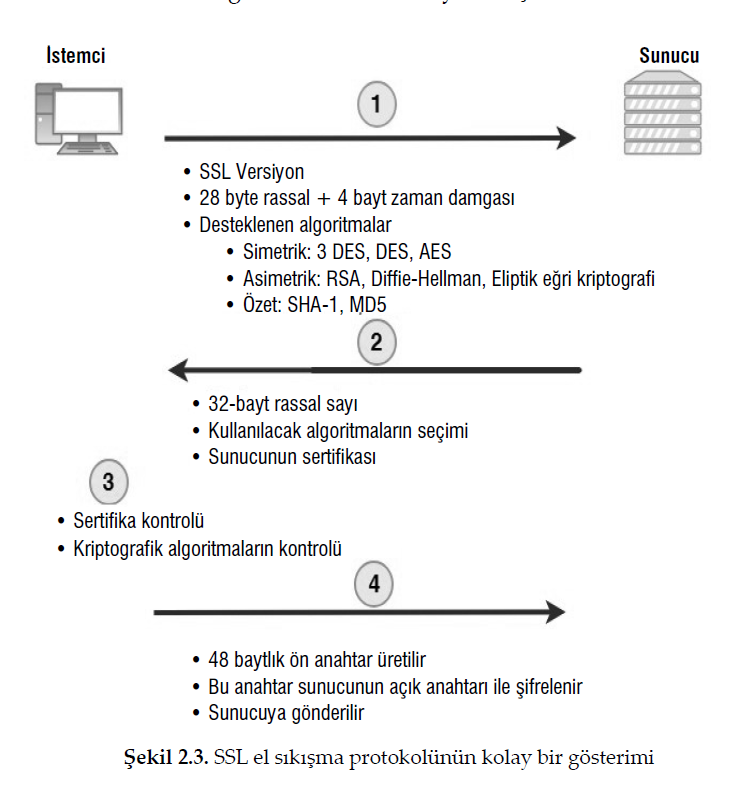
• Veri şifreleme: İstemci ve sunucu arasındaki aktarımdaki verileri müdahaleden korumak için ve yalnızca hedeflenen alıcı tarafından okunabilir.

• Sunucu ve istemci kimlik doğrulaması: SSL protokolü, birbirleriyle iletişim kuran tarafların kimliğini doğrulamak için standart açık anahtar şifrelemesini kullanır.

• Mesaj bütünlüğü: oturum anahtarlarının kullanılmasıyla elde edilir, böylece veriler kasıtlı veya kasıtsız olarak değiştirilemez. Bu hizmetler, İnternet TCP bağlantılarına güvenilir uçtan uca güvenli hizmetler sunar ve iki katmandan oluşan bir SSL mimarisine dayanır: üç protokolden, yani SSL Handshake protokolünden oluşan, uygulama katmanının hemen altındaki üst katman, SSL Change Cipher Spec protokolü ve SSL Alert protokolü. Bu protokollerin altında ikinci SSL katmanı olan SSL Record Protokolü katmanı, TCP katmanının hemen üzerindedir.



*SSL record protocol*

****

**Transport Layer Security (TLS) =>**

TLS, iki uygulama arasındaki aktarım katmanında güvenlik ve veri bütünlüğü sağlamakla görevlendirildi. TLS sürüm 1.0, gelişmiş bir SSL 3.0'dı. Bu nedenle TLS, SSL 3.0'ın halefidir. Sıklıkla, yeni standart, SSL / TLS olarak adlandırılır. Ancak o zamandan beri aşağıdaki ek özellikler eklendi:

• Interoperability: bir tarafın diğerinin TLS uygulama ayrıntılarını bilmesine gerek kalmadan TLS parametrelerini herhangi bir tarafça değiştirme yeteneği

• Expandability: gelecekteki genişletmeleri ve yeni protokollerin yerleştirilmesini planlamak için

**Ağ Katmanı (katman 3):**

• Cihaz adreslemelerini yönetir.

• Ağdaki cihazların lokasyonunu izler.

• Verinin taşınması için en iyi yolu belirler.

• Lokal olarak bağlı olmayan cihazlar arasındaki trafiği aktarmakla görevlidir.

• Bu katmanda harekete geçen datanın hedefe ulaşabilmesi için en iyi yol seçimi yapılır.

• Bu işleme Routing bu işlemi yerine getiren cihaza ise Router denir.

**Internet Protocol Security (IPsec) =>**

IPsec, IP tabanlı ağlar için doğal güvenlik eksikliğini gidermek üzere tasarlanmış bir kimlik doğrulama ve şifreleme protokolleri paketidir. IPsec, şimdiye kadar tartıştığımız diğer protokollerin aksine, RFC 2401 ve 2411 dahil olmak üzere bir dizi RFC'de açıklanan çok karmaşık bir protokoller kümesidir. Bunu görmeyen katman ve uygulama katmanı protokollerini taşımak için şeffaf olarak çalışır. İnternet Protokolünün yeni sürümü olan IP sürüm 6'da (IPv6) çalışmak üzere tasarlanmış olmasına rağmen, eski IPv4'te de başarıyla çalışmıştır. IPsec, ağ katmanında aşağıdaki hizmetleri sağlayarak koruma sağlamayı amaçlamaktadır:

• Access control: kaynağa yetkisiz erişimi önlemek için.

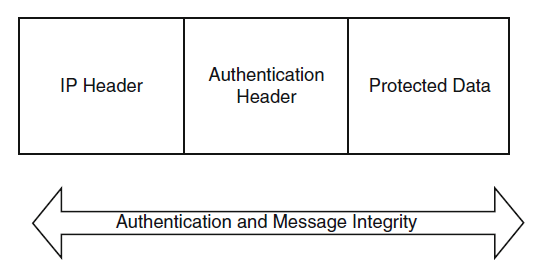
• Connectionless integrity: alınan trafiğin herhangi bir şekilde değiştirilmediğine dair bir güvence vermek için.

• Confidentiality: İnternet trafiğinin yetkisiz taraflarca incelenmemesini sağlamak için. Bu, tüm IP datagramlarının veri alanlarının, TCP, UDP, ICMP veya diğer datagram veri alanı segmentlerinin şifrelenmiş olmasını gerektirir.

• Authentication: özellikle kaynak kimlik doğrulaması, böylece bir hedef ana bilgisayar belirli bir IP kaynak adresine sahip bir IP datagramı aldığında, IP datagramının gerçekten de kaynak IP adresine sahip ana bilgisayar tarafından oluşturulduğundan emin olmak mümkündür. Bu sahte IP adreslerini önler.

• Replay protection: iki taraf arasında değiş tokuş edilen her paketin farklı olmasını garanti etmek için.

IPsec protokolü, protokol paketini iki ana protokole bölerek bu iki amaca ulaşır: Kimlik Doğrulama Başlığı (AH) protokolü ve Kapsülleme Güvenliği Yükü (ESP) protokolü. AH protokolü, kaynak kimlik doğrulaması ve veri bütünlüğü sağlar, ancak gizlilik sağlamaz. ESP protokolü, kimlik doğrulama, veri bütünlüğü ve gizlilik sağlar. Bir kaynaktan gelen herhangi bir datagram, AH veya ESP ile güvence altına alınmalıdır.

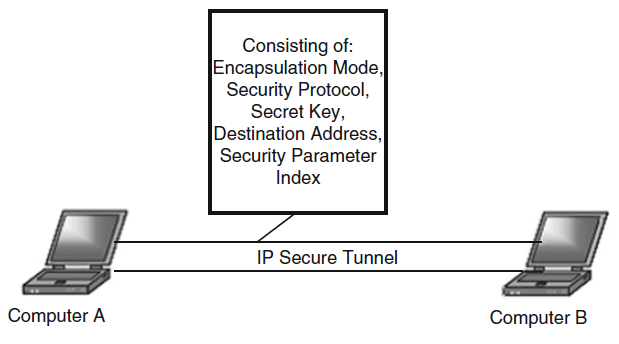


*Authentication Header (AH):*

AH protokolü, kaynak kimlik doğrulaması ve veri bütünlüğü sağlar, ancak gizlilik sağlamaz. Bu, ilk önce bir SA kurarak bir datagram göndermek isteyen bir kaynak tarafından yapılır, bu kaynak aracılığıyla datagramı gönderebilir. Bir kaynak datagram, artık standart bir IP datagramı olarak kapsüllenmiş olan veri alanını korumak için orijinal IP datagram verisi ile IP başlığı arasına yerleştirilmiş bir AH içerir. IP datagramının alınması üzerine, hedef ana bilgisayar AH'yi fark eder ve AH protokolünü kullanarak onu işler. Bununla birlikte, yönlendiriciler gibi ara ana bilgisayarlar, hedef IP adresi için her veri katarını incelemek ve ardından onu iletmek gibi olağan işlerini yaparlar.

*Encapsulating Security Payload (ESP):*

AH protokolünün aksine, ESP protokolü kaynak kimlik doğrulaması, veri bütünlüğü ve gizlilik sağlar. Bu, ESP'yi en yaygın kullanılan IPsec başlığı haline getirmiştir. AH'ye benzer şekilde ESP, hedefe güvenli datagramlar göndermek için kullandığı bir AS kuran kaynak ana bilgisayarla başlar. Datagramlar, tümü yeni bir IP datagramı içine kapsüllenmiş orijinal IP datagramlarını yeni bir başlık ve fragman alanlarıyla çevreleyerek ESP tarafından güvence altına alınır. Gizlilik DES\_CBC şifreleme ile sağlanır. Datagram üzerindeki ESP tanıtım alanının yanında ESP Kimlik Doğrulama Verileri alanı bulunur.

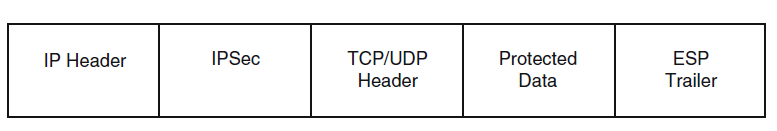


*Transport and Tunnel Modes :*

Güvenlik ilişkileri iki modda uygulanmaktadır: ulaşım ve tünel. Bu, IPsec'in iki modda çalıştığı anlamına gelir.

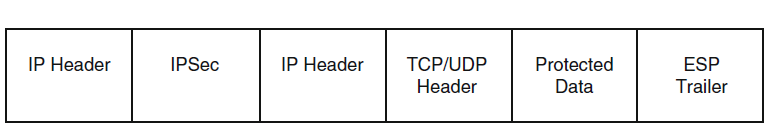
*Transport Mode*

Aktarım modu, hem IPv4 hem de IPv6'da iki ana bilgisayar arasındaki iletişimde daha yüksek katman protokollerine ana bilgisayardan ana bilgisayara koruma sağlar.



*Tunnel Mode*

Tünel modu, iki IPsec ağ geçidi arasında hem AH hem de ESP'de tüm IP datagramı için koruma sağlar. Bu, hem IPv4 hem de IPv6'da eklenen yeni IP başlığı nedeniyle mümkündür. İki ağ geçidi arasında, datagram güvenlidir ve orijinal IP adresi de güvenlidir. Ancak, ağ geçitlerinin ötesinde, datagram güvenli olmayabilir. Bu tür bir koruma, ilk IPsec ağ geçidi, IP adresi dahil olmak üzere veri katarını, alıcı IPsec ağ geçidinin yeni bir IP adresi ile yeni bir kalkan datagramına kapsüllediğinde oluşturulur. Alıcı ağ geçidinde, yeni veri katarının açılması ve orijinal datagrama geri getirilmesi. Orijinal IP adresini temel alan bu datagram, alıcı ağ geçidi tarafından daha fazla aktarılabilir, ancak bu noktadan itibaren korumasız hale gelir.



*Diğer IPsec Sorunları:*

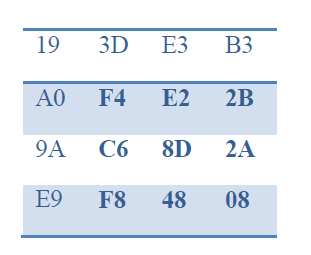
IPsec uyumlu herhangi bir sistem, mutlak minimum olarak tek DES, MD5 ve SHA-1'i desteklemelidir; bu, bağlantının her bir ucundaki iki IPsec uyumlu birimle temel düzeyde birlikte çalışmanın mümkün olmasını sağlar. IPsec, ağ ve aktarım katmanları arasında yer aldığından, uygulanması için en iyi yer esas olarak donanımdadır.

**Programlama Projesi:**

*AES ile Şifreleme ve Deşifreleme:*

***Şifreleme* =>**

**“***19 A0 9A E9 3D F4 C6 F8 E3 E2 8D 48 B3 2B 2A 08*” bu şekilde yani onaltılık tabanda ifade edilmiş 16 tane 8’er bitlik diziyi şifrelemek için, verinin durum matrisi haline getirilmesi gerekir. İlk dört eleman, matrisin ilk sütunundan başlanarak yerleştirilir. Oluşan matris aşağıdaki gibidir.



**DÖNGÜ YAPISI**

Durum matrisinin oluşumuyla algoritma yürürlüğe girer. Aes algoritmasının döngü kullanarak işlem yapması algoritmayı güçlü yapan bir özelliktir. Aes algoritması sırasıyla bayt değiştirme, satır kaydırma, sütun karıştırma ve tur anahtarı ile toplama işlemlerini gerçeklemesiyle şifrelenmiş veriyi elde eder ve tekrar bayt değiştirme adımına döner. Döngü sayısı anahtar uzunluğuna göre değişir. Sadece son döngüde sütun karıştırma işlemi yapılmaz, tur anahtarı ile toplama işlemi yapılır ve şifrelenmiş blok elde edilir Şifrelenmiş veriyi çözerken de bu alt işlemlerin tersi uygulanır.

Döngüler durum matrislerinde 4 dönüşüm uygular.

 SubBytes

 ShiftRows,

 MixColumns

 AddRoundKey

Her döngüde işleme farklı anahtar materyali sokulur. Bu farklı anahtarlar, başlangıçta belirlenen anahtardan anahtar oluşumu işlemleri sırasında üretilirler.

Şifre Çözme kısmında kullanılan ters dönüşümler:

 InvSubByte

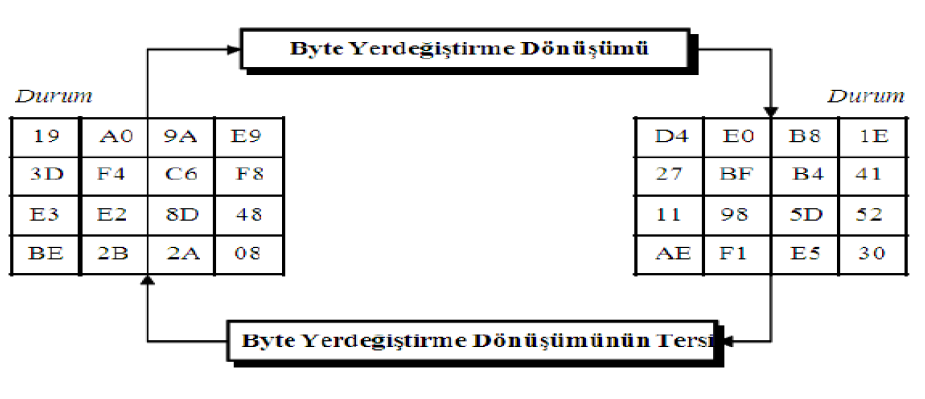
 InvShiftRows

 InvMixColumns

 AddRounKey (tersi kendisidir- XOR işlemi)

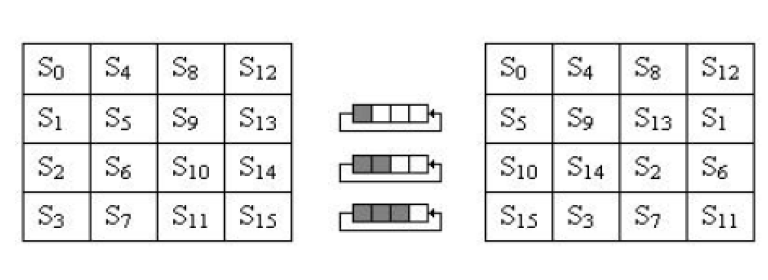
**BAYT DEĞİŞTİRME**

Döngünün ilk gerçekleştirilen işlemi ve algoritmanın tek doğrusal olmayan işlemidir. Bit dizilerinden elde edilen durum matrisi bu aşamada eleman değişikliğine uğrar. Değişiklik değerleri önceden hesaplanmış S-Kutusuna göre yapılır. S-Kutusu, durum matrisinin elemanları onaltılık tabana göre oluştuğu için 16x16 boyutunda bir matristir denebilir. 16 satırdan ve 16 sütunda oluşur. Satır ve sütun göstergeleri onaltılık tabanda “0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F” elemanları ile yapılır.



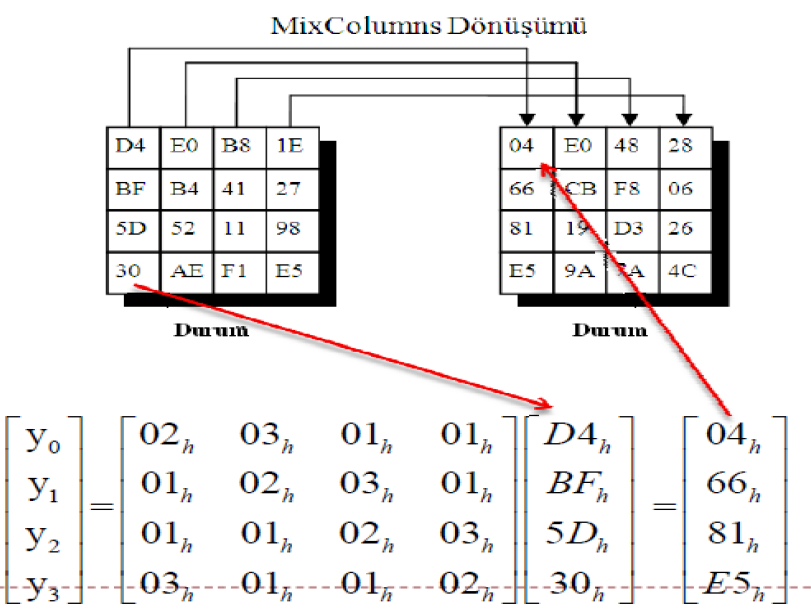
**SATIR KAYDIRMA**

Satır kaydırma işlemi yeni durum matrisi üzerinde yapılır. Bu işlemde matrisin ilk satırı aynı kalırken, ikinci satır 1 bayt, üçüncü satır 2 bayt, dördüncü satır ise 3 bayt sola ötelenir. Bunun sonunda ikinci satırda ilk bayt, üçüncü satırda ilk 2 bayt, dördüncü satırda ilk 3 bayt ve bu baytlar da satır sonuna eklenir ve tekrar yeni bir durum matrisi elde edilir.



**SÜTUN KARIŞTIRMA**

Sütunları karıştırma işlemi, satır kaydırmadan elde edilen durum matrisinin her bir sütununu birbirinden bağımsız şekilde a(x) = {03}x3+{01}x2+{01}x+{02} denklemiyle matris çarpımına tabi tutar. Eski sütunun yerine elde edilen sütun yazılır. Yine durum matrisimiz değişikliğe uğrar. Zaten dönüşüm işlemleri verinin değiştirilmesini hedefler.



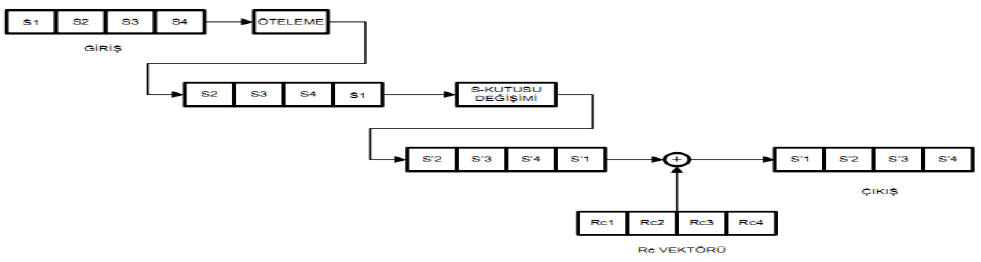
**DÖNGÜ ANAHTARINI EKLEME**

AES algoritmasında her döngünün sonunda anahtar materyali eklenir. Bu anahtar, başlangıçta anahtar üretim bloğu tarafından üretilen anahtar dizisidir. Tur anahtarının uzunluğu blok anahtarının uzunluğuna eşittir(=16bayt). Bu toplama işlemi sonlu alanlarda yapılan her bit için özel veya (XOR) işlemine karşılık düşer.

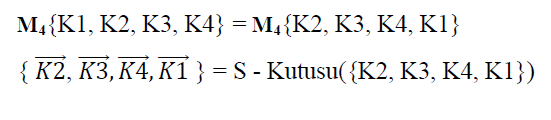
**ANAHTARIN ÜRETİLMESİ**

AES algoritmasında anahtar üretme işlemi şifreleme işlemi için önceden yapılması gerekir. Her döngüde farklı bir anahtarın girişi sağlanır. Dolayısıyla anahtar üretme işlemi de döngü sayısı kadar tur içermektedir ve bütün anahtarlar bir önceki turda hesaplanan anahtarların kullanılmasıyla elde edilir.

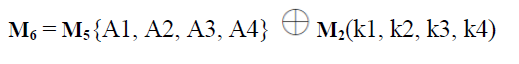
Anahtar üretim bloğu öncelikle anahtar uzunluğunu bit dizilerinin uzunluğuna göre uygun matrislere çevirir. Tur sayısına: N, matrisin boyutuna: 4xK dersek, daha sonra yapılacak işlemlerle genişlemiş matrisin boyutu 4x(K\*(N+1)) olur.



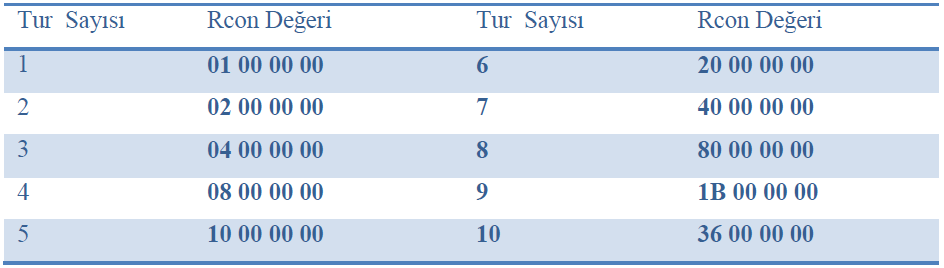
Öncelikle anahtar bitlerinden oluşan matristeki son sütunun(M4) ilk elemanının sona kaydırılmasıyla başka sütun oluşturulur ve S-Kutusundan bayt değiştirme işlemiyle sütun elemanları değiştirilir.



Bu sütun ile ilk sütun(M1) ve RCON vektör matrisinin 1. sütunun ex-or’lanması işlemi sonucu oluşan yeni sütun, matrise 5. sütun olarak eklenir.

Daha sonra 5. sütun ile 2.sütun ex-or’lanır ve bu yeni sütunda matrise 6. Sütun olarak eklenir. Matrisin her K’nın katı olan sütununa gelince başlangıçtaki ex-or’lanma işlemi yapılır.

Bu işlemler tur sayısı kadar devam eder ve matrisin genişlemiş hali elde edilir. Rcon vektörünün hangi sütunun ekleneceği hangi turda olduğuna göre değişiklik gösterir.



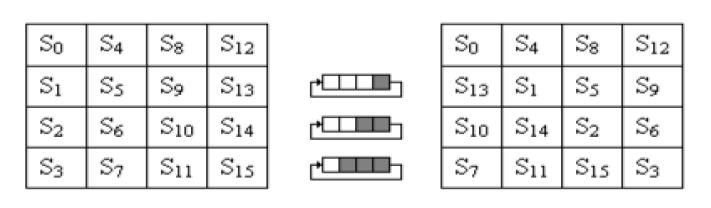
***Deşifreleme=>***

**ŞİFRE ÇÖZME İŞLEMİ**

Rijndael algoritmasında şifreli metni çözmek için uygulanan adımlar şifreleme işlemi için kullanılan adımların benzeridir ve fakat tersi şeklinde uygulanır. Şifrelemek için uygulan dönüşümler tersine çevrilir ve şifreleme sırasının tersinden başlanır. Şifre çözmede Ters sütun kaydırma, Ters bayt yer değiştirme, Ters sütun karıştırma ve Ters tur anahtarı ekleme dönüşümleri kullanılır.

**TERS SATIR KAYDIRMA**

Ters satır kaydırma işlemi satır kaydırma işleminin tersidir. Bu sefer durum matrisi sola değil sağa doğru kaydırılır. İkinci satır bir bayt, üçüncü satır iki bayt, dördüncü satır üç bayt sağa doğru kaydırılır.

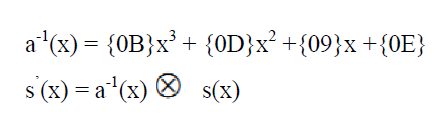
****

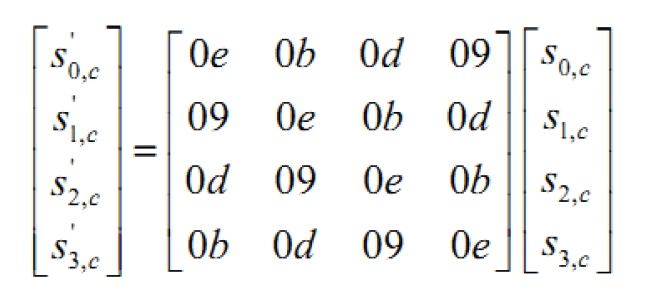
**TERS BAYT DEĞİŞTİRME**

Şifreleme işleminde bayt değiştirme için bir S-kutusundan yararlanılmıştı. Şifre çözme işleminde de yine aynı şekilde bir S-kutusu kullanılır. Bu S-Kutusu aynı S-Kutusu değildir ve şifreleme için kullanılan kutunu tersidir.

**TERS SÜTUN DEĞİŞTİRME**

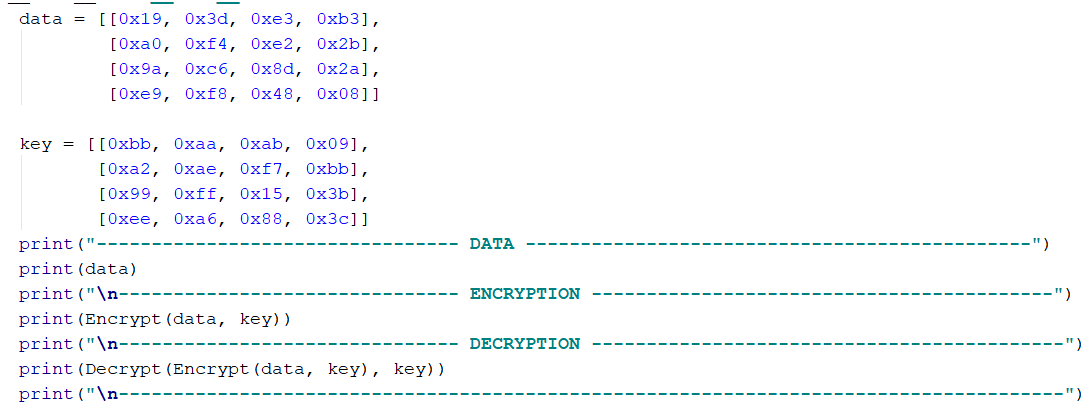
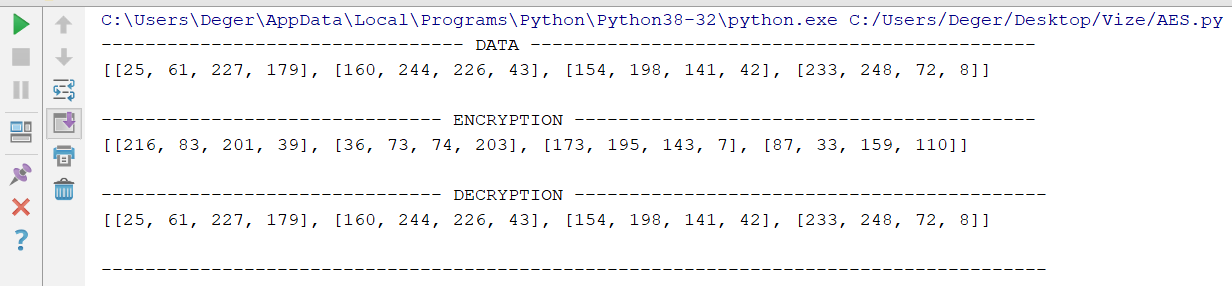
Ters sütun değiştirmede şifrelemedeki sütun değiştirme mantığı ile aynıdır. Yine her sütun bir polinom ile çarpılır ve elde edilen yeni sütun eskisinin yerine yazılır. Fakat buradaki matris çarpımında kullanılan polinom farklıdır. Durum matrisinin her sütunu sonlu alanında tanımlı dört terimli bir polinomlar olarak düşünülür.



ile ifade edildiğinde, bu işlem aşağıda bulunan şekildeki gibi matris çarpması halinde gösterilebilir.

**ÇÖZME İŞLEMİNDE DÖNGÜ ANAHTARINI EKLEME**

Döngü anahtarını eklemenin tersi yine kendisidir. AES algoritması şifreleme ve şifreyi çözmede aynı anahtarı kullanan simetrik yapıya sahiptir. Aynı anahtarı kullanmak demek anahtar üretme bloğunda yürütülen matris genişleme işlemlerinin girişine aynı matrisin geleceği demektir. Genişletilen matriste üretilen matrisler aynı olacağından şifre çözme içi yapılan döngünün sonunda eklenen anahtar materyalleri de aynısı olur.

**Örnek Main ve Elde Edilen Çıktı:**