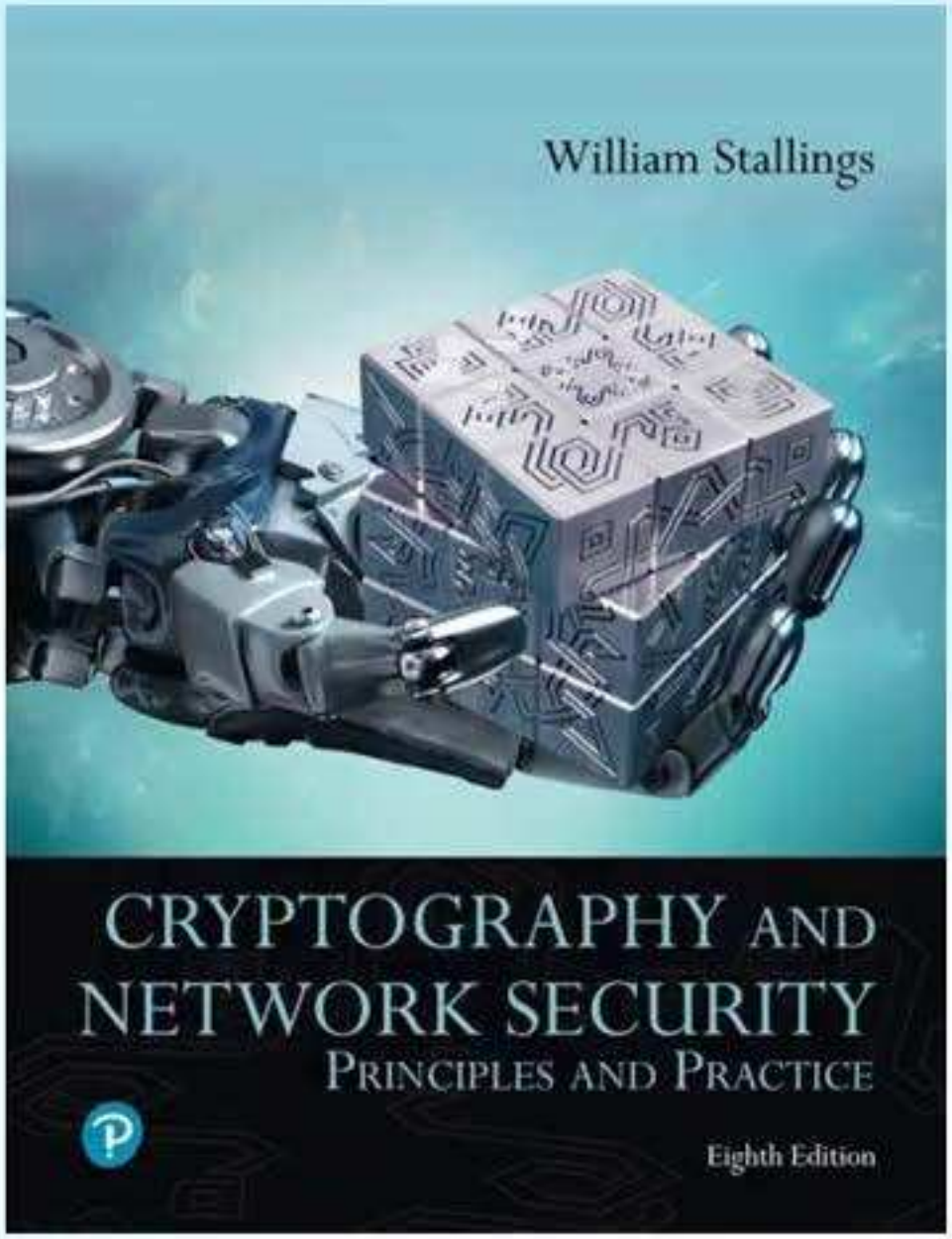
Kriptografi ve Ağ Güvenliği: İlkeler ve Uygulamalar

Sekizinci Baskı



Bölüm 1

Bilgi ve Ağ Güvenliği Kavramları

Pearson

Telif Hakkı © 2020 Pearson Education, Inc. Tüm Hakları Saklıdır.

Siber güvenlik (1/3)

Siber güvenlik, siber uzay ortamını, organizasyonu ve kullanıcıların varlıklarını korumak için kullanılabilecek

- araçların,
- politikaların,
- güvenlik kavramlarının,
- güvenlik önlemlerinin,
- yönergelerin,
- risk yönetimi yaklaşımlarının,
- eylemlerin,
- eğitimlerin,
- en iyi uygulamaların,
- güvencelerin ve teknolojilerin bir araya getirilmesidir.

Şirketlerin ve kullanıcıların varlıkları, bağlı bilgi işlem cihazlarını, personeli, altyapıyı, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber uzay ortamında iletilen ve / veya depolanan bilgilerin tamamını içerir.

Siber güvenlik (2/3)

Siber güvenlik, siber uzay ortamındaki ilgili güvenlik risklerine karşı kuruluşun ve kullanıcıların varlıklarının güvenlik özelliklerinin elde edilmesini ve sürdürülmesini sağlamaya çalışır.

Genel güvenlik hedefleri şunları içerir:

- kullanılabilirlik;
- veri gerçekliğini ve reddedilmemeyi içerebilecek bütünlük ve gizlilik

Siber güvenlik (3/3)

Bilgi güvenliği

- Bu terim, bilgilerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin korunmasını ifade eder. Ek olarak, özgünlük, hesap verebilirlik, reddetmeme ve güvenilirlik gibi diğer alanlarda dahil olabilir.

Ağ Güvenliği

- Bu terim, ağların ve hizmetlerinin yetkisiz değişiklik, imha veya ifşadan korunması ve ağın kritik işlevlerini doğru bir şekilde yerine getirdiğine ve zararlı yan etkileri olmadığına dair güvence sağlanması anlamına gelir.

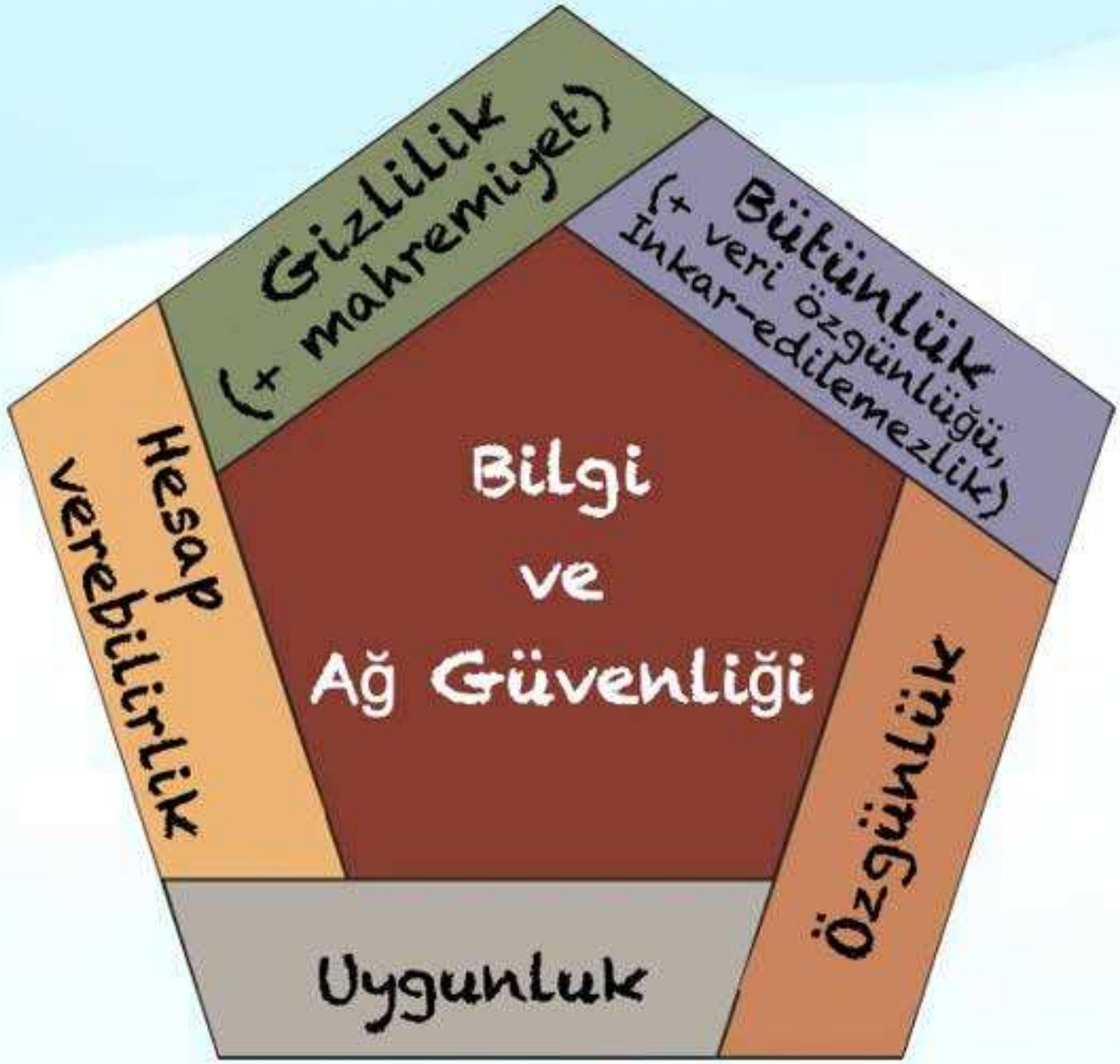
Güvenlik Hedefleri (1/2)

- Siber güvenlik tanımı, bilgi ve ağ güvenliğinin merkezinde yer alan üç temel hedef sunar:
  - Gizlilik: Bu terim iki ilgili kavramı kapsar:
    - Veri gizliliği: Özel veya gizli bilgilerin yetkisiz kişilere sunulmamasını veya ifşa edilmemesini sağlar
    - Gizlilik (mahremiyet): Bireylerin, kendileriyle ilgili hangi bilgilerin toplanabileceğini ve saklanabileceğini ve bu bilgilerin kim tarafından ve kimlere açıklanabileceğini kontrol etmelerini veya etkilemelerini sağlar.

Güvenlik Hedefleri (2/2)

- **Bütünlük:** Bu terim iki ilgili kavramı kapsar:
  - **Veri bütünlüğü:** Verilerin ve programların yalnızca belirli ve yetkili bir şekilde değiştirilmesini sağlar. Bu kavram aynı zamanda veri gerçekliğini de kapsar; bu, dijital bir nesnenin gerçekten iddia ettiği veya iddia ettiği şey olduğu anlamına gelir ve **reddetmeme**, yani bilgiyi gönderene teslimat kanıtı sağlandığı ve alıcıya gönderenin kimliğinin kanıtı sağlandığının güvencesidir, bu nedenle daha sonra bilgileri işlediğini inkar edemez.
  - **Sistem bütünlüğü:** Bir sistemin, amaçlanan işlevini, sistemin kasıtlı veya kasıtsız yetkisiz manipülasyonundan uzak, bozulmamış bir şekilde yerine getirmesini sağlar
- **Kullanılabilirlik (Uygunluk):** Sistemlerin derhal çalışmasını ve yetkili kullanıcılara hizmetin reddedilmemesini sağlar

Şekil 1.1 Temel Bilgi ve Ağ Güvenliği Hedefleri



Bilgisayar Güvenliği Zorlukları

- Güvenlik basit değil
- Güvenlik özelliklerine yönelik potansiyel saldırıların dikkate alınması gerekir
- Belirli hizmetleri sağlamak için kullanılan prosedürler genellikle sezgiseldir
- Çeşitli güvenlik mekanizmalarının nerede kullanılacağına karar vermek gerekir
- Sürekli izleme gerektirir
- Çok sık sonradan akla gelen bir şeydir
- Güvenlik mekanizmaları tipik olarak belirli bir algoritmadan veya protokolden daha fazlasını içerir.
- Güvenlik aslında bir fail ve tasarımcı arasında bir fikir savaşıdır.
- Güvenlik yatırımından çok az fayda bir güvenlik hatası meydana gelene kadar algılanmaktadır.
- Güçlü güvenlik genellikle verimli ve kullanıcı dostu çalışmaya engel olarak görülür.

OSI Güvenlik Mimarisi

- Güvenlik saldırısı
  - Bir kuruluşun sahip olduğu bilgilerin güvenliğini tehlikeye atan herhangi bir eylem
- Güvenlik mekanizması
  - Bir güvenlik saldırısını algılamak, önlemek veya bu saldırıdan kurtulmak için tasarlanmış bir işlem (veya böyle bir işlemi içeren bir cihaz)
- Güvenlik hizmeti
  - Veri işleme sistemlerinin güvenliğini ve bir kuruluşun bilgi aktarımını artıran bir işlem veya iletişim hizmeti
  - Güvenlik saldırılarına karşı koymayı amaçlamaktadır ve hizmeti sağlamak için bir veya daha fazla güvenlik mekanizmasından yararlanırlar

Tehditler ve Saldırılar

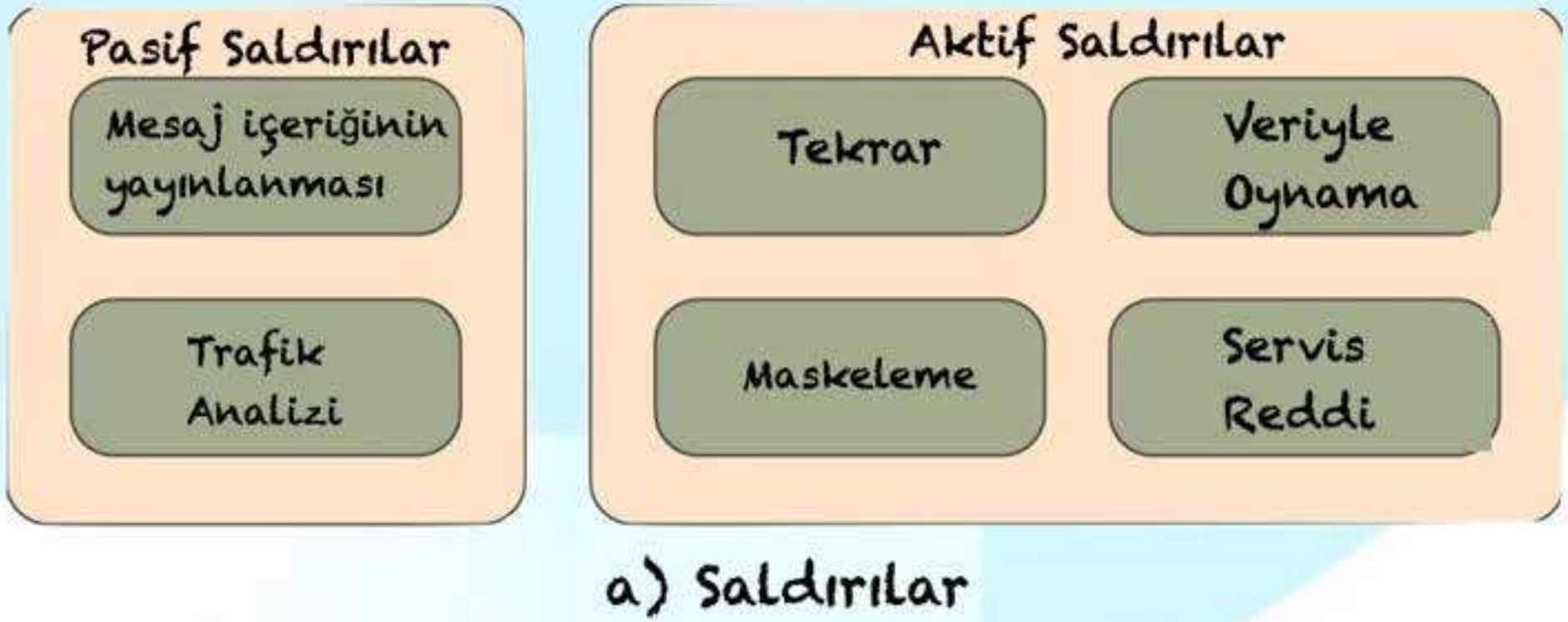
Tehdit

Güvenliği ihlal edebilecek ve zarar verebilecek bir durum, yetenek, eylem veya olay olduğunda ortaya çıkan güvenlik ihlali potansiyeli. Diğer bir deyişle, tehdit, bir güvenlik açığından yararlanabilecek olası bir tehlikedir.

Saldırı

Akıllı bir tehditten kaynaklanan sistem güvenliğine yönelik bir saldırı; yani, güvenlik hizmetlerinden kaçmak ve bir sistemin güvenlik politikasını ihlal etmek için kasıtlı bir girişim (özellikle bir yöntem veya teknik anlamında) olan akıllı bir eylem.

Şekil 1.2 Güvenlikte Temel Kavramlar (1/2)



a) Saldırılar

b) Servisler

Şekil 1.2 Güvenlikte Temel Kavramlar (2/2)

c) Mekanizmalar

Güvenlik Saldırıları

- Hem X.800 hem de RFC 4949'da kullanılan güvenlik saldırılarını sınıflandırmanın bir yolu, pasif saldırılar ve aktif saldırılar açısındandır.
- Pasif bir saldırı, sistemdeki bilgileri öğrenmeye veya kullanmaya çalışır, ancak sistem kaynaklarını etkilemez
- Aktif bir saldırı, sistem kaynaklarını değiştirmeye veya operasyonlarını etkilemeye çalışır

Pasif Saldırılar

- İletimlerin gizlice dinlenmesi veya izlenmesi niteliğinde olanlar
- Rakibin amacı, iletilen bilgileri elde etmektir.
- İki tür pasif saldırı vardır:
  - Mesaj içeriğinin yayınlanması
  - Trafik analizi

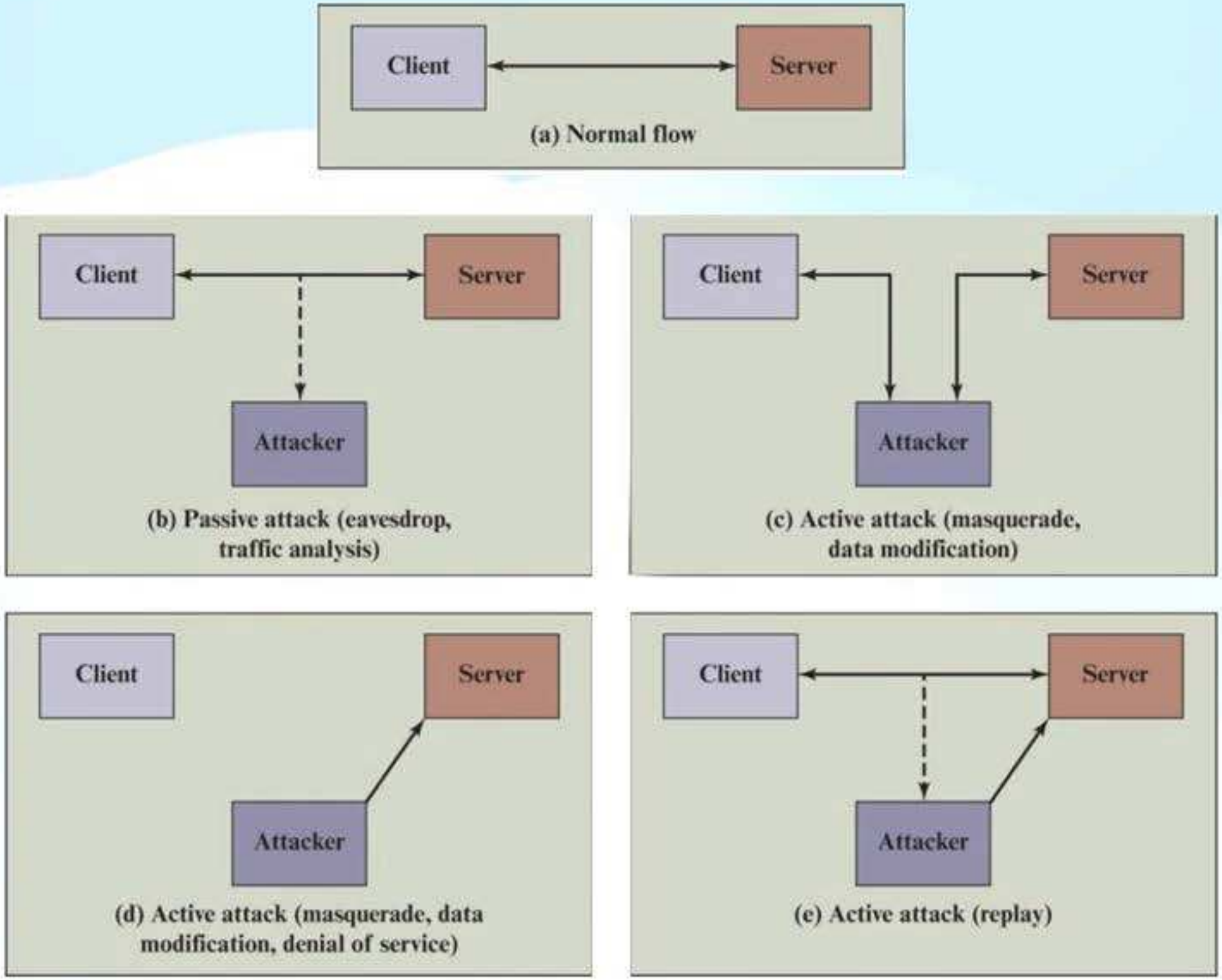
Aktif Saldırılar

- Veri akışında bazı değişiklikler veya yanlış akış oluşturulmasını dahil etme
- Çok çeşitli potansiyel fiziksel, yazılım ve ağ güvenlik açıkları nedeniyle önlenmesi zor
- Amaç, saldırıları tespit etmek ve bunların neden olduğu herhangi bir kesinti veya gecikmeden kurtarmaktır.

- Maskeleme
  - Bir varlık farklı bir varlıkmış gibi davrandığında gerçekleşir
  - Genellikle diğer aktif saldırı biçimlerinden birini içerir
- Tekrar
  - Bir veri biriminin pasif olarak yakalanmasını ve ardından yetkisiz bir etki yaratmak için yeniden iletilmesini içerir
- Veri Değişikliği
  - Meşru bir iletinin bazı bölümleri değiştirilir veya iletiler yetkisiz bir etki yaratacak şekilde geciktirilir veya yeniden sıralanır.
- Hizmet reddi

  İletişim tesislerinin normal kullanımını veya yönetimini önler veya engeller.

Şekil 1.3 Güvenlik Saldırıları



Kimlik Doğrulama (1/2)

- Bir iletişimin gerçek olduğundan emin olmakla ilgilidir.
  - Tek bir ileti söz konusu olduğunda, alıcıya iletinin geldiğini iddia ettiği kaynaktan geldiğini garanti eder.
  - Devam eden etkileşim durumunda, iki varlığın gerçek olduğunu ve bağlantıya üçüncü bir tarafın iki meşru taraftan biri olarak maskelenebileceği şekilde müdahale edilmemesini sağlar.

- X.800'de iki özel kimlik doğrulama hizmeti tanımlanmıştır:
  - Eş varlık kimlik doğrulaması
  - Veri kaynağı kimlik doğrulaması

Kimlik Doğrulama (2/2)

- Eş varlık kimlik doğrulaması
  - İlişkilendirmedeki bir eş varlığın kimliğinin doğrulanmasını sağlar. İki varlık, aynı protokolü farklı sistemlerde uygularlarsa eş olarak kabul edilir. Eş varlık kimlik doğrulaması, bir bağlantının kurulmasında veya zaman zaman veri aktarımı aşamasında kullanılmak üzere sağlanır. Bir varlığın maskeleme veya önceki bir bağlantının yetkisiz bir tekrarını gerçekleştirmediğine dair güven sağlamaya çalışır.
- Veri kaynağı kimlik doğrulaması
  - Bir veri biriminin kaynağının doğrulanmasını sağlar. Veri birimlerinin çoğaltılmasına veya değiştirilmesine karşı koruma sağlamaz. Bu hizmet türü, iletişim kuran varlıklar arasında sürekli etkileşimin olmadığı elektronik posta gibi uygulamaları destekler.

Erişim Kontrolü

- İletişim bağlantıları aracılığıyla ana bilgisayar sistemlerine ve uygulamalarına erişimi sınırlama ve kontrol etme yeteneği
- Bunu başarmak için, erişim kazanmaya çalışan her varlığın önce tanımlanması veya kimliğinin doğrulanması gerekir, böylece erişim hakları kişiye göre uyarlanabilir.

Veri Gizliliği

- İletilen verilerin pasif saldırılardan korunması
  - En geniş hizmet, belirli bir süre boyunca iki kullanıcı arasında iletilen tüm kullanıcı verilerini korur
  - Daha dar hizmet biçimleri, tek bir mesajın veya hatta bir mesajdaki belirli alanların korunmasını içerir
- Trafik akışının analizden korunması
  - Bu, saldırganın bir iletişim tesisindeki trafiğin kaynağını ve hedefini, sıklığını, uzunluğunu veya diğer özelliklerini gözlemleyememesini gerektirir.

Veri Bütünlüğü

- Bir mesaj akışına, tek bir iletiye veya bir iletideki seçili alanlara uygulanabilir
- Bir mesaj akışıyla ilgilenen bağlantı odaklı bütünlük hizmeti, iletilerin çoğaltma, ekleme, değiştirme, yeniden sıralama veya yeniden yürütme olmadan gönderildiği gibi alınmasını sağlar
- Daha geniş bir bağlama bakılmaksızın tek tek iletilerle ilgilenen bağlantısız bütünlük hizmeti, genellikle yalnızca ileti değişikliklerine karşı koruma sağlar

Reddetmeme

- Gönderenin veya alıcının iletilen bir mesajı reddetmesini önler
- Bir mesaj gönderildiğinde, alıcı, iddia edilen gönderenin mesajı gerçekten gönderdiğini kanıtlayabilir.
- Bir mesaj alındığında, gönderen iddia edilen alıcının mesajı gerçekten aldığını kanıtlayabilir.

Kullanılabilirlik Hizmeti

- Kullanılabilirliğini sağlamak için bir sistemi korur
- Bu hizmet, hizmet reddi saldırılarının neden olduğu güvenlik sorunlarını giderir
- Sistem kaynaklarının uygun şekilde yönetilmesine ve kontrolüne bağlıdır ve bu nedenle erişim kontrol hizmetine ve diğer güvenlik hizmetlerine bağlıdır.

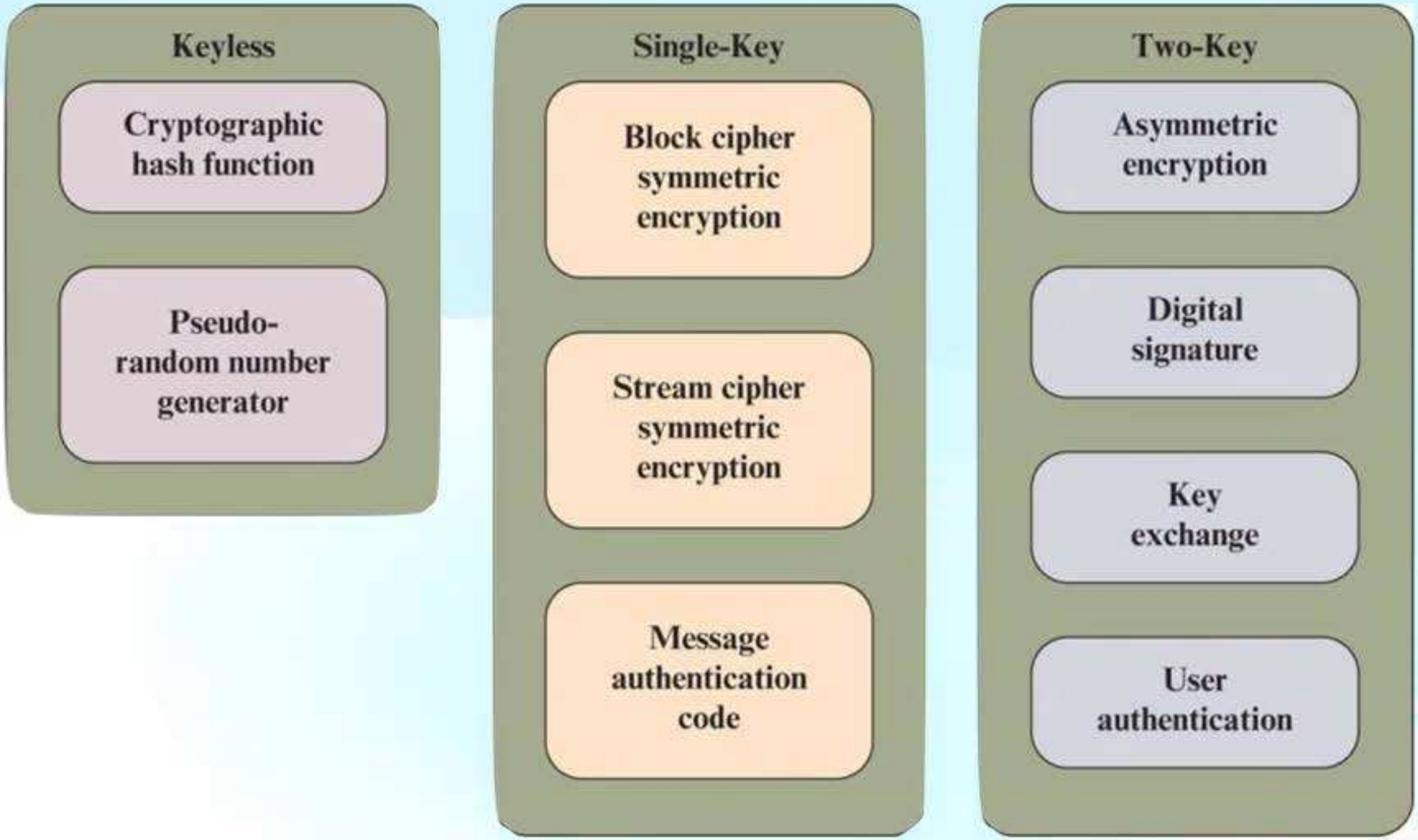
Güvenlik Mekanizmaları (1/2)

- Şifreleme algoritmaları: Geri dönüşümlü kriptografik mekanizmalar ile geri dönüşümsüz kriptografik mekanizmalar arasında ayrım yapabiliriz.
  - Geri dönüşümlü bir şifreleme mekanizması, verilerin şifrelenmesini ve daha sonra şifresinin çözülmesini sağlayan bir şifreleme algoritmasıdır.
  - Geri dönüşümsüz şifreleme mekanizmaları, dijital imza ve ileti kimlik doğrulama uygulamalarında kullanılan karma algoritmaları ve ileti kimlik doğrulama kodlarını içerir.
- Veri bütünlüğü: Bu kategori, bir veri biriminin veya veri birimi akışının bütünlüğünü sağlamak için kullanılan çeşitli mekanizmaları kapsar.
- Dijital imza: Veri biriminin alıcısının veri biriminin kaynağını ve bütünlüğünü kanıtlamasına ve sahteciliğe karşı korunmasına olanak tanıyan bir veri birimine eklenen veriler veya bu birimin kriptografik dönüşümü.

Güvenlik Mekanizmaları (2/2)

- **Kimlik doğrulama değişimi:** Bilgi alışverişi yoluyla bir işletmenin kimliğini sağlamayı amaçlayan bir mekanizma.
- **Trafik doldurma:** Trafik analizi girişimlerini boşa çıkarmak için veri akışındaki boşluklara bit eklenmesi.
- **Yönlendirme kontrolü:** Belirli veriler için belirli fiziksel veya mantıksal olarak güvenli yolların seçilmesini sağlar ve özellikle bir güvenlik ihlalinden şüphelenildiğinde yönlendirme değişikliklerine izin verir.
- **Noter onayı:** Veri alışverişinin belirli özelliklerini güvence altına almak için güvenilir bir üçüncü tarafın kullanılması
- **Erişim kontrolü:** Kaynaklara erişim haklarını zorlayan çeşitli mekanizmalar.

Şekil 1.4 Şifreleme Algoritmaları



Anahtarsız Algoritmalar

- Kriptografi için yararlı belirli özelliklere sahip deterministik fonksiyonlar
- Bir tür anahtarsız algoritma, şifreleme karma fonksiyonudur.
  - Bir hash fonksiyonu, değişken miktardaki bir metni, hash değeri, hash kodu veya özet olarak adlandırılan küçük, sabit uzunlukta bir değere dönüştürür.
  - Bir kriptografik hash fonksiyonu, onu ileti kimlik doğrulama kodu veya dijital imza gibi başka bir şifreleme algoritmasının parçası olarak yararlı kılan ek özelliklere sahip olan bir fonksiyondur.
- Bir sözde rasgele sayı üreteci, gerçekten rastgele bir dizi gibi görünen deterministik bir sayı veya bit dizisi üretir.

Tek Anahtarlı Algoritmalar (1/3)

- Tek anahtarlı şifreleme algoritmaları, gizli anahtarın kullanımına bağlıdır
- Tek bir anahtar kullanan şifreleme algoritmalarına simetrik şifreleme algoritmaları denir
  - Simetrik şifreleme ile, bir şifreleme algoritması korunacak bazı verileri ve gizli bir anahtarı girdi olarak alır ve bu veriler üzerinde anlaşılmaz bir dönüşüm üretir.
  - İlgili bir şifre çözme algoritması, dönüştürülen verileri ve aynı gizli anahtarı alır ve orijinal verileri kurtarır

Tek Anahtarlı Algoritmalar (2/3)

- Simetrik şifreleme aşağıdaki biçimleri alır:
  - Blok şifreleme
    - Bir blok şifresi, veriler üzerinde bir blok dizisi olarak çalışır
    - Çalışma modları olarak bilinen blok şifresinin çoğu sürümünde, dönüşüm yalnızca geçerli veri bloğuna ve gizli anahtara değil, aynı zamanda önceki blokların içeriğine de bağlıdır.
  - Akış şifreleme
    - Akış şifresi, veriler üzerinde bir bit dizisi olarak çalışır
    - Blok şifresinde olduğu gibi, dönüşüm gizli bir anahtara bağlıdır

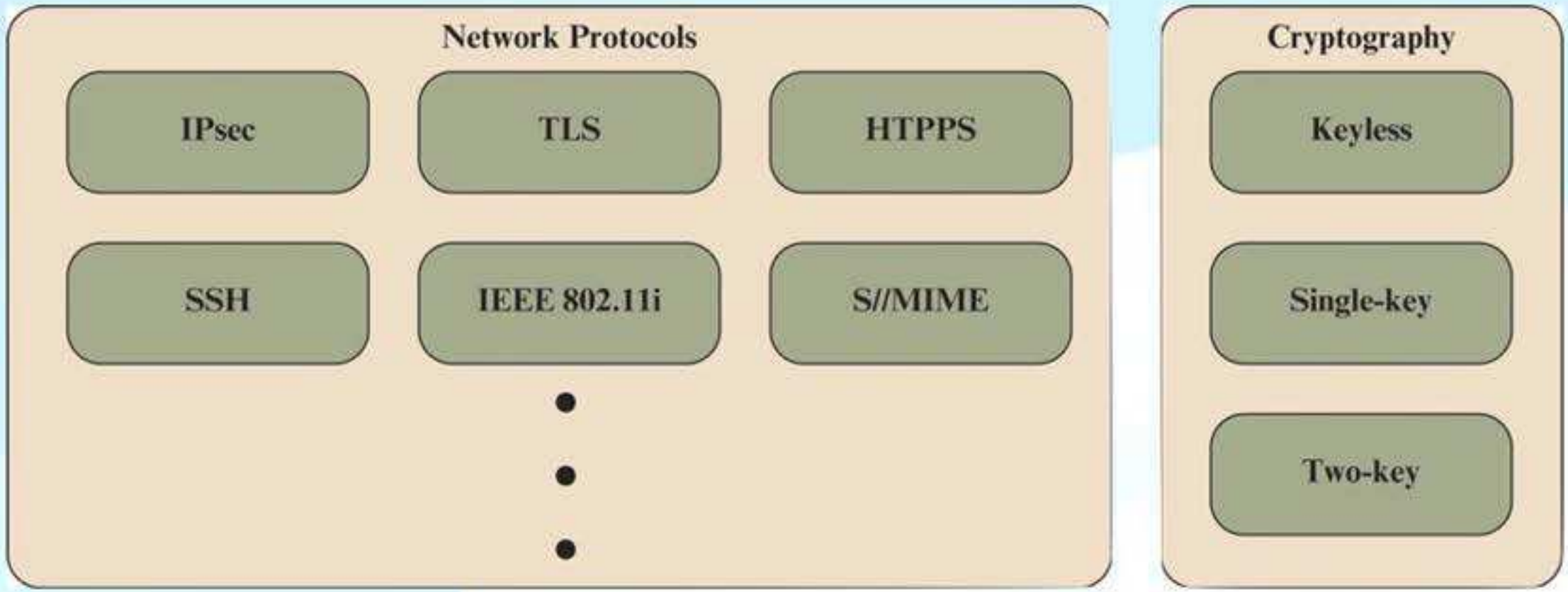
Tek Anahtarlı Algoritmalar (3/3)

- Tek anahtarlı şifreleme algoritmasının bir başka biçimi de mesaj kimlik doğrulama kodudur (MKD)
  - MKD kodu,
    - bir veri bloğu veya mesajla ilişkili bir veri öğesidir
    - gizli bir anahtarı ve tipik olarak iletinin şifreleme karma işlevini içeren bir şifreleme dönüşümü tarafından oluşturulur.
    - gizli anahtara sahip olan birinin iletinin bütünlüğünü doğrulayabilmesi için tasarlanmıştır
  - İletinin alıcısı ve MKD kodu, ileti üzerinde aynı hesaplamayı yapabilir; hesaplanan MKD kodu, iletiye eşlik eden MKD kodu ile eşleşiyorsa, bu iletinin değiştirilmediğine dair güvence sağlar

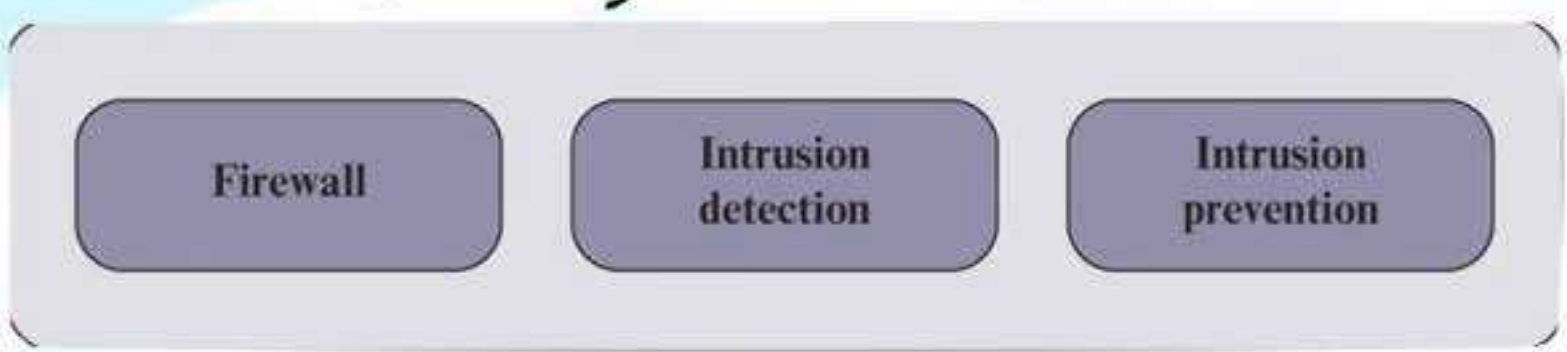
Asimetrik Algoritmalar

- Tek bir anahtar kullanan şifreleme algoritmalarına asimetrik şifreleme algoritmaları denir
- Dijital imza algoritması
  - Dijital imza, şifreleme algoritmasıyla hesaplanan ve verilerin herhangi bir alıcısının verilerin kaynağını ve bütünlüğünü doğrulamak için imzayı kullanabileceği şekilde bir veri nesnesiyle ilişkilendirilen bir değerdir.
- Anahtar değişimi
  - Simetrik bir anahtarı iki veya daha fazla tarafa güvenli bir şekilde dağıtma işlemi
- Kullanıcı kimlik doğrulaması
  - Bir uygulamaya veya hizmete erişmeye çalışan bir kullanıcının orijinal olduğunu ve benzer şekilde uygulamanın veya hizmetin orijinal olduğunu doğrulama işlemi

Şekil 1.5 Ağ Güvenliğinin Temel Unsurları



a) İletişim servisleri



b) Cihaz güvenliği

İletişim Güvenliği

- Hem pasif hem de aktif saldırılara karşı koruma önlemleri de dahil olmak üzere ağ üzerinden iletişimin korunmasıyla ilgilenir
- İletişim güvenliği öncelikle ağ protokolleri kullanılarak uygulanır
  - Ağ protokolü, bir ağdaki noktalar arasında veri iletimini ve alınmasını yöneten biçim ve prosedürlerden oluşur.
  - Bir protokol, tek tek veri birimlerinin yapısını ve veri aktarımını yöneten kontrol komutlarını tanımlar
- Ağ güvenliği ile ilgili olarak, bir güvenlik protokolü, varolan bir protokolün veya tek başına bir protokolün parçası olan bir geliştirme olabilir.

Cihaz Güvenliği (1/2)

- Ağ güvenliğinin diğer yönü, yönlendiriciler ve anahtarlar gibi ağ cihazlarının ve istemci sistemleri ve sunucular gibi ağa bağlı son sistemlerin korunmasıdır.
- Birincil güvenlik endişeleri, yetkisiz eylemler gerçekleştirmek, kötü amaçlı yazılım (kötü amaçlı yazılım) eklemek veya kullanılabilirliği azaltmak için sistem kaynaklarını boğmak için sisteme erişim sağlayan davetsiz misafirlerdir.

Cihaz Güvenliği (2/2)

- Üç tür cihaz güvenliği vardır:
  - Güvenlik duvarı
    - Belirli bir güvenlik ilkesine uygun olarak, bir ağ ile ağa bağlı cihaz arasındaki erişimi sınırlayan bir donanım ve/veya yazılım özelliği. Güvenlik duvarı, trafik içeriğine ve/veya trafik modeline dayalı bir dizi kurala bağlı olarak hem gelen hem de giden veri trafiğine izin veren veya reddeden bir filtre görevi görür
  - İzinsiz giriş algılama
    - Bir bilgisayar veya ağ içindeki çeşitli alanlardan bilgi toplamak ve analiz etmek, bulmak ve gerçek zamanlı veya neredeyse gerçek zamanlı uyarı vermek amacıyla sistem kaynaklarına yetkisiz bir şekilde erişmeye çalışan donanım veya yazılım ürünleri
  - İzinsiz giriş önleme
    - Müdahaleci etkinliği algılamak ve ideal olarak hedefine ulaşmadan önce etkinliği durdurmaya çalışmak için tasarlanmış donanım veya yazılım ürünleri

Güven Modeli (1/2)

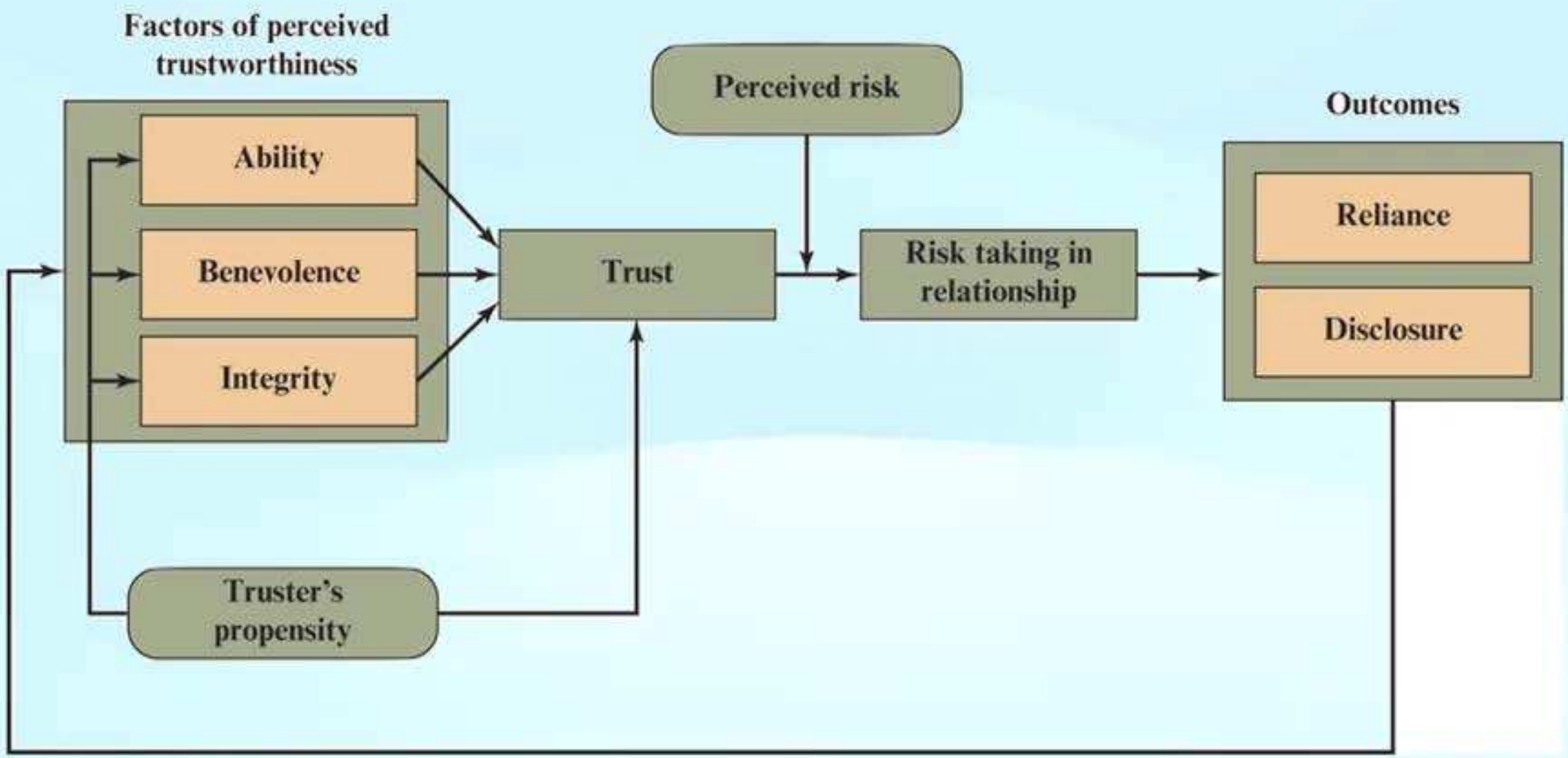
- En yaygın kabul gören ve en çok alıntı yapılan güven tanımlarından biri şudur:

  "Bir tarafın, diğer tarafın izleme veya kontrol etme kabiliyetine bakılmaksızın, diğerinin mütevelli için önemli olan belirli bir eylemi gerçekleştireceği beklentisine dayanarak başka bir tarafın eylemlerine karşı savunmasız olma istekliliği"

Güven Modeli (2/2)

- Bir güven modeliyle ilgili üç ilgili kavram vardır:
  - **Güvenilirlik:** Bir varlığın güveni hak etme derecesini yansıtan bir özelliği
  - **Güvenme eğilimi:** Geniş bir durum yelpazesinde başkalarına güvenmeye istekli olma eğilimi ve güven hedefleri. Bu, her bireyin, kişinin başkalarının sözlerine ve eylemlerine güvenme isteğini etkileyecek bir temel güven seviyesine sahip olduğunu göstermektedir.
  - **Risk:** Bir işletmenin potansiyel bir durum veya olay tarafından ne ölçüde tehdit edildiğinin bir ölçüsü ve tipik olarak
    - 1) durum veya olayın meydana gelmesi durumunda ortaya çıkacak olumsuz etkiler; ve
    - 2) oluşma olasılığı

Şekil 1.6 Güven Modeli



Güven Modeli ve Bilgi Güvenliği

- Güven, bir varlığın, parçası olduğu sistemin kullanıcısının güvenliğine zarar vermeyecek şekilde performans göstereceğine dair güvendir.
- Güven her zaman belirli işlevlerle veya davranış biçimleriyle sınırlıdır ve yalnızca bir güvenlik ilkesi bağlamında anlamlıdır.
- Genel olarak, ilk varlık ikinci varlığın tam olarak ilk varlığın beklediği gibi davranacağını varsaydığında bir varlığın ikinci bir varlığa güvendiği söylenir.
- Bu bağlamda, varlık terimi tek bir donanım bileşenini veya yazılım modülünü, marka ve model tarafından tanımlanan bir ekipman parçasını, bir siteyi veya konumu veya bir kuruluşu ifade edebilir.

Bir Bireyin Güvenilirliği (1/2)

- Kuruluşların, bilgi sistemlerinin hem iç kullanıcıları (çalışanlar, yerinde yükleniciler) hem de dış kullanıcıları (müşteriler, tedarikçiler) hakkında endişelenmeleri gerekir.
- Dahili kullanıcılarla ilgili olarak, bir kuruluş aşağıdaki iki alandaki politikalarla bireylere güven düzeyi geliştirir:
  - İnsan kaynakları güvenliği
    - Sağlam güvenlik uygulaması, bilgi güvenliği gereksinimlerinin istihdam yaşam döngüsünün her aşamasına dahil edilmesini, her bireyin indüksiyonu, devam eden yönetimi ve istihdamının sona erdirilmesi sırasında gerekli güvenlikle ilgili eylemleri belirterek dikte eder. İnsan kaynakları güvenliği ayrıca, yetenekli bireylere bilginin sahipliğini (koruma sorumluluğu dahil) atamayı ve anlayışlarının ve kabullerinin onayını almayı da içerir.

Bir Bireyin Güvenilirliği (2/2)

- Güvenlik farkındalığı ve eğitimi
  - Bu alan, güvenlik bilgilerinin IT personeli, IT güvenlik personeli ve yönetimin yanı sıra IT kullanıcıları ve diğer çalışanlar da dahil olmak üzere tüm çalışanlara yayılmasını ifade eder. Yüksek düzeyde güvenlik bilincine ve her bireyin rolü için uygun güvenlik eğitimine sahip bir işgücü, diğer güvenlik önlemlerinden veya denetimlerinden daha önemli olmasa da daha önemlidir.

Bir Kuruluşun Güvenilirliği

- Çoğu kuruluş, bilgi sistemi hizmetine ve dış kuruluşlar tarafından sağlanan bilgilere, ayrıca misyonları ve iş işlevlerini yerine getirmek için ortaklıklara güvenir (örnekler, bulut hizmeti sağlayıcıları ve kuruluşun tedarik zincirinin bir parçasını oluşturan şirketlerdir)
- Kuruluşa yönelik riski yönetmek için, bu dış kuruluşlarla güven ilişkileri kurması gerekir.
- NIST SP 800-39 (*Managing Information Security Risk*, March 2011), bu tür güven ilişkilerinin şunlar olabileceğini belirtir:
  - Resmi olarak, örneğin, sözleşmelerde, hizmet seviyesi sözleşmelerinde, iş bildirimlerinde, anlaşma/mutabakat muhtıralarında veya ara bağlantı güvenliği anlaşmalarında güvene ilişkin bilgilerin belgelenmesiyle oluşturulmuştur.
  - Ölçeklenebilir ve kuruluşlar arası veya kurum içi doğası gereği
  - İki ortak arasındaki basit (ikili) ilişkiler veya çok çeşitli ortaklar arasında daha karmaşık çok-çok ilişkiler ile temsil edilir

Bilgi Sistemlerinin Güvenilirliği

- SP 800-39 bilgi sistemleri için güvenilirliği şu şekilde tanımlar:
  "Bilgi sistemlerinin (sistemlerin inşa edildiği bilgi teknolojisi ürünleri dahil), sistemler tarafından işlenen, saklanan veya iletilen bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini tüm tehdit yelpazesinde korumasının beklenebileceği derece"
- Bilgi sistemlerinin güvenilirliğini etkileyen iki faktör şunlardır:
  - Güvenlik işlevselliği: Sistem içinde kullanılan güvenlik özellikleri/işlevleri. Bunlar şifreleme ve ağ güvenliği teknolojilerini içerir
  - Güvenlik güvencesi: Güvenlik işlevselliğinin uygulamasında etkili olduğuna dair güvenin gerekçeleri. Bu alan, güvenlik konularını denetleme ve sistem geliştirme yaşam döngüsüne dahil etme gibi güvenlik yönetimi tekniklerileyle ele alınmaktadır.

Güven İlişkileri Kurmak

- Doğrulanmış güven:
  - Güven, güvenen kuruluş tarafından güvenilen kuruluş veya varlık hakkında elde edilen kanıtlara dayanır. Bilgiler, bilgi güvenliği politikasını, güvenlik önlemlerini ve gözetim düzeyini içerebilir.
- Doğrudan tarihsel güven:
  - Bu tür bir güven, geçmişte bir kuruluş tarafından sergilenen güvenlikle ilgili sicile, özellikle de güven oluşturmak isteyen kuruluşla etkileşimlere dayanır.
- Aracılı güven:
  - Aracılı güven, iki tarafın karşılıklı olarak güvendiği üçüncü bir tarafın kullanılmasını içerir ve üçüncü taraf, ilk iki taraf arasında belirli bir güven düzeyinin güvencesini veya garantisini sağlar.
- Zorunlu güven:
  - Bir kuruluş, yetkili bir konumda üçüncü bir tarafça verilen belirli bir yetkiye dayanarak başka bir kuruluşla bir güven düzeyi oluşturur

Standartlar (1/2)

- National Institute of Standards and Technology:
  - NIST, ABD hükümetinin kullanımı ve ABD özel sektör inovasyonunun teşvik edilmesiyle ilgili ölçüm bilimi, standartları ve teknolojisi ile ilgilenen bir ABD federal ajansıdır. Ulusal kapsamına rağmen, NIST Federal Bilgi İşleme Standartları (FIPS) ve Özel Yayınlar (SP) dünya çapında bir etkiye sahiptir.
- İnternet Topluluğu:
  - ISOC, dünya çapında örgütsel ve bireysel üyeliğe sahip profesyonel bir üyelik topluluğudur. İnternetin geleceğiyle yüzleşen sorunların ele alınmasında liderlik sağlar ve İnternet Mühendisliği Görev Gücü (IETF) ve İnternet Mimarisi Kurulu (IAB) dahil olmak üzere İnternet altyapı standartlarından sorumlu grupların organizasyonudur. Bu kuruluşlar, hepsi Yorum İstekleri (R.F.C.) olarak yayınlanan İnternet standartlarını ve ilgili spesifikasyonları geliştirir.

Standartlar (2/2)

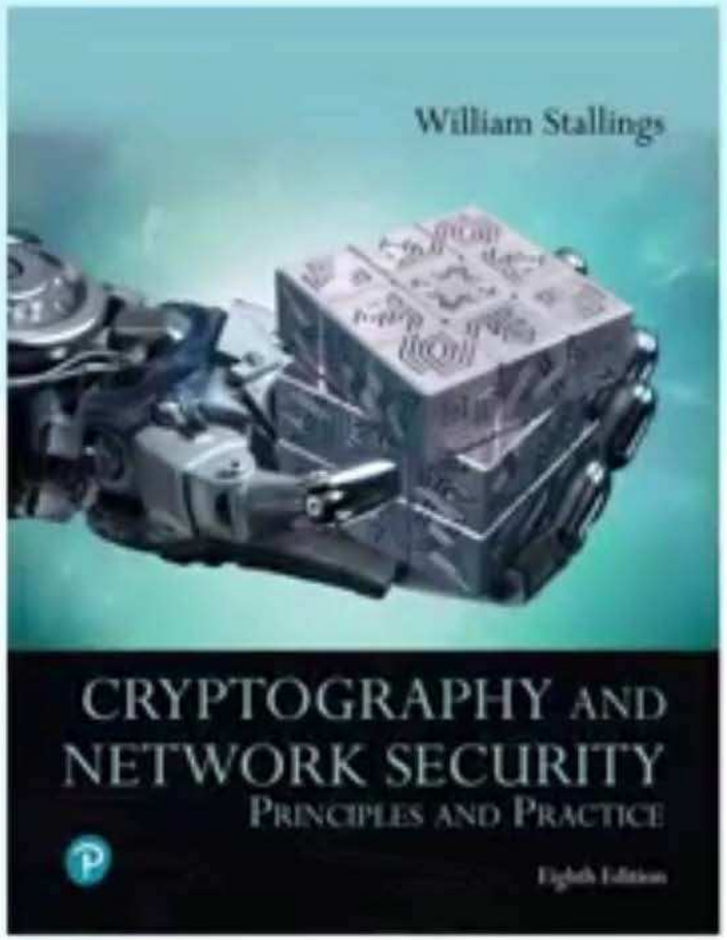
- ITU-T:
  - Uluslararası Telekomünikasyon Birliği (ITU), Birleşmiş Milletler Sistemi içinde hükümetlerin ve özel sektörün küresel telekom ağlarını ve hizmetlerini koordine ettiği uluslararası bir organizasyondur. ITU Telekomünikasyon Standardizasyon Birliği (ITU-T), ITU'nun üç sektöründen biridir. ITU-T'nin misyonu, telekomünikasyonun tüm alanlarını kapsayan teknik standartların geliştirilmesidir. ITU-T standartları öneriler olarak adlandırılır
- ISO:
  - Uluslararası Standardizasyon Örgütü (ISO), her ülkeden bir tane olmak üzere 140'tan fazla ülkeden ulusal standart kuruluşlarının dünya çapında bir federasyonudur. ISO, uluslararası mal ve hizmet alışverişini kolaylaştırmak ve entelektüel, bilimsel, teknolojik ve ekonomik faaliyet alanlarında işbirliğini geliştirmek amacıyla standardizasyon ve ilgili faaliyetlerin geliştirilmesini teşvik eden bir sivil toplum kuruluşudur. ISO'nun çalışmaları, Uluslararası Standartlar olarak yayınlanan uluslararası anlaşmalarla sonuçlanmaktadır.

Özet.....olarak eve gidince

- Gizlilik, bütünlük ve kullanılabilirliğin temel güvenlik gereksinimlerini açıklayın
- Kriptografi standartlarına dahil olan önemli kuruluşları listeleyin ve kısaca açıklayın
- Anahtarsız, tek anahtarlı ve iki anahtarlı şifreleme algoritmalarına genel bir bakış sağlayın
- Ağ güvenliğinin ana alanlarına genel bir bilgi verin
- Bilgi güvenliği için bir güven modeli tanımlama Ele alınması gereken güvenlik tehdidi ve saldırı türlerini tartışın ve farklı bilgisayar ve ağ varlığı kategorileri için geçerli olan tehdit ve saldırı türlerine örnekler verin

Kriptografi ve Ağ Güvenliği: İlkeler ve Uygulamalar

Sekizinci Baskı



Bölüm 2

Sayı Teorisine Giriş

Pearson

Telif Hakkı © 2020 Pearson Education, Inc. Tüm Hakları Saklıdır.

Bölünebilirlik

- a, b ve m tamsayı olmak üzere bazı m'ler için $a = mb$ ise sıfır olmayan bir b'nin a'yı **böldüğünü** söyleriz.
- Eğer bölme işleminde kalan yoksa b, a'yı böler.
- $b|a$ gösterimi genellikle b'nin a'yı böldüğü anlamında kullanılır.
- Eğer $b|a$, b'nin a'nın **böleni** olduğunu söyleriz.

24'ün pozitif bölenleri 1, 2, 3, 4, 6, 8, 12 ve 24'tür.

$13|182$; $-5|30$; $17|289$; $-3|33$; $17|0$

Bölünebilirliğin Özellikleri (1/2)

- Eğer $a|1$, ise $a = \pm 1$
- Eğer $a|b$ ve $b|a$, ise $a = \pm b$.
- Herhangi bir $b \neq 0$, 0'ı böler
- Eğer $a|b$ ve $b \mid c$, ise $a|c$

$$\boxed{11|66 \text{ ve } 66|198 = 11|198}$$

- Eğer $b|g$ ve $b|h$, ise $b|(mg + nh)$ rasgele m ve n tamsayıları için geçerli olur

Bölünebilirliğin Özellikleri (2/2)

- Bu son noktayı görmek için şunları unutmayın:
  - Eğer $b|g$, ise g, bazı g_1 tamsayıları için $g = b * g_1$ biçimindedir.

    Eğer $b|h$, o zaman h, bazı h_1 tamsayıları için $h = b * h_1$ biçimindedir.
- Dolayısıyla:
- $mg + nh = mbg_1 + nbh_1 = b * (mg_1 + nh_1)$
- ve bu nedenle b, $mg + nh$'yi böler

$b = 7;\ g = 14;\ h = 63;\ m = 3;\ n = 2$

$7|14$ ve $7|63$.

$7(3*14 + 2*63)$ olduğunu göstermek istersek,

$(3*14 + 2*63) = 7(3*2 + 2*9)$, sahibiz

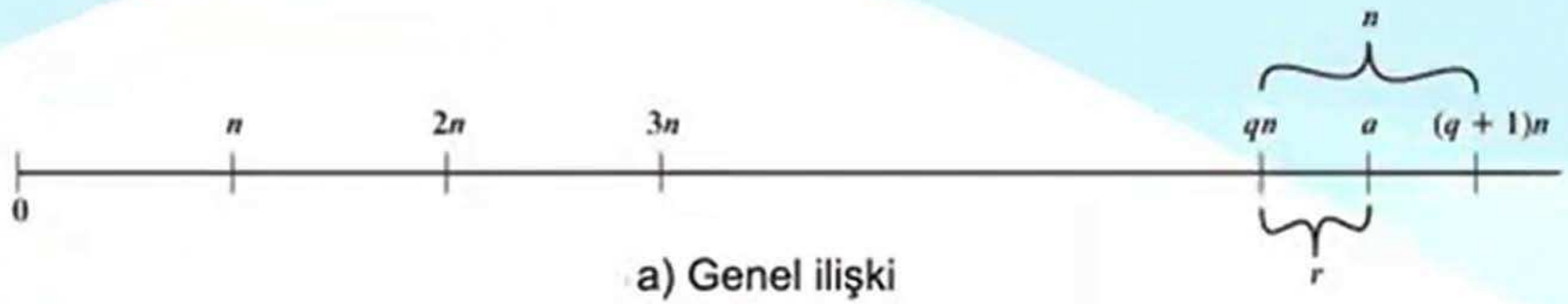
ve; $7|(7(3*2 + 2*9))$ olduğu açık bir şekilde görülmektedir.

Bölme Algoritması

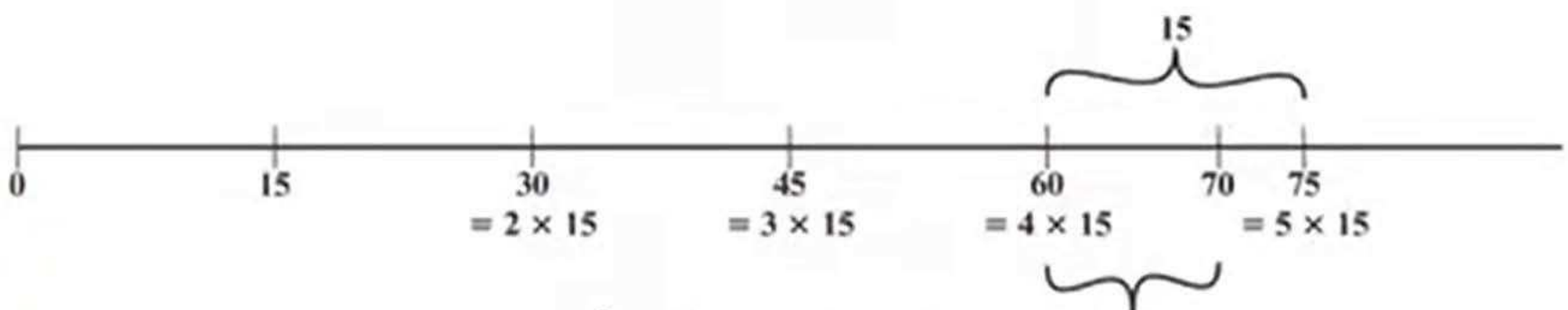
- n herhangi bir pozitif tamsayısı ve
- a herhangi bir negatif olmayan tam sayı,
- a'yı n'ye bölersek,
- aşağıdaki ilişkiye uyan bir tamsayı bölümü q ve bir tamsayı kalanı r elde ederiz:

$$a = qn + r \qquad 0 \leq r < n;\ q = [a/n]$$

Şekil 2.1 $a = qn + r;\ 0 \le r < n$ İlişkisi



a) Genel ilişki



b) Örnek: $70 = (4 \times 15) + 10$

Öklid Algoritması

- Sayılar teorisinin temel tekniklerinden biri
- İki pozitif tamsayının en büyük ortak bölenini belirleme prosedürü
- İki tamsayının, tek ortak pozitif tamsayı çarpanı 1 ise nispeten asaldır.

En Büyük Ortak Bölen (EBOB)

- a ve b'nin en büyük ortak böleni, hem a'yı hem de b'yi bölen en büyük tam sayıdır.
- a ve b'nin en büyük ortak bölenini belirtmek için ebob(a,b) gösterimini kullanabiliriz.
- Ayrıca ebob$(0,0)=0$ olarak tanımlarız
- Pozitif c tamsayısının, aşağıdaki durumlarda a ve b'nin ebob'u olduğu söylenir:
  - c, a ve b'nin bölenidir
  - a ve b'nin herhangi bir böleni c'nin bölenidir.
- Eşdeğer bir tanım şudur:

  ebob(a,b) = max[k, öyle ki k|a ve k|b]

EBOB

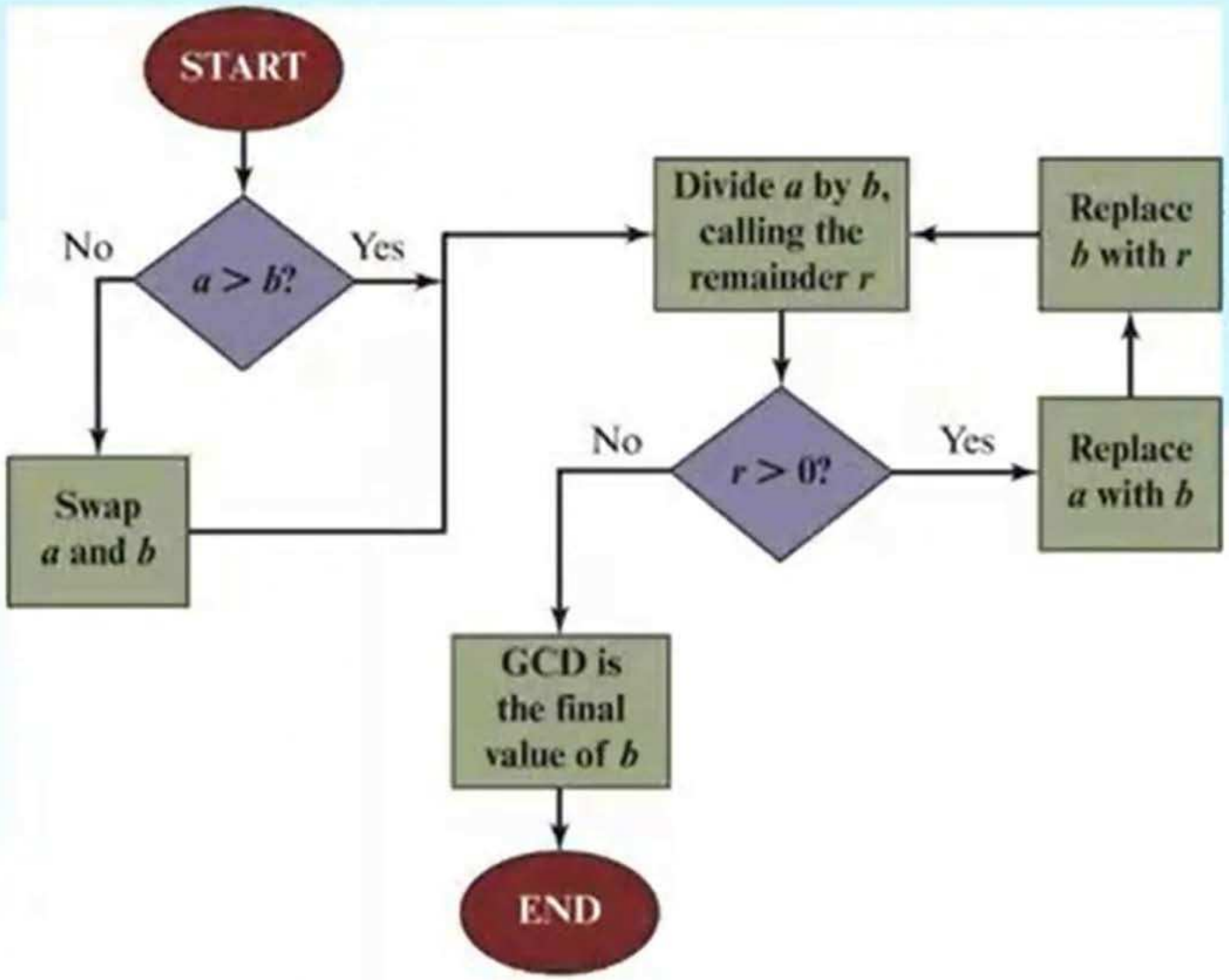
- En büyük ortak bölenin pozitif olmasını istediğimiz için, $ebob(a,b)=ebob(a,-b)=ebob(-a,b)=ebob(-a,-b)$
- Genel olarak, $ebob(a,b)=ebob(|a|,|b|)$

$$\boxed{ebob(60,24)=ebob(60,-24)=12}$$

- Ayrıca, sıfır olmayan tüm tamsayılar 0'a bölündüğü için, $ebob(a,0)=|a|$ elde ederiz.
- İki tam sayı a ve b'nin, tek ortak pozitif tamsayı çarpanları 1 ise göreli asal olduklarını belirtmiştik; bu, $ebob(a,b)=1$ ise a ve b'nin göreli olarak (nispeten) asal olduğunu söylemekle eşdeğerdir.

- 8 ve 15 göreli olarak asaldır çünkü
- 8'in pozitif bölenleri 1, 2, 4 ve 8'dir;
- 15'in pozitif bölenleri 1, 3, 5 ve 15'tir. Yani her iki listedeki tek tam sayı 1'dir.

Şekil 2.2 Öklid Algoritması



Şekil 2.3 Öklid Algoritması

Örnek: ebob(710,310)

Same GCD

GCD GCD

$$710 = 2 \times 310 + 90$$

Şekil 2.3 Öklid Algoritması

Örnek: ebob(710,310)

Same GCD

GCD GCD

$$710 = 2 \times 310 + 90$$

$$310 = 3 \times 90 + 40$$

$$90 = 2 \times 40 + 10$$

$$40 = 4 \times 10$$

Tablo 2.1 Öklid Algoritması Örneği

Dividend	Divisor	Quotient	Remainder
$a = 1160718174$	$b = 316258250$	$q_1 = 3$	$r_1 = 211943424$

Tablo 2.1 Öklid Algoritması Örneği

Dividend	Divisor	Quotient	Remainder
$a = 1160718174$	$b = 316258250$	$q_1 = 3$	$r_1 = 211943424$
$b = 316258250$	$r_1 = 211943434$	$q_2 = 1$	$r_2 = 104314826$

Tablo 2.1 Öklid Algoritması Örneği

Dividend	Divisor	Quotient	Remainder
$a = 1160718174$	$b = 316258250$	$q_1 = 3$	$r_1 = 211943424$
$b = 316258250$	$r_1 = 211943434$	$q_2 = 1$	$r_2 = 104314826$
$r_1 = 211943424$	$r_2 = 104314826$	$q_3 = 2$	$r_3 = 3313772$
$r_2 = 104314826$	$r_3 = 3313772$	$q_4 = 31$	$r_4 = 1587894$
$r_3 = 3313772$	$r_4 = 1587894$	$q_5 = 2$	$r_5 = 137984$
$r_4 = 1587894$	$r_5 = 137984$	$q_6 = 11$	$r_6 = 70070$
$r_5 = 137984$	$r_6 = 70070$	$q_7 = 1$	$r_7 = 67914$
$r_6 = 70070$	$r_7 = 67914$	$q_8 = 1$	$r_8 = 2156$
$r_7 = 67914$	$r_8 = 2156$	$q_9 = 31$	$r_9 = 1078$
$r_8 = 2156$	$r_9 = 1078$	$q_{10} = 2$	$r_{10} = 0$

Modüler Aritmetik (1/3)

- Modül
  - Eğer a ve n pozitif bir tamsayı ise, a n'ye bölündüğünde bir mod n'yi kalan kısım olarak tanımlarız; n tamsayısına **modül** denir
  - Böylece, herhangi bir tamsayı için a:

$$a = qn + r \quad 0 \le r < n; \; q = [a/n]$$

$$a = [a/n] * n + (a \bmod n)$$

$$\boxed{11 \bmod 7 = 4; \; -11 \bmod 7 = 3}$$

Modüler Aritmetik (2/3)

- *Uyumlu* `modulo n`
  - Eğer $(a \bmod n) = (b \bmod n)$ ise, a ve b tamsayılarının **uyumlu modulo n** olduğu söylenir
  - Bu $a=b \pmod{n}$[2] şeklinde yazılır.
  - $a=0 \pmod{n}$ ise, o zaman $n|a$

$$\boxed{73=4 \pmod{23}; \quad 21=-9 \pmod{10}}$$

Uyumlulukların Özellikleri

- Uyumluluklar aşağıdaki özelliklere sahiptir:
  1. $a=b \pmod n$ eğer $n(a-b)$ ise
  - $a=b \pmod n$, $b=a \pmod n$ anlamına gelir
  - $a=b \pmod n$ ve $b=c \pmod n$, $a=c \pmod n$ anlamına gelir.
- İlk noktayı örnekle açıklarsak eğer, burada $n(a-b)$ ise, o zaman bazı k değerleri için $(a-b)=kn$ olur
  - Böylece $a = b + kn$ yazabiliriz
  - Bu nedenle, $(a \bmod n)=(b + kn$ n'ye bölündüğünde kalan kısım$)=(b$ n'ye bölündüğünde kalan kısma$)=(b \bmod n)$

$23=8 \pmod 5$	çünkü	$23-8=15=5*3$
$-11=5 \pmod 8$	çünkü	$-11-5=-16=8*(-2)$
$81=0 \pmod{27}$	çünkü	$81-0=81=27*3$

Modüler Aritmetik (3/3)

- Modüler aritmetik aşağıdaki özellikleri gösterir:
  1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
  2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
  3. $[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$
- İlk özelliği örneklersek eğer::
  - $(a \bmod n) = r_a$ ve $(b \bmod n) = r_b$ şeklinde tanımlayın. Daha sonra bazı j tamsayıları için $a = r_a + jn$ ve bazı k tamsayıları için $b = r_b + kn$ yazabiliriz.
  - Sonra:

$$
\begin{aligned}
(a + b) \bmod n &= (r_a + jn + rb + kn) \bmod n \\
&= (ra + rb + (k + j)n) \bmod n \\
&= (ra + rb) \bmod n \\
&= [(a \bmod n) + (b \bmod n)] \bmod n
\end{aligned}
$$

Kalan Özellikler

- Kalan üç özelliğe örnekler:

```
11 mod 8 = 3; 15 mod 8 = 7
[(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2
(11 + 15) mod 8 =  26 mod 8 = 2
[(11 mod 8) - (15 mod 8)] mod 8 = - 4 mod 8 = 4
(11 - 15) mod 8 = - 4 mod 8 =  4
[(11 mod 8) *  (15 mod 8)] mod 8 =  21 mod 8 = 5
(11 * 15) mod 8 = 165 mod 8 =  5
```

Tablo 2.2 (a) Aritmetik Modülo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Tablo 2.2 (b) Çarpma Modülü 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Tablo 2.2 (c) Toplama ve Çarpma Ters Modülü 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

Tablo 2.3 Z_n'deki Tamsayılar için Modüler Aritmetik Özellikleri

Özellik	İfade
Değişme Özelliği	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Birleştirme Özelliği	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Dağılma Özelliği	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Özdeşlik	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Toplamın Tersi $(-w)$	Her $w \in Z_n$ için, $w + z = 0 \bmod n$ olacak şekilde bir z vardır.

Tablo 2.4 Genişletilmiş Öklid Algoritması Örneği

i	r_i	q_i	x_i	y_i
−1	1759		1	0
0	550		0	1
1	109	3	1	−3
2	5	5	−5	16
3	4	21	106	−339
4	1	1	−111	355
5	0	4		

Sonuç: $d = 1;\ x = -111;\ y = 355$

Asal Sayılar

- Asal sayıların sadece 1 ve kendisine bölünürler
  - Diğer sayıların çarpımı olarak yazılamazlar
- Asal sayılar sayı teorisinin merkezindedir
- $a > 1$ olan herhangi bir tamsayı aşağıdaki gibi benzersiz bir şekilde çarpanlarına ayrılabilir:

$$a = p_1^{a1} * p_2^{a2} * \ . \ . \ . \ * p_{pt}^{at}$$

  burada $p_1 < p_2 < \ . \ . \ . \ < p_t$ asal sayılardır ve burada her a_i pozitif bir tam sayıdır.
- Bu, aritmetiğin temel teoremi olarak bilinir.

Tablo 2.5 2000'in Altındaki Asal Sayılar

3	103	211	307	401	503	601	701	809	907	1009	1103	1203	1301	1409	1511	1601	1709	1803	1901
5	105	223	311	409	509	607	709	811	911	1015	1109	1215	1303	1423	1523	1607	1721	1811	1907
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319	1429	1543	1611	1733	1831	1931
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
13	127	239	337	437	547	631	739	829	941	1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
29	149	263	359	457	571	653	761	859	971	1063	1181	1277	1381	1459	1579	1663	1783	1877	1987
31	151	269	367	461	577	659	769	863	977	1069	1187	1279	1399	1471	1583	1667	1787	1879	1993
37	157	271	373	463	587	661	773	877	983	1087	1193	1283		1483	1597	1669	1789	1889	1997
41	163	277	379	467	593	673	783	881	991	1091		1289		1489		1693			1999
43	167	281	383	479	599	677	797	883	997	1093		1291		1493		1697			
47	173	283	389	487		683		887		1097		1297		1499		1699			
53	179	293	397	491		691				1099				1503					
59	181			499										1509					
61	191																		
67	193																		
71	197																		
73	199																		
79																			
83																			
89																			
97																			

Fermat Teoremi

- Şunları söyler:
  - Eğer p asal ise ve a, p ile bölünemeyen pozitif bir tamsayı ise, o zaman

$$a^{p-1} = 1 \, (mod \, p)$$

- Alternatif bir form şudur:
  - Eğer p asal ise ve a pozitif bir tamsayı ise, o zaman

$$a^{p} = a \, (mod \, p)$$

Tablo 2.6 Euler Totient Fonksiyonunun Bazı Değerleri $\phi(n)$

- $\phi(1) = 1$.
- Bir p asal sayısı için $\phi(p) = p - 1$

- $\phi(n)$, n'den küçük ve n'ye göre asal olan pozitif tamsayıların sayısı

n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

Euler Teoremi

- Nispeten asal olan her a ve n için şunu belirtir:

$$a^{\phi(n)} = 1 \, (mod \, n)$$

- Alternatif bir form şudur:

$$a^{\phi(n)+1} = a \, (mod \, n)$$

Miller-Rabin Algoritması

- Tipik olarak asallık için büyük bir sayıyı test etmek için kullanılır
- Algoritma:

TEST (n)

1. $k>0$, q tek sayı alarak k, q tamsayılarını bulun, $(n-1)=2^k q$;
2. Rastgele bir a tamsayısı seçin, $1<a<n-1$;
3. Eğer $a^q \bmod n = 1$ ise, ("sonuç yok") ifadesini geri dönün;
4. $j=0$'dan $k-1$'e kadar bunu yapın
5. Eğer $(a^{2jq} \bmod n = n-1)$ ise ("sonuç yok") ifadesini geri dönün;
6. ("bileşik") ifadesi dönsün;

Deterministik Asallık Algoritması

- 2002'den önce, çok büyük sayıların asallığını etkili bir şekilde kanıtlamak için bilinen bir yöntem yoktu.
- Kullanımdaki tüm algoritmalar olasılıksal bir sonuç üretiyordu
- 2002'de Agrawal, Kayal ve Saxena, belirli bir büyük sayının asal olup olmadığını verimli bir şekilde belirleyen bir algoritma geliştirdiler.
  - AKS algoritması olarak bilinir
  - Miller-Rabin algoritması kadar verimli görünmemektedir

Çin Kalan Teoremi (CKT)

- MS 100 yıllarında çinli matematikçi Sun-Tsu tarafından keşfedildiğine inanılıyor.
- Sayı teorisinin en faydalı sonuçlarından biridir.
- Tamsayıları, belirli bir aralıkta, bir ikili nispeten asal modüller kümesinden, kalan modüllerinden yeniden oluşturmanın mümkün olduğunu söylüyor.
- Birkaç şekilde ifade edilebilir.

- mod M'deki (potansiyel olarak çok büyük) sayıları daha küçük sayı demetleri cinsinden manipüle etmenin bir yolunu sağlar.
  - Bu, M 150 basamak veya daha fazla olduğunda yararlı olabilir
  - Ancak, M'nin çarpanlarına ayrılmasını önceden bilmek gerekir.

Tablo 2.7 Tam Sayıların Kuvvetleri, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Tablo 2.8 Ayrık Logaritma Tabloları, Modulo 19 (1/2)

(a) Discrete logarithms to the base 2, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{2,19}(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(b) Discrete logarithms to the base 3, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{3,19}(a)$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

(c) Discrete logarithms to the base 10, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{10,19}(a)$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9

Tablo 2.8 Ayrık Logaritma Tabloları, Modulo 19 (2/2)

(d) Discrete logarithms to the base 13, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{13,19}(a)$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9

(e) Discrete logarithms to the base 14, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{14,19}(a)$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	4	9

(f) Discrete logarithms to the base 15, modulo 19

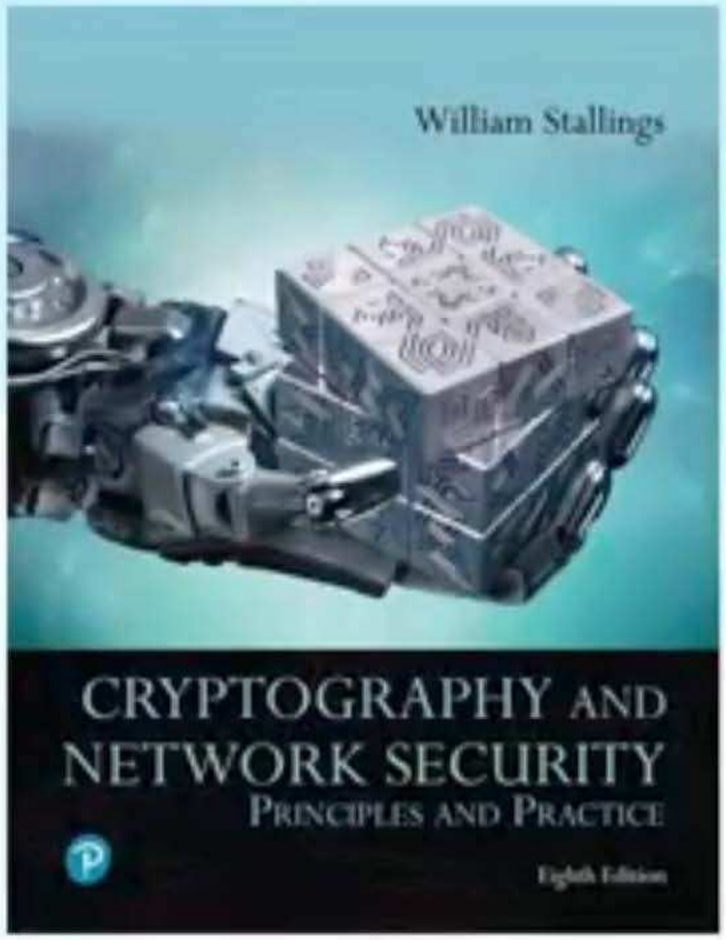
a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{15,19}(a)$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9

Özet

- Bölünebilirlik kavramını ve bölme algoritmasını anladık.
- En büyük ortak böleni bulmak için Öklid algoritmasını nasıl kullanacağımızı öğrendik.
- Modüler aritmetik kavramlarına genel bir bakış sunduk.
- Genişletilmiş Öklid algoritmasının işleyişini açıkladık.
- Asal sayılarla ilgili temel kavramları tartıştık.
- Fermat teoremini anladık
- Euler teoremini anladık
- Euler'in totient işlevini tanımladık
- Asallık testi konusunda bir sunum yaptık
- Çin kalan teoremini açıkladık
- Ayrık logaritmaları tanımladık

Kriptografi ve Ağ Güvenliği: İlkeler ve Uygulamalar

Sekizinci Baskı



Bölüm 3

Klasik Şifreleme Teknikleri

Pearson

Telif Hakkı © 2020 Pearson Education, Inc. Tüm Hakları Saklıdır.

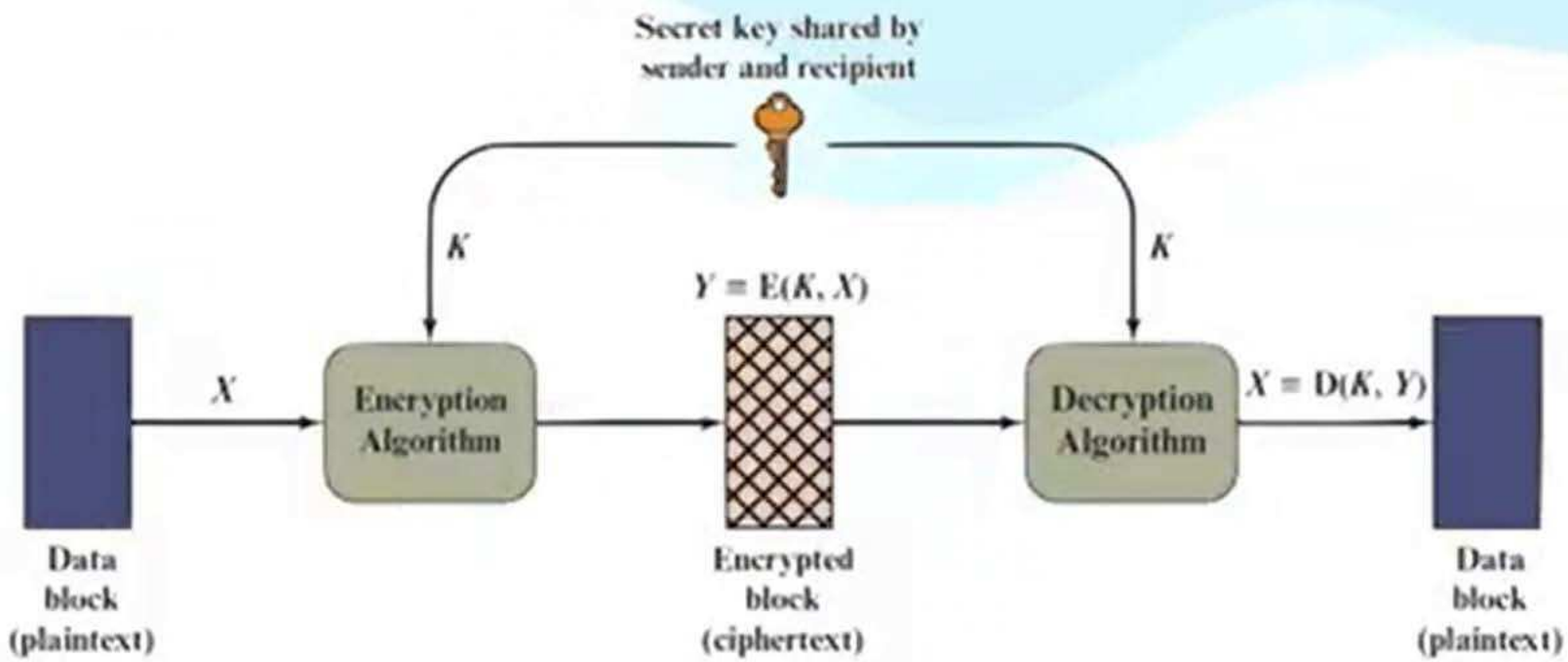
Tanımlar (1/2)

Düz metin (Plaintext)	• Orijinal bir mesaj • Şifreli metin • Kodlanmış mesaj
Şifreleme	• Düz metinden şifreli metne dönüştürme işlemi
Deşifre etme/ şifre çözme	• Düz metni şifreli metinden geri yükleme

Tanımlar (2/2)

Kriptografi	• Şifreleme için kullanılan birçok şemanın çalışma alanı
Kriptografik sistem/şifre	• Bir şema
Kriptoanaliz	• Şifreleme detayları hakkında herhangi bir bilgi sahibi olmadan bir mesajı deşifre etmek için kullanılan teknikler
Kriptoloji	• Kriptografi ve kriptanaliz alanları

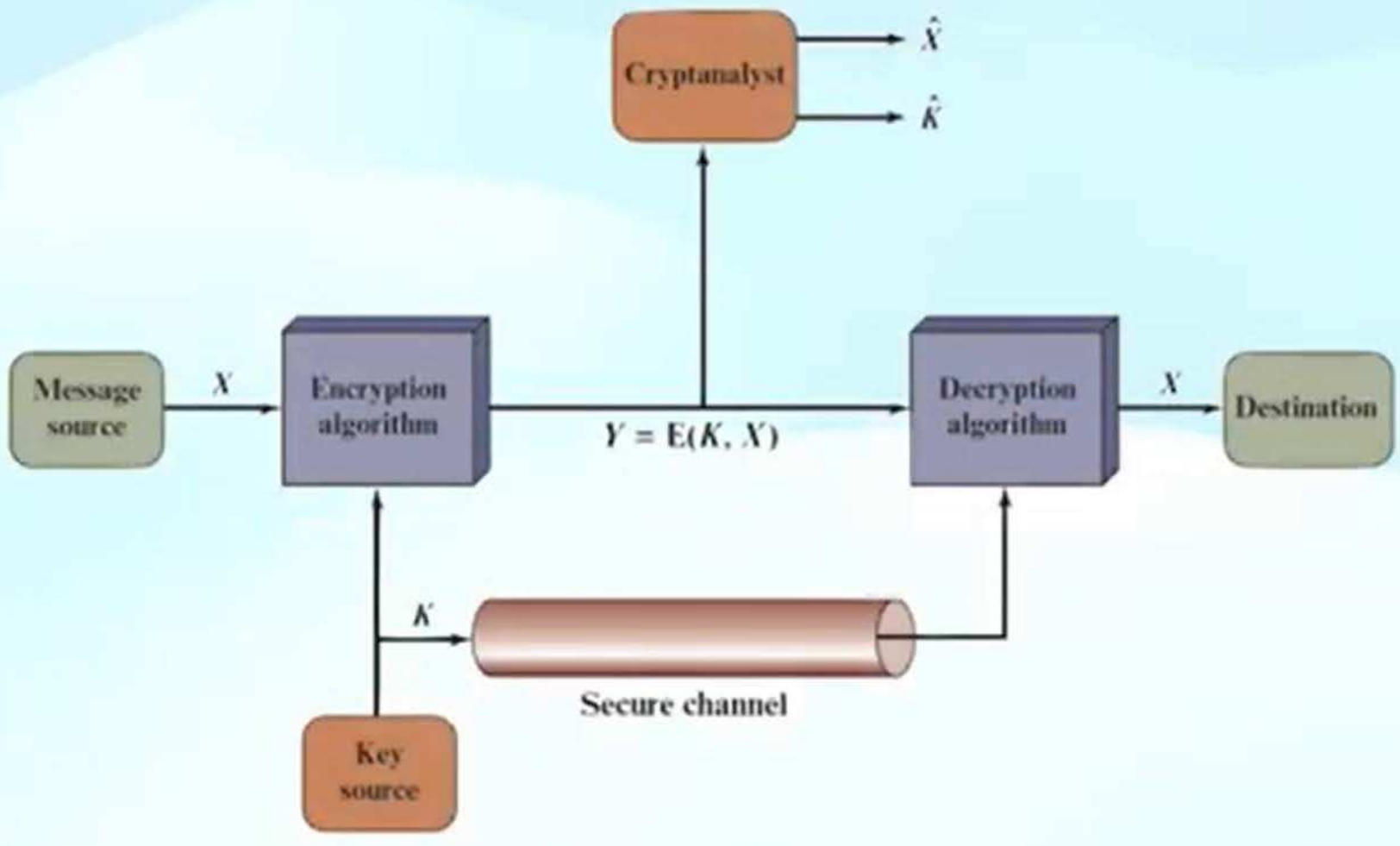
Şekil 3.1 Basitleştirilmiş Simetrik Şifreleme Modeli



Simetrik Şifre Modeli

- Geleneksel şifrelemenin güvenli kullanımı için iki gereksinim vardır:
  - Güçlü bir şifreleme algoritması
  - Gönderen ve alıcı, gizli anahtarın kopyalarını güvenli bir şekilde almış olmalı ve anahtarı güvende tutmalıdır.

Şekil 3.2 Simetrik Şifreleme Sistemi Modeli



Kriptografik Sistemler

Üç bağımsız boyut boyunca karakterize edilir:

Düz metni şifreli metne dönüştürmek için kullanılan işlem türleri	• İkame (yerine koyma) • Transpozisyon (yer değiştirme)
Kullanılan anahtar sayısı	• Simetrik, • tek anahtarlı, • gizli anahtarlı, • geleneksel şifreleme • Asimetrik, iki anahtarlı veya ortak anahtarlı şifreleme
Düz metnin işlenme şekli	• Blok şifreleme • Akış şifresi

Kriptoanaliz ve Kaba Kuvvet Saldırısı

Kriptoanaliz

- Saldırı, algoritmanın doğasına ve düz metnin genel özellikleri hakkında bazı bilgilere dayanır.
- Saldırı, belirli bir düz metni çıkarmaya veya kullanılan anahtarı çıkarmaya çalışmak için algoritmanın özelliklerinden yararlanır

Kaba kuvvet saldırısı (Brute-force attack)

- Saldırgan, düz metne anlaşılır bir çeviri elde edilene kadar bir şifreli metin parçası üzerinde mümkün olan her anahtarı dener.
- Ortalama olarak, başarıya ulaşmak için tüm olası anahtarların yarısı denenmelidir.

Tablo 3.1 Şifrelenmiş Mesajlara Yönelik Saldırı Türleri

Saldırı Türü	Kriptoanalizci tarafından bilinir
Yalnızca şifreli metin	• Şifreleme algoritması • şifreli metin
Bilinen Düz Metin	• Şifreleme algoritması • şifreli metin • Gizli anahtarla oluşturulmuş bir veya daha fazla düz metin-şifreli metin çifti
Seçilen Düz Metin	• Şifreleme algoritması • şifreli metin • Kriptanalizör tarafından seçilen düz metin mesajı ve gizli anahtarla oluşturulan karşılık gelen şifreli metin
Seçilen şifreli metin	• Şifreleme algoritması • şifreli metin • Kriptanalizör tarafından seçilen şifreli metin ve gizli anahtarla oluşturulan karşılık gelen şifresi çözülmüş düz metin
Seçilen Metin	• Şifreleme algoritması • şifreli metin • Kriptanalizör tarafından seçilen düz metin mesajı ve gizli anahtarla oluşturulan karşılık gelen şifreli metin • Kriptanalizör tarafından seçilen şifreli metin ve gizli anahtarla oluşturulan karşılık gelen şifresi çözülmüş düz metin

Pearson
Doç. Dr. ALİ YILMAZ

Şifreleme Şeması (Düzeni) Güvenliği

- Koşulsuz güvenli
  - Rakibin ne kadar zamanı olursa olsun, gerekli bilgi orada olmadığı için şifreli metnin şifresini çözmesi imkansızdır.
- Hesaplama açısından güvenli
  - Şifreyi kırmanın maliyeti, şifrelenmiş bilginin değerini aşıyor
  - Şifreyi kırmak için gereken süre, bilginin faydalı ömrünü aşıyor

Kaba Kuvvet Saldırısı

- Şifreli metnin anlaşılır bir çevirisi düz metne dönüştürülene kadar mümkün olan her anahtarı denemeyi içerir
- Ortalama olarak, başarıya ulaşmak için olası tüm anahtarların yarısı denenmelidir.
- Kaba kuvvet yaklaşımını desteklemek için, beklenen düz metin hakkında bir dereceye kadar bilgiye ihtiyaç vardır ve düz metni otomatik olarak çöpten ayırt etmenin bazı yollarına da ihtiyaç vardır.

Güçlü Şifreleme

Güçlü şifreleme terimi, yetkisiz kişilerin veya sistemlerin şifrelenmiş düz metne erişmesini pratik olmayan bir şekilde zorlaştıran şifreleme şemalarını ifade eder.

Bir şifreleme algoritmasını güçlü kılan özellikler şunlardır:

- Uygun şifreleme algoritması seçimi
- Yeterince uzun anahtar uzunluklarının kullanımı
- Uygun protokol seçimi
- İyi tasarlanmış bir uygulama
- Kasıtlı olarak ortaya konan gizli kusurların yokluğu

İkame (yerine koyma) Tekniği

- Düz metindeki harflerin başka harflerle veya rakamlarla veya sembollerle değiştirildiği bir tekniktir.
- Düz metin bir bit dizisi olarak görülüyorsa, ikame, düz metin bit modellerinin şifreli metin bit modelleriyle değiştirilmesini içerir.

Sezar Şifresi

- Bir ikame şifresinin bilinen en basit ve en eski kullanımı
- Julius Caesar tarafından kullanılmıştır
- Alfabenin her harfini, alfabenin üç adım aşağısında duran harfle değiştirmeyi içerir
- Alfabe, Z'yi takip eden harf A olacak şekilde sarılır.

Düz-metin:	meet	me	after	the	toga	party
Şifre :	PHHW	PH	DIWHU	WKH	WRJD	SDUWB

Sezar Şifreleme Algoritması

- Dönüşümü şu şekilde tanımlayabilir:

a b c d e f g h i j k l m n o p q r s t u v w x y z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- Matematiksel olarak her harfe bir sayı verin

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Algoritma şu şekilde ifade edilebilir::

$$c = E(3, p) = (p + 3) \bmod (26)$$

- Kayma herhangi bir miktarda olabilir, böylece genel Sezar algoritması şöyledir:

$$C = E(k, p) = (p + k) \bmod 26$$

- k, 1 ile 25 arasında bir değer aldığında; şifre çözme algoritması basitçe:

$$p = D(k, C) = (C - k) \bmod 26$$

Şekil 3.3 Sezar Şifresinin Kaba Kuvvet Kriptoanalizi

KEY	
	PHAN PH DINSU MNR MRJD SDUMB
1	oggv og chvyt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	ssh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Sıkıştırılmış Metin Örneği

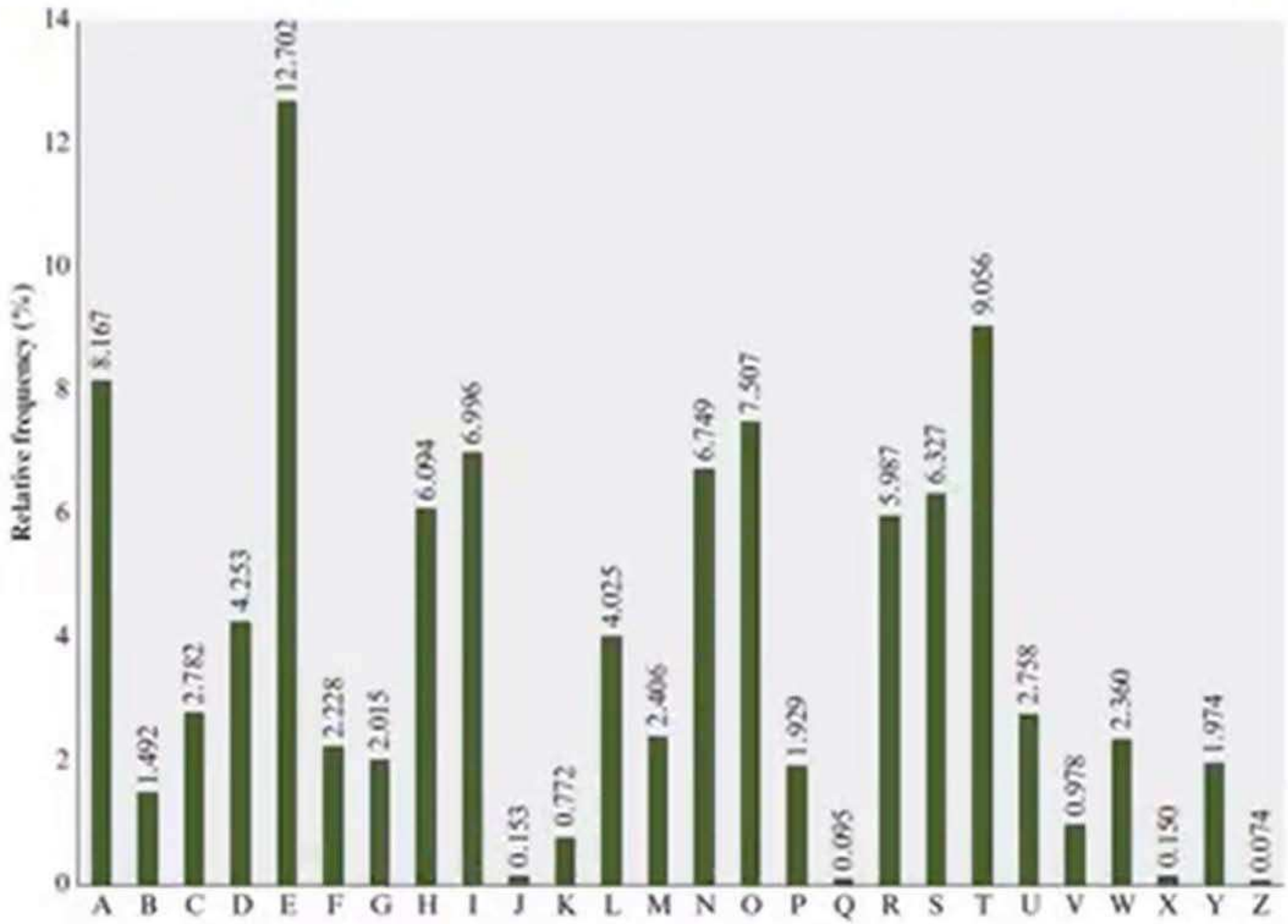
Şekil 3.4 Sıkıştırılmış Metin Örneği

```
˜+Wµ"— Ω-O)≤4{∞‡¸ ë~Ω%ràu·¯í ◊¯Z-
Ú≠2Ò#Åæ∂ œ«q7¸Ωn·®3N◊Ú Œz'Y-ƒ∞Í[±Û_ èΩ,<NO¬±«ˇxã  Åä£èü3Å
x}ö§k°Â
_yÍ ˆΔÉ] ¸¤ J/˙iTê&ı 'c<uΩ-
 ÄD(G WÄC~y_ïõÄW PÔı«ÎÜ†ç],¤¡ˇÌˆüÑπ˜≈ˇLˇ9OgflOˇ&Œ≤ ¬≤ ØÔ§˝:
 ˇŒ!SGqèvoˆ ú\¸S>h<-*6ø‡%x´˝|fiÓ#=˜my‰ˇ≥ñP<,ƒi Áj  Å◊¿˝Zù-
Ω¨Õ¯6Œÿ{% „ΩÊó ¸ï π+ÁÎ˙úO2çSÿ´O-
2ÄflßÌ /@^"∏K¤ªPŒπ¸úéˆ´3∑˜ö˘ÔZÌ"Y¬ŸΩæY> Ω+eô/˙<K£¿*÷˜"≤Ù˜
B ZøK˜Qßÿüƒ¸!ÒflÎzsS/]>ÈQ ü
```

Monoalfabetik Şifre

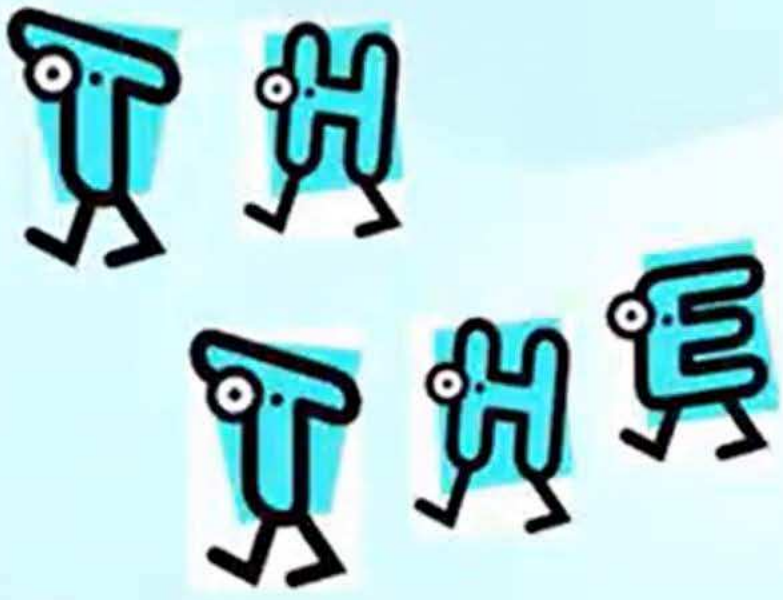
- Permütasyon
  - Sonlu bir elemanlar kümesinden S, S'nin tüm elemanlarının sıralı bir dizisidir ve her eleman tam olarak bir kez görünür.
- "Şifre" satırı 26 alfabetik karakterin herhangi bir permütasyonu olabilirse, o zaman $26!$ veya 4×10^{26}'dan büyük olası anahtar vardır.
  - Bu, DES için anahtar alanından 10 kat daha büyüktür.
  - Yaklaşım, *tek alfabetik ikame şifresi* olarak adlandırılır, çünkü ileti başına tek bir şifreleme alfabesi kullanılır.

Şekil 3.5 İngilizce Metindeki Harflerin Göreli Sıklığı



Tek Alfabetik Şifreler

- Orijinal alfabenin frekans verilerini yansıttıkları için kırılması kolaydır
- Karşı önlem, tek bir harf için birden fazla ikame (homofon) sağlamaktır.
- Digram
  - İki harfli kombinasyon
  - En yaygın olanı *th*
- Trigram
  - Üç harfli kombinasyon
  - En sık *the*



Playfair Şifresi

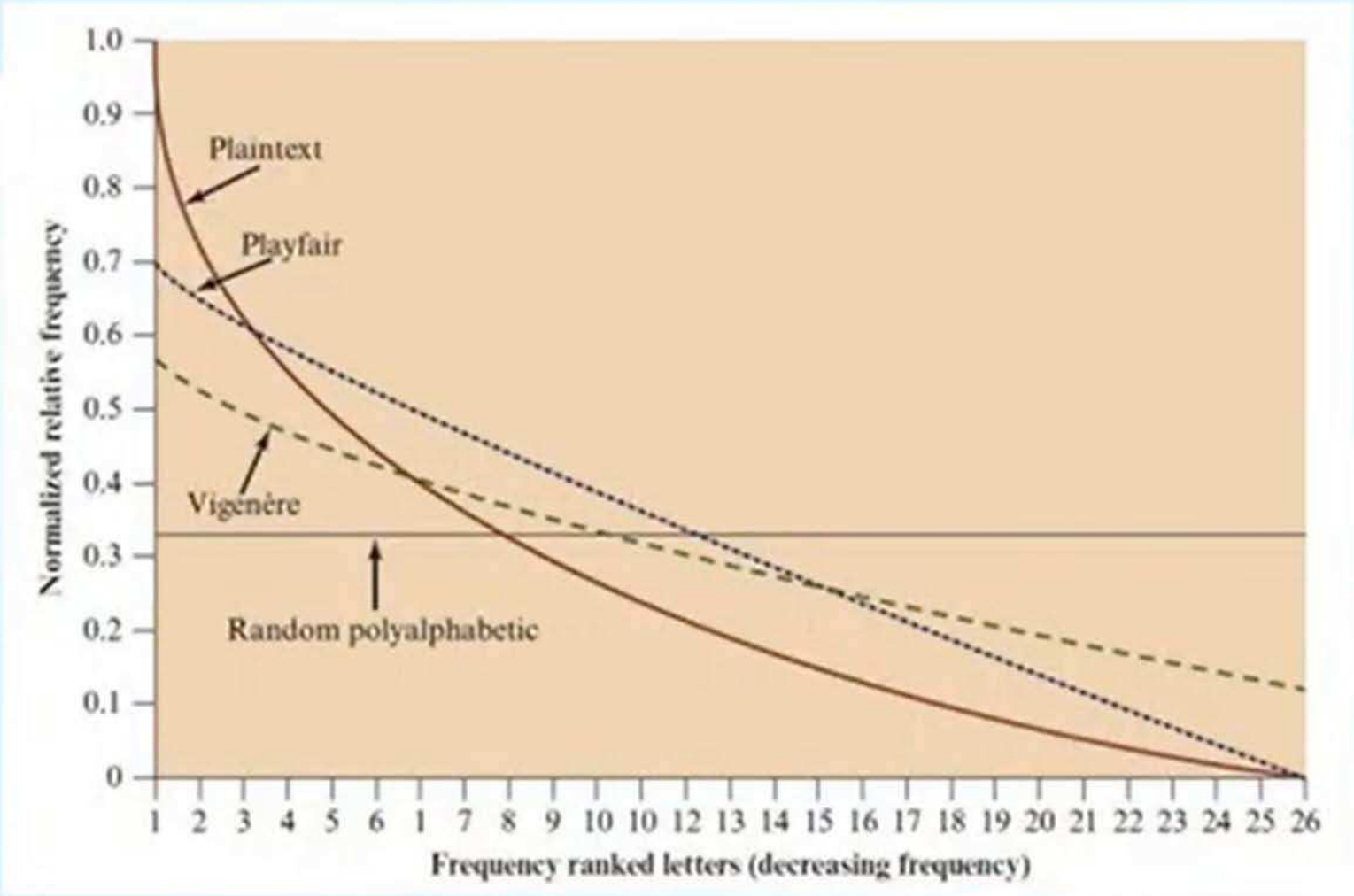
- En iyi bilinen çok harfli şifreleme şifresi
- Düz metindeki digramları tek birimler olarak ele alır ve bu birimleri şifreli metin digramlarına çevirir
- Bir anahtar kelime kullanılarak oluşturulan 5×5 harf matrisinin kullanımına dayanır
- 1854 yılında İngiliz bilim adamı Sir Charles Wheatstone tarafından icat edildi.
- I. Dünya Savaşı'nda İngiliz Ordusu ve II. Dünya Savaşı sırasında ABD Ordusu ve diğer Müttefik kuvvetler tarafından standart saha sistemi olarak kullanılmıştır.

Playfair Anahtar Matrisi

- Anahtar kelimenin harflerini (eksi çiftler) soldan sağa ve yukarıdan aşağıya doldurun, ardından matrisin geri kalanını kalan harflerle alfabetik sırayla doldurun
- MONARCHY anahtar kelimesini kullanarak:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Şekil 3.6 Harflerin Oluşumunun Göreceli Sıklığı



Hill Şifresi

- 1929'da matematikçi Lester Hill tarafından geliştirildi
- Gücü, tek harfli frekansları tamamen gizlemesidir.
- Daha büyük bir matrisin kullanılması daha fazla frekans bilgisini gizler.
  - 3 x 3 Hill şifresi sadece tek harfli değil, aynı zamanda iki harfli frekans bilgilerini de gizler.
- Yalnızca şifreli metin saldırısına karşı güçlü, ancak bilinen bir düz metin saldırısıyla kolayca kırılabilir.

Çoklu Alfabetik Şifreler

- Çoklu alfabetik ikame şifresi
  - Düz metin mesajında ilerledikçe farklı tek alfabetik ikameler kullanarak basit tek alfabeli tekniği geliştirir

- Tüm bu tekniklerin ortak özellikleri şunlardır:
  - Bir dizi ilgili monoalfabetik ikame kuralı kullanılır
  - Bir anahtar, belirli bir dönüşüm için hangi özel kuralın seçildiğini belirler

Vigènere Şifreleme

- En iyi bilinen ve en basit çok alfabetik ikame şifrelerinden biri
- Bu şemada, ilgili monoalfabetik ikame kuralları seti, 0'dan 25'e kaydırmalı 26 Sezar şifresinden oluşur.
- Her şifre, düz metin a harfinin yerine geçen şifreli metin harfi olan bir anahtar harfle gösterilir.

Vigenère Şifresi Örneği

- Bir mesajı şifrelemek için, mesaj kadar uzun bir anahtar gereklidir

  Genellikle, anahtar tekrarlanan bir anahtar kelimedir

- Örneğin, anahtar kelime "*deceptive*", ve "we are discovered save yourself" mesajı şu şekilde şifrelenir:

anahtar: deceptivedeceptivedeceptive

Düz metin: wearediscoveredsaveyourself

Şifreli metin: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

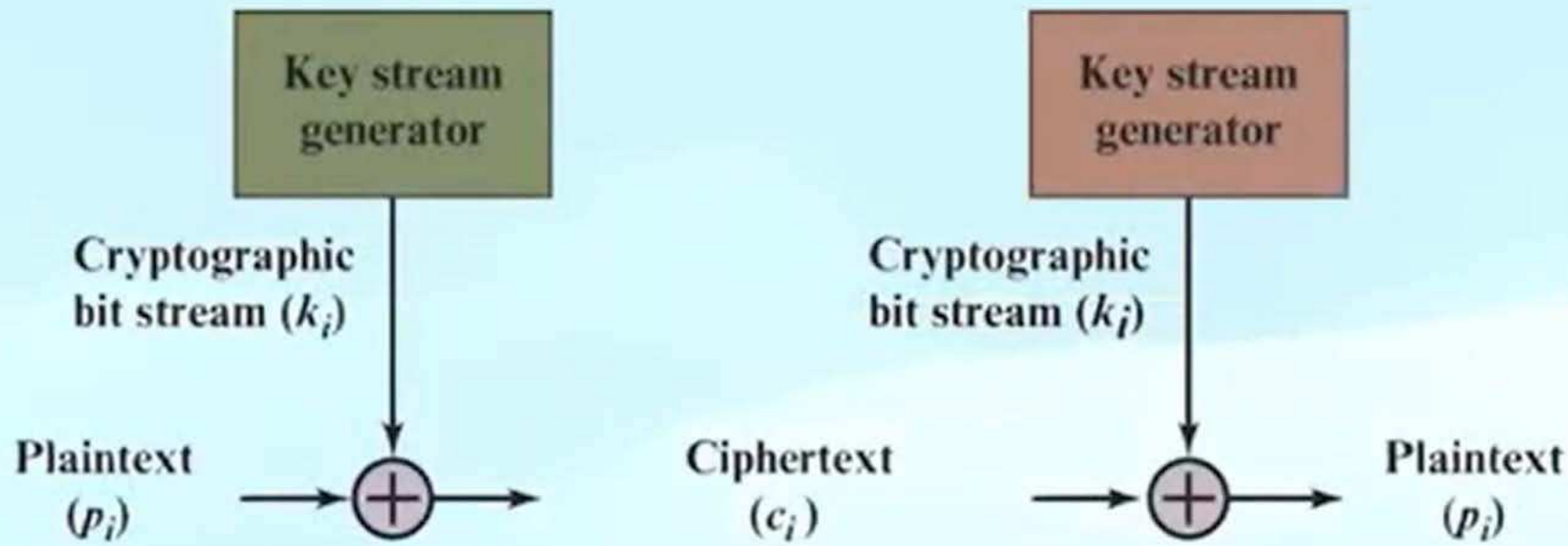
Vigenère Otomatik Anahtar Sistemi

- Çalışan bir anahtar sağlamak için bir anahtar sözcük düz metinle birleştirilir
- Örnek:

anahtar: deceptivewearediscoveredsav
düz metin: wearediscoveredsaveyourself
şifreli metin: ZICVTWQNGKZEIIGASXSTSLVVWLA

- Bu şema bile kriptoanalize karşı savunmasızdır
  - Anahtar ve düz metin, harflerin aynı sıklık dağılımını paylaştığından, istatistiksel bir teknik uygulanabilir.

Vernam Şifresi



Tek Seferlik Bloknot

- Bir Sinyal Kolordusu subayı Joseph Mauborgne tarafından önerilen Vernam şifresinin iyileştirilmesi.
- Anahtarın yinelenmesine gerek kalmaması için ileti kadar uzun rastgele bir anahtar kullanın.
- Anahtar tek bir iletiyi şifrelemek ve şifresini çözmek için kullanılır ve sonra atılır.
- Her yeni ileti, yeni iletiyle aynı uzunlukta yeni bir anahtar gerektirir.
- Şema kırılmaz
  - Düz metinle istatistiksel bir ilişki taşımayan rastgele çıktı üretir.
  - Şifreli metin düz metin hakkında hiçbir bilgi içermediğinden, kodu kırmanın bir yolu yoktur.

Zorluklar

Tek seferlik bloknot tam güvenlik sunar, ancak pratikte iki temel zorluğu vardır:

Büyük miktarlarda rastgele anahtar yapmanın pratik sorunu var.

- Yoğun olarak kullandan herhangi bir sistem düzenli olarak milyonlarca rastgele karakter gerektirebilir.

anahtar dağıtım problemi

Gönderilecek her mesaj için, hem gönderen hem de alıcı tarafından eşit uzunlukta bir anahtara ihtiyaç vardır.

Bu zorluklar nedeniyle, bir kerelik bloknot sınırlı bir faydaya sahiptir.

Öncelikle çok yüksek güvenlik gerektiren düşük bant genişliğine sahip kanallar için kullanışlıdır

Tek seferlik bloknot, mükemmel gizlilik sergileyen tek şifreleme sistemidir (bakınız Ek F)

Raylı Çit Şifresi

- En basit transpozisyon şifresi
- Düz metin, bir köşegen dizisi olarak yazılır ve ardından bir satır dizisi olarak okunur
- "meet me after the toga party" mesajını derinlik 2'lik bir demiryolu çitiyle şifrelemek için şunları yazacağız:

m e m a t r h t g p r y
e t e f e t e o a a t

Şifreli mesaj:

MEMATRHTGPRYETEFETEOAAT

Satır Yer Değiştirme Şifresi

- Daha karmaşık bir transpozisyondur
- İletiyi dikdörtgen içinde, satır satır yazın ve iletiyi kapalı olarak sütundan sütuna okuyun, ancak sütunların sırasını kalıcı hale getirin.
  - Sütunların sırası daha sonra algoritmanın anahtarı haline gelir

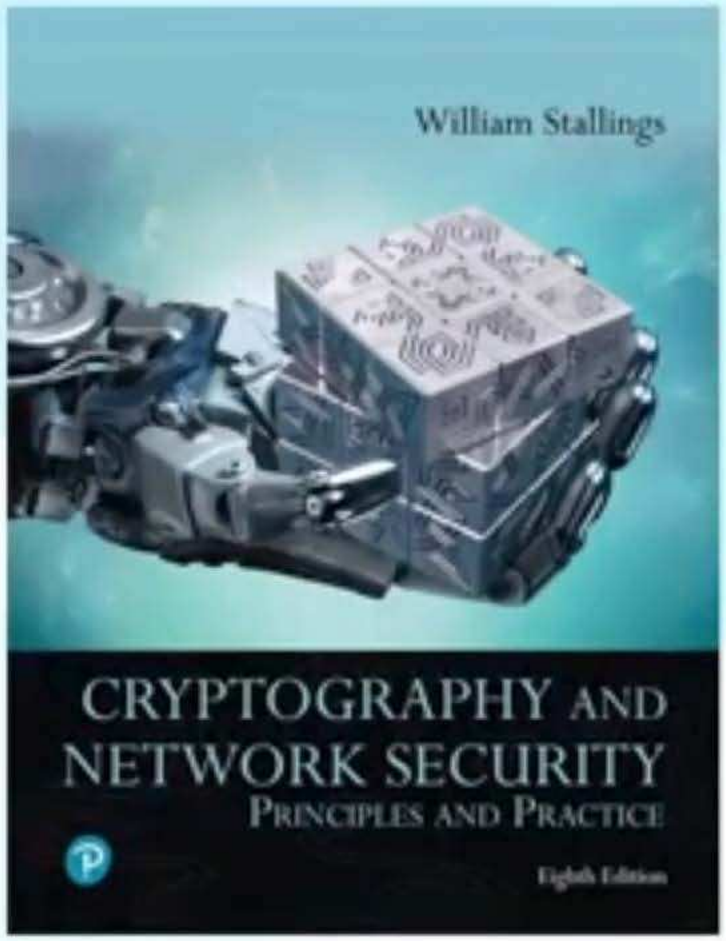
Anahtar:	4 3 1 2 5 6 7
Düz metin:	a t t a c k p
	o s t p o n e
	d u n t i l t
	w o a m x y z
Şifreli Metin:	TTNAAPTMTSUOAODWCOIXKNLYPETZ

Özet

- Simetrik kriptografinin ana kavramlarına genel bir bakış sunar.
- Kriptanaliz ve kaba kuvvet saldırısı arasındaki farkı açıklayın.
- Monoalfabetik bir ikame şifresinin çalışmasını anlayın.
- Polialfabetik bir şifrenin çalışmasını anlama
- Hill şifresine genel bir bakış sunun.

Kriptografi ve Ağ Güvenliği: İlkeler ve Uygulamalar

Sekizinci Baskı



Bölüm 4

Blok Şifreleri ve Veri Şifreleme Standardı

Pearson

Doç. Dr. Ali YILMAZ

Telif Hakkı © 2020 Pearson Education, Inc. Tüm Hakları Saklıdır.

Akış Şifresi (1/2)

- Dijital veri akışını her seferinde bir bit veya bir bayt olarak şifreler
  - Örnekler:
    - Otomatik anahtarlı Vigenère şifresi
    - Vernam şifresi
- İdeal durumda, anahtar akışının düz metin bit akışı kadar uzun olduğu Vernam şifresinin tek seferlik bir bloknot versiyonu kullanılacaktır.
  - Kriptografik anahtar akışı rasgeleyse, bu şifre, anahtar akışını elde etmek dışında herhangi bir yöntemle kırılmaz.
    - Anahtar akışı, her iki kullanıcıya da bağımsız ve güvenli bir kanal aracılığıyla önceden sağlanmalıdır.
    - Amaçlanan veri trafiği çok büyükse, bu aşılmaz lojistik sorunları ortaya çıkarır.

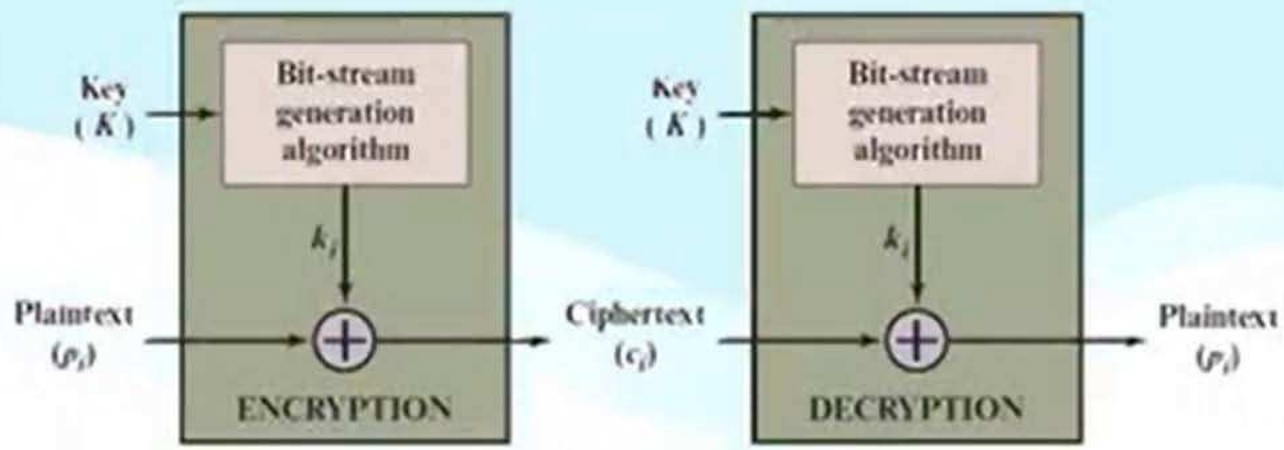
Akış Şifresi (2/2)

- Pratik nedenlerle, bit akışı üreteci, kriptografik bit akışının her iki kullanıcı tarafından üretilebilmesi için algoritmik bir prosedür olarak uygulanmalıdır.
  - Bit akışının önceki bölümlerine dayalı olarak bit akışının gelecekteki bölümlerini tahmin etmek hesaplama açısından pratik olmamalıdır.
  - İki kullanıcının yalnızca oluşturma anahtarını paylaşması gerekir ve her biri anahtar akışını üretebilir

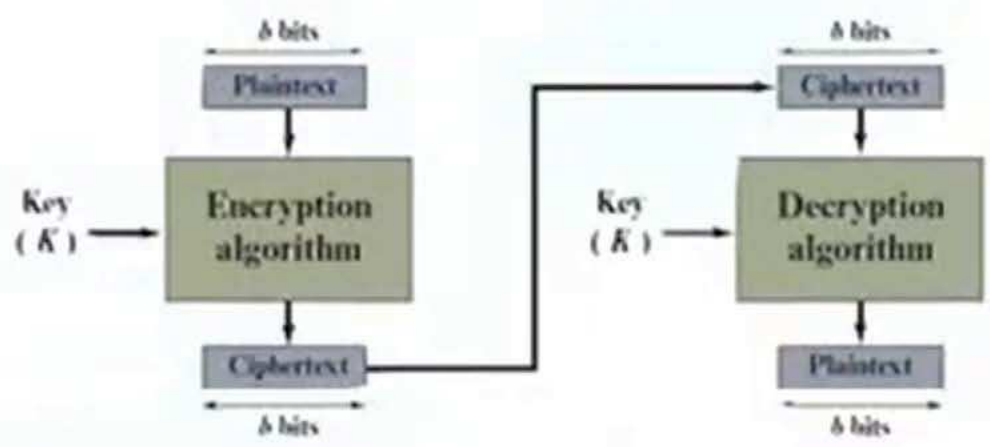
Blok Şifreleme

- Bir düz metin bloğu bir bütün olarak ele alınır ve eşit uzunlukta bir şifreli metin bloğu üretmek için kullanılır.
- Tipik olarak 64 veya 128 bitlik bir blok boyutu kullanılır
- Bir akış şifresinde olduğu gibi, iki kullanıcı simetrik bir şifreleme anahtarını paylaşır.
- Ağ tabanlı simetrik kriptografik uygulamaların çoğu, blok şifrelerden yararlanır.

Şekil 4.1 Akış Şifresi ve Blok Şifresi

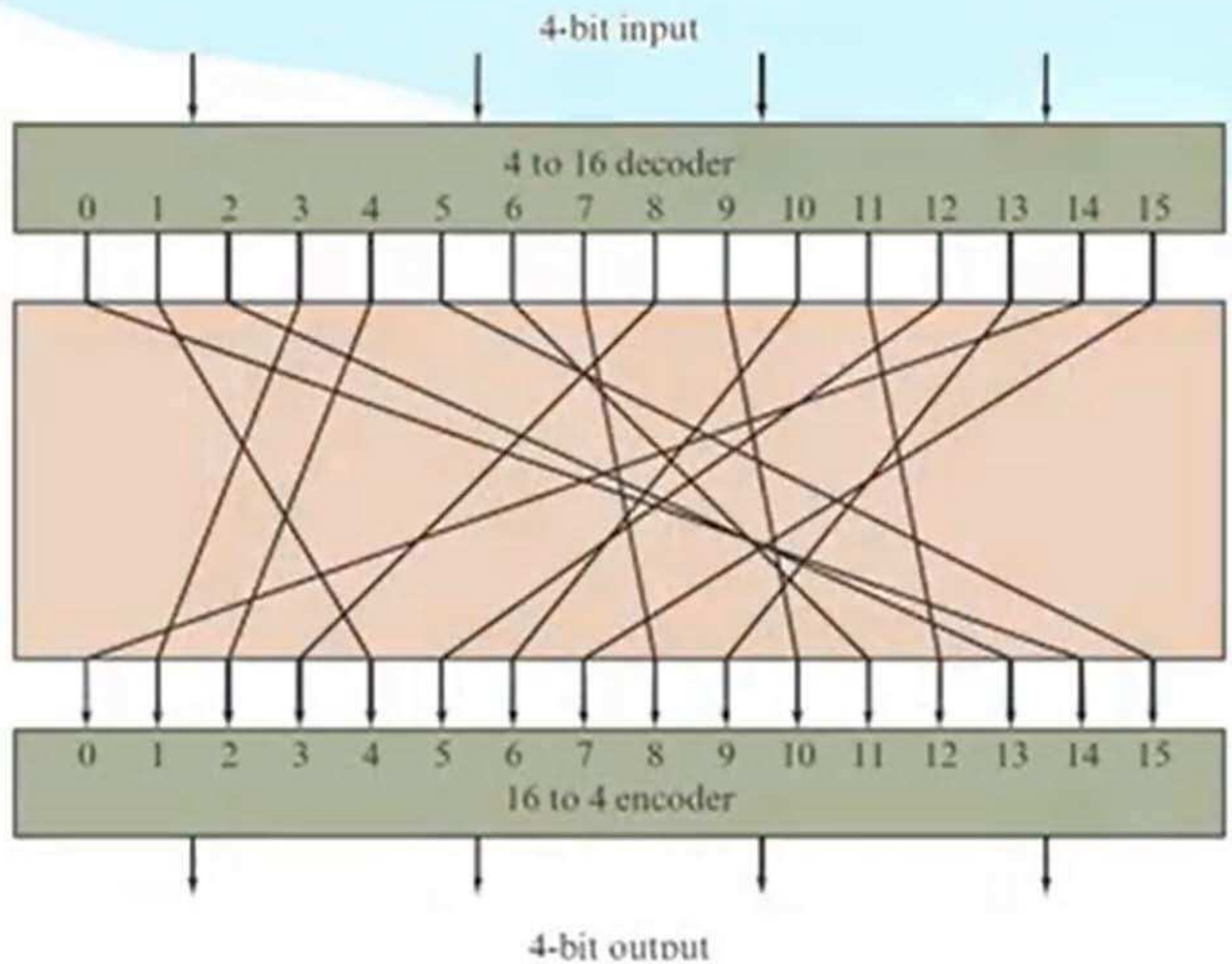


(a) Stream cipher using algorithmic bit-stream generator



(b) Block cipher

Şekil 4.2 Genel n-bit-n-bit Blok Değiştirme ($n = 4$ ile gösterilmiştir)



Tablo 4.1 Şekil 4.2'deki Yer Değiştirme Şifresi için Şifreleme ve Şifre Çözme Tabloları

Düz metin	Şifreli metin
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Şifreli metin	Düz metin
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100
0110	1010
0111	1111
1000	0111
1001	1101
1010	1001
1011	0110
1100	1011
1101	0010
1110	0000
1111	0101

Feistel Şifresi

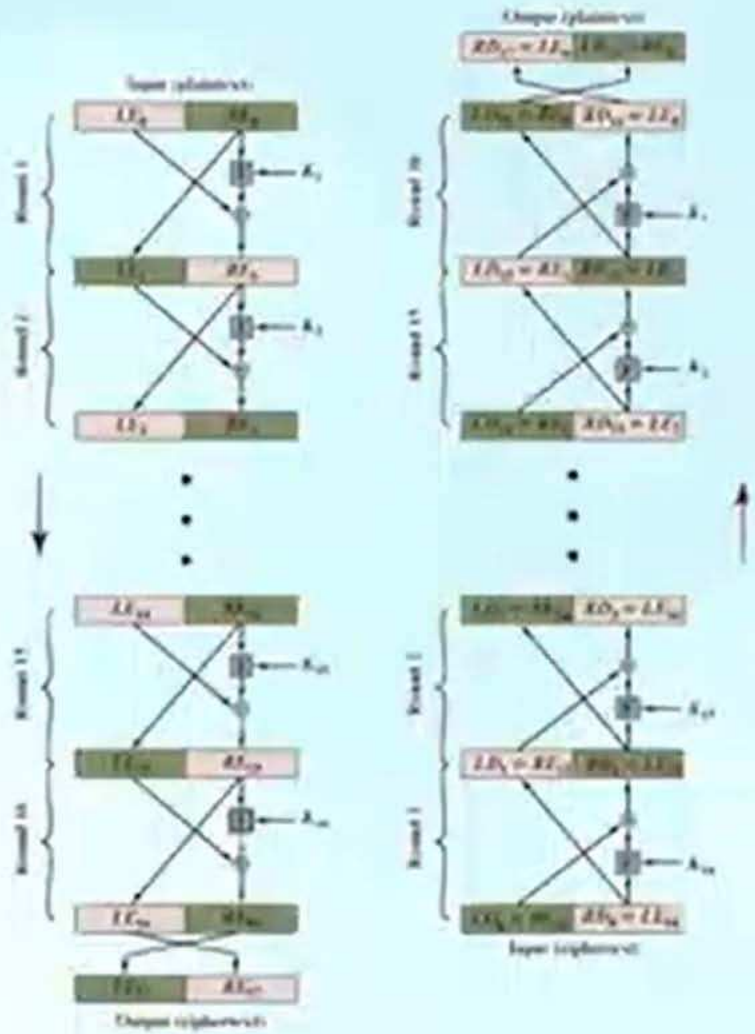
- Feistel, ikameleri ve permütasyonları değiştiren bir şifrenin kullanılmasını önermiştir.
- Yer değiştirme (Substitutions)
  - Her düz metin öğesi veya öğe grubu, karşılık gelen bir şifreli metin öğesi veya öğe grubuyla benzersiz bir şekilde değiştirilir.
- Permütasyon
  - Dizide hiçbir öğe eklenmez, silinmez veya değiştirilmez, bunun yerine öğelerin dizide görünme sırası değiştirilir.
- Karışıklık ve difüzyon fonksiyonlarını değiştiren bir çarpım şifresi geliştirmek için Claude Shannon'ın önerisinin pratik bir uygulamasıdır.
- Şu anda kullanımda olan birçok önemli simetrik blok şifre tarafından kullanılan yapıdır.

Difüzyon ve Karışıklık (Confusion)

- Herhangi bir şifreleme sistemi için iki temel yapı taşını anlamak için Claude Shannon tarafından sunulan terimler
  - Shannon'un endişesi, istatistiksel analize dayalı kriptanalizi engellemekti.
- Difüzyon
  - Düz metnin istatistiksel yapısı, şifreli metnin uzun vadeli istatistiklerine dağıtılır.
  - Bu, her düz metin basamağının birçok şifreli metin basamağının değerini etkilemesiyle elde edilir.
- Karışıklık
  - Şifreli metnin istatistikleri ile şifreleme anahtarının değeri arasındaki ilişkiyi olabildiğince karmaşık hale getirmeye çalışır.

Saldırgan şifreli metnin istatistiklerini biraz ele geçirebilse bile, anahtarın bu şifreli metni üretmek için kullanılma şekli o kadar karmaşıktır ki, anahtarın çıkarılmasını zorlaştırır.

Şekil 4.3 Feistel Şifreleme ve Şifre Çözme (16 turlu)



Feistel Şifre Tasarım Özellikleri (1/2)

- Blok boyutu
  - Daha büyük blok boyutları, belirli bir algoritma için daha fazla güvenlik sunar, ancak daha düşük şifreleme / şifre çözme hızı anlamına gelir
- Anahtar boyutu
  - Daha büyük anahtar boyutu, daha fazla güvenlik anlamına gelir, ancak şifreleme/şifre çözme hızlarını azaltabilir
- Tur sayısı
  - Feistel şifresinin özü, tek bir turun yetersiz güvenlik sunması, ancak birden fazla turun artan güvenlik sunmasıdır.
- Alt anahtar oluşturma algoritması
  - Bu algoritmadaki daha fazla karmaşıklık, kriptanalizin daha fazla zorluğuna yol açmalıdır.

Feistel Şifre Tasarım Özellikleri (2/2)

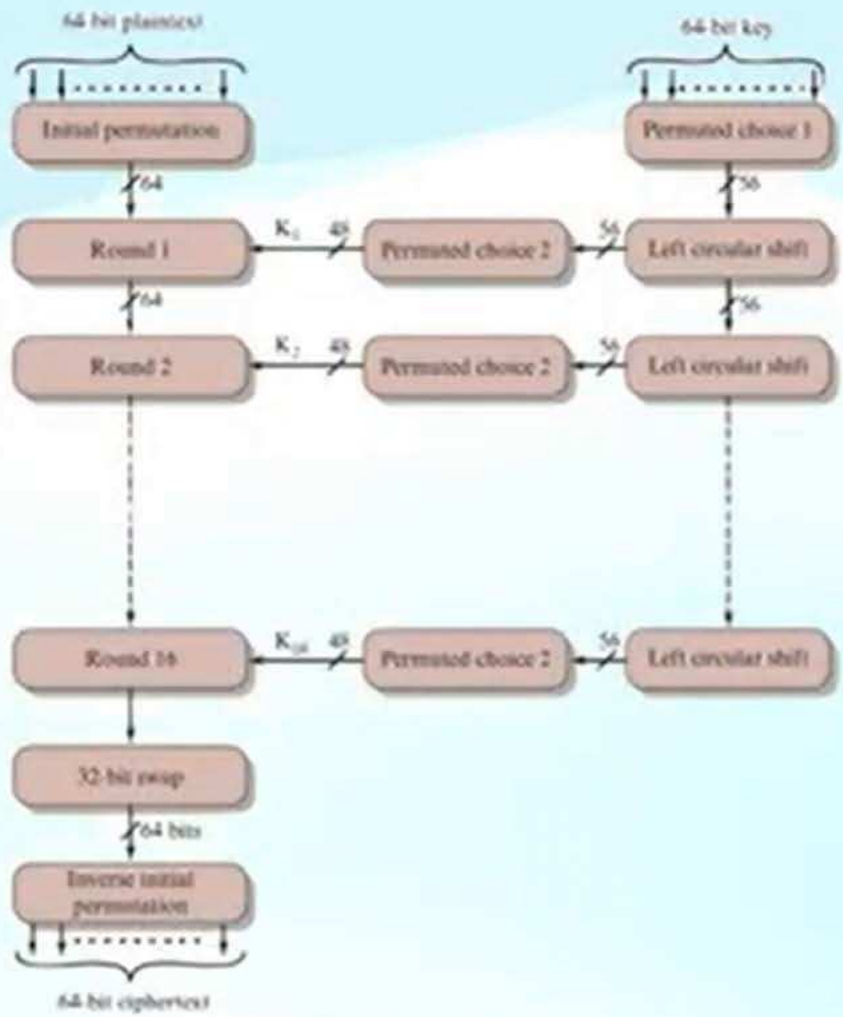
- F tur Fonksiyonu
  - Daha fazla karmaşıklık genellikle kriptanalize karşı daha fazla direnç anlamına gelir
- Hızlı yazılım şifreleme/şifre çözme
  - Çoğu durumda, şifreleme, bir donanım uygulamasını engelleyecek şekilde uygulamalara veya yardımcı program işlevlerine katıştırılır; Buna göre, algoritmanın yürütme hızı bir endişe haline gelir
- Analiz kolaylığı
  - Algoritma kısa ve net bir şekilde açıklanabilirse, bu algoritmayı kriptanalitik güvenlik açıkları için analiz etmek ve bu nedenle gücü konusunda daha yüksek bir güvence seviyesi geliştirmek daha kolaydır.

Feistel Örneği

Veri Şifreleme Standardı (DES)

- 1977 yılında Ulusal Standartlar Bürosu (şimdi NIST) tarafından Federal Bilgi İşleme Standardı 46 olarak yayınlanmıştır.
- 2001 yılında Gelişmiş Şifreleme Standardı'nın (AES) tanıtılmasına kadar en yaygın kullanılan şifreleme şemasıydı.
- Algoritmanın kendisi Veri Şifreleme Algoritması (DEA) olarak adlandırılır.
  - Veriler, 56 bit anahtar kullanılarak 64 bit bloklar halinde şifrelenir
  - Algoritma, 64 bit girişi bir dizi adımda 64 bit çıkışa dönüştürür
  - Şifrelemeyi tersine çevirmek için aynı anahtarla aynı adımlar kullanılır

Şekil 4.5 DES Şifreleme Algoritmasının Genel Tasviri



Tablo 4.2 DES Örneği

Round	*Ki*	*Li*	*Ri*
IP		5a005a00	3cf03c0f
1	1e030f03080d2930	3cf03c0f	bad22845
2	0a31293432242318	bad22845	99e9b723
3	23072318201d0c1d	99e9b723	0bae3b9e
4	05261d3824311a20	0bae3b9e	42415649
5	3325340136002c25	42415649	18b3fa41
6	123a2d0d04262a1c	18b3fa41	9616fe23
7	021f120b1c130611	9616fe23	67117cf2
8	1c10372a2832002b	67117cf2	c11bfc09
9	04292a380c341f03	c11bfc09	887fbc6c
10	2703212607280403	887fbc6c	600f7e8b
11	2826390c31261504	600f7e8b	f596506e
12	12071c241a0a0f08	f596506e	738538b8
13	300935393c0d100b	738538b8	c6a62c4e
14	311e09231321182a	c6a62c4e	56b0bd75
15	283d3e0227072528	56b0bd75	75e8fd8f
16	2921080b13143025	75e8fd8f	25896490
IP−1		da02ce3a	89ecac3b

Not: DES alt anahtarları, onaltılık biçimde sekiz adet 6 bitlik değer olarak gösterilir

Tablo 4.3 DES'te Çığ Etkisi: Düz Metindeki Değişim

Round		δ
	02468aceeca86420 12468aceeca86420	1
1	3cf03c0fbad22845 3cf03c0fbad32845	1
2	bad2284599e9b723 bad3284539a9b7a3	5
3	99e9b7230bae3b9e 39a9b7a3171cb8b3	18
4	0bae3b9e42415649 171cb8b3ccaca55e	34
5	4241564918b3fa41 ccaca55ed16c3653	37
6	18b3fa419616fe23 d16c3653cf402c68	33
7	9616fe2367117cf2 cf402c682b2cefbc	32
8	67117cf2c11bfc09 2b2cefbc99f91153	33

Round		δ
9	c11bfc09887fbc6c 99f911532eed7d94	32
10	887fbc6c600f7e8b 2eed7d94d0f23094	34
11	600f7e8bf596506e d0f23094455da9c4	37
12	f596506e738538b8 455da9c47f6e3cf3	31
13	738538b8c6a62c4e 7f6e3cf34bc1a8d9	29
14	c6a62c4e56b0bd75 4bc1a8d91e07d409	33
15	56b0bd7575e8fd8f 1e07d4091ce2e6dc	31
16	75e8fd8f25896490 1ce2e6dc365e5f59	32
IP-1	da02ce3a89ecac3b 057cde97d7683f2a	32

Tablo 4.4 DES'te Çığ Etkisi: Anahtardaki Değişim

Round		δ
	02468aceeca86420 02468aceeca86420	0
1	3cf03c0fbad22845 3cf03c0f9ad628c5	3
2	bad2284599e9b723 9ad628c59939136b	11
3	99e9b7230bae3b9e 9939136b768067b7	25
4	0bae3b9e42415649 768067b75a8807c5	29
5	4241564918b3fa41 5a8807c5488dbe94	26
6	18b3fa419616fe23 488dbe94aba7fe53	26
7	9616fe2367117cf2 aba7fe53177d21e4	27
8	67117cf2c11bfc09 177d21e4548f1de4	32

Round		δ
9	c11bfc09887fbc6c 548f1de471f64dfd	34
10	887fbc6c600f7e8b 71f64dfd4279876c	36
11	600f7e8bf596506e 4279876c399fdc0d	32
12	f596506e738538b8 399fdc0d6d208dbb	28
13	738538b8c6a62c4e 6d208dbbb9bdeeaa	33
14	c6a62c4e56b0bd75 b9bdeeaad2c3a56f	30
15	56b0bd7575e8fd8f d2c3a56f2765c1fb	33
16	75e8fd8f25896490 2765c1fb01263dc4	30
IP-1	da02ce3a89ecac3b ee92b50606b62b0b	30

Tablo 4.5 Kapsamlı Anahtar Arama için Gerekli Ortalama Süre

Anahtar Boyutu (bits)	Şifre	Alternatif Anahtar Sayısı	10^9 Şifre Çözmede/ sn'de Gerekli Süre	10^{12} Şifre Çözmede/ sn'de Gerekli Süre
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 Yıl	1 saat
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} Yıl	5.3×10^{17} Yıl
168	Üçlü DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} Yıl	5.8×10^{29} Yıl
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} Yıl	9.8×10^{36} Yıl
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} Yıl	1.8×10^{56} Yıl
26 karakterli (permütasyon)	Monoalfabetik	$2! = 4 \times 10^{26}$	2×10^{26} ns = 6.3×10^{9} Yıl	6.3×10^{6} Yıl

DES'in Gücü

- Zamanlama saldırıları
  - Belirli bir uygulamanın çeşitli şifreli metinlerde şifre çözme gerçekleştirmesinin ne kadar sürdüğünü gözlemleyerek anahtar veya düz metin hakkındaki bilgilerin elde edildiği bir sistem.
  - Bir şifreleme veya şifre çözme algoritmasının genellikle farklı girdilerde biraz farklı süreler aldığı gerçeğinden yararlanır
  - Şimdiye kadar, bu tekniğin DES'e veya üçlü DES ve AES gibi daha güçlü simetrik şifrelere karşı başarılı olması pek olası görünmüyor.

Blok Şifre Tasarım İlkeleri: Tur Sayısı

- Tur sayısı ne kadar fazlaysa kriptanaliz yapmak o kadar zor olur.
- Genel olarak kriter, tur sayısının, bilinen kriptanalitik çabaların basit bir kaba kuvvet anahtar arama saldırısından daha fazla çaba gerektirecek şekilde seçilmesi olmalıdır.
- DES'in 15 veya daha az turu olsaydı, diferansiyel kriptanaliz kaba kuvvet anahtar aramasından daha az çaba gerektirirdi.

Blok Şifre Tasarım İlkeleri: F Fonksiyonunun Tasarımı

- Feistel blok şifresinin kalbi F fonksiyonudur
- Doğrusal olmayan F ne kadar fazla olursa, herhangi bir kriptanaliz türü o kadar zor olacaktır.
- SAC ve BIC kriterleri, karışıklık fonksiyonunun etkinliğini güçlendiriyor gibi görünmektedir.

Algoritma iyi çığ özelliklerine sahip olmalıdır

- Katı çığ kriteri (KÇK) Strict avalanche criterion (SAC)
  - Bir S-kutusunun herhangi bir çıkış biti j'nin, tüm i, j için herhangi bir tek giriş biti ters çevrildiğinde, 1/2 olasılıkla değişmesi gerektiğini belirtir.
- Bit bağımsızlık kriteri (BBK) Bit independence criterion (BIC)
  - j ve k çıkış bitlerinin, tüm i, j ve k için herhangi bir i giriş biti ters çevrildiğinde bağımsız olarak değişmesi gerektiğini belirtir

Blok Şifre Tasarım İlkeleri: Anahtar Zamanlama Algoritması

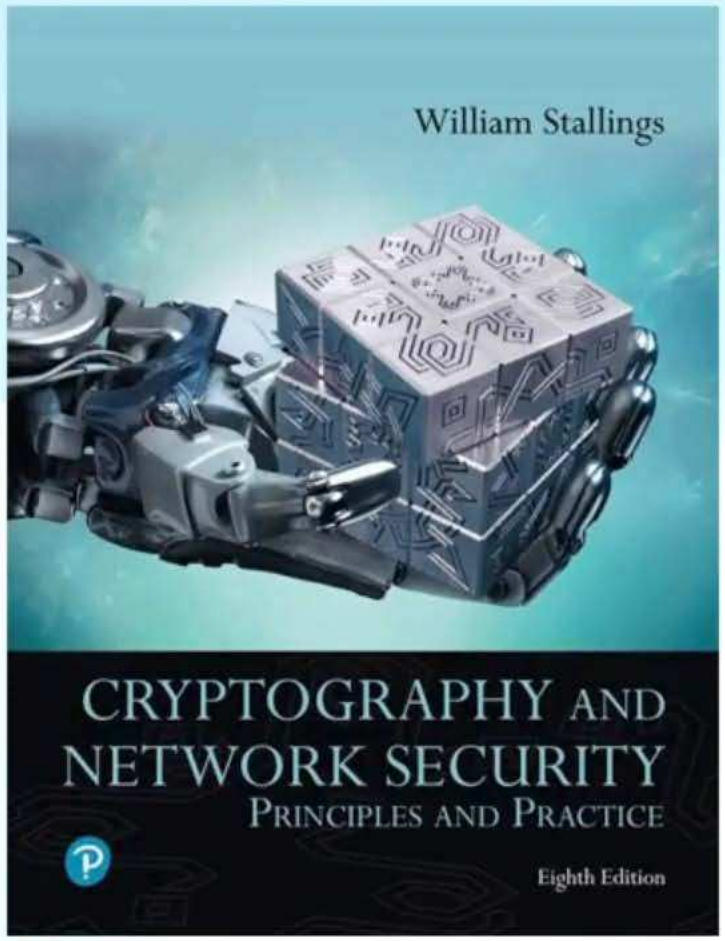
- Herhangi bir Feistel blok şifresiyle, anahtar, her tur için bir alt anahtar oluşturmada kullanılır
- Genel olarak, tek tek alt anahtarları çıkarmanın zorluğunu ve ana anahtara geri dönmenin zorluğunu en üst düzeye çıkarmak için alt anahtarları seçmek istiyoruz.
- En azından, anahtar zamanlamanın anahtar/şifreli metin Katı Çığ Kriteri ve Bit Bağımsızlığı Kriteri'ni garanti etmesi önerilmektedir.

Özet

- Çığ etkisi kavramını açıklar
- DES'in şifreleme gücünü tartışın
- Temel blok şifre tasarım ilkelerini özetleyin
- Akış şifreleri ve blok şifreler arasındaki ayrımı anlama
- Feistel şifresine genel bir bakış sunun ve şifre çözmenin şifrelemenin tersi olduğunu açıklayın
- Veri Şifreleme Standardı'na (DES) genel bir bakış sunun

Kriptografi ve Ağ Güvenliği: İlkeler ve Uygulamalar

Sekizinci Baskı



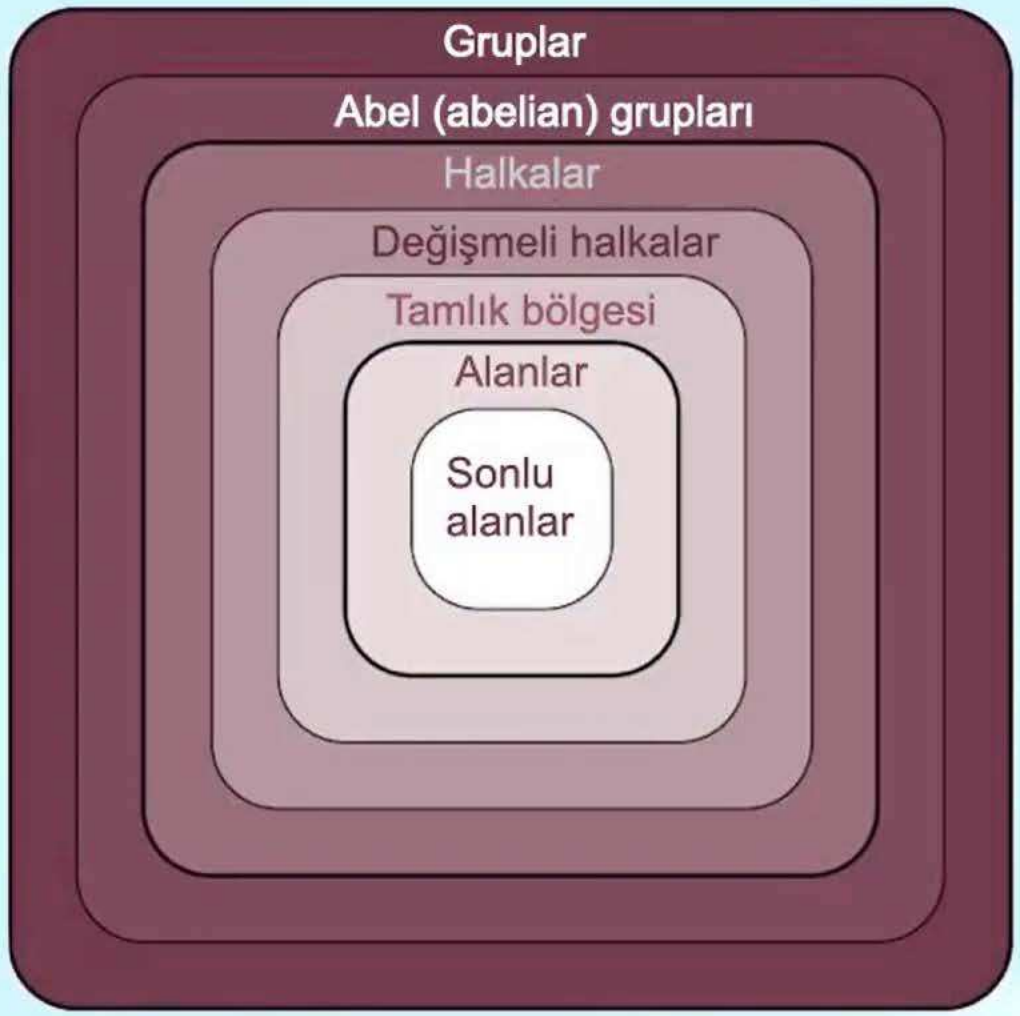
Bölüm 5

Sonlu Alanlar

Pearson

Telif Hakkı © 2020 Pearson Education, Inc. Tüm Hakları Saklıdır.

Şekil 5.1 Gruplar, Halkalar ve Alanlar



Gruplar

- "•" ile gösterilen ikili bir işlem kümesi, G'deki elemanların her sıralı çiftine (a,b) G'deki bir elemanı $(a \bullet b)$ ilişkilendirir, böylece aşağıdaki aksiyomlara uyulur::
  - **(A1) Kapsama:**
    - Eğer a ve b G'ye aitse, o zaman $a \bullet b$ de G'dedir.
  - **(A2) Birleşme:**
    - $a \bullet (b \bullet c) = (a \bullet b) \bullet c$; G 'deki tüm a, b, c için
  - **(A3) Birim öğe (etkisiz eleman):**
    - G'de bir e elemanı vardır, öyle ki G'deki tüm a için $a \bullet e = e \bullet a = a$ vardır.
  - **(A4) Ters eleman:**
    - G'deki her a için, G'de $a \bullet a^1 = a^1 \bullet a = e$ olacak şekilde bir a^1 öğesi vardır.
  - **(A5) Değişme:**
    - $a \bullet b = b \bullet a$, G'deki tüm a, b için.

Döngüsel Grup

- Üs alma, bir grup içinde grup operatörünün tekrarlanan bir uygulaması olarak tanımlanır, dolayısıyla,

$$a^3 = a \bullet a \bullet a$$

- $a^0 = e$'yi birim elemanı olarak ve $a^{-n} = (a')^n$ olarak tanımlarız, burada a', grup içindeki a'nın ters elemanıdır.
- G'nin her elemanı, sabit bir a € G öğesinin a^k (k bir tamsayıdır) kuvveti ise, bir G grubu **döngüseldir**.
- a elemanının G grubunu **oluşturduğu** veya G'nin bir **üreteç** olduğu söylenir.
- Döngüsel bir grup her zaman değişmeli ve sonlu / sonsuz olabilir

Halkalar (1/3)

- Bazen $\{R , + , * \}$ ile gösterilen bir **halka** R, ***toplama*** ve ***çarpma*** adı verilen iki ikili işleme sahip bir elemanlar kümesidir, böylece tüm a, b , c in için aşağıdaki aksiyomlara uyulur:

(A1–A5)

R, toplamaya göre bir değişmeli gruptur; yani R, A1'den A5'e kadar olan aksiyomları karşılar. Toplama grubu durumunda, birim öğesini 0 olarak ve a'nın tersini $-a$ olarak gösteririz.

Halkalar (2/3)

(M1) Çarpma altında kapsama:

– a ve b R'ye aitse, ab da R'dedir

(M2) Çarpmanın birleştirilebilirliği:

– $a\,(bc) = (ab)c$ R'deki tüm a, b, c için

(M3) Dağılım yasaları:

– $a\,(b + c) = ab + ac$ R'deki tüm a, b, c için

– $(a + b)c = ac + bc$, R'deki tüm a, b, c için

- Özünde halka, kümeden çıkmadan toplama, çıkarma $[a - b = a + (-b)]$ ve çarpma işlemlerini yapabildiğimiz bir kümedir.

Halkalar (3 / 3)

- Aşağıdaki ek koşulu sağlıyorsa, bir halkanın değişmeli olduğu söylenir:

(M4) Çarpmanın değiştirilebilirliği:

$ab = ba$, R'deki tüm a, b için

Bir integral alanı, aşağıdaki aksiyomlara uyan değişmeli bir halkadır.

(M5) Çarpımsal özdeşlik:

R'de, R'deki tüm a için $a1 = 1a = a$ olacak şekilde bir eleman 1 vardır.

(M6) Sıfır bölen yok:

R'de a, b ve $ab = 0$ ise, o zaman $a = 0$ veya $b = 0$

Alanlar

- Bazen {F, +,* } ile gösterilen F **alanı**, ***toplama*** ve ***çarpma*** adı verilen iki ikili işleme sahip bir elemanlar kümesidir, böylece F'deki tüm *a, b, c* için aşağıdaki aksiyomlara uyulur:

  (A1–M6)

  F bir tam bölgedir; yani *F*, A1'den A5'e ve M1'den M6'ya kadar olan aksiyomları karşılar

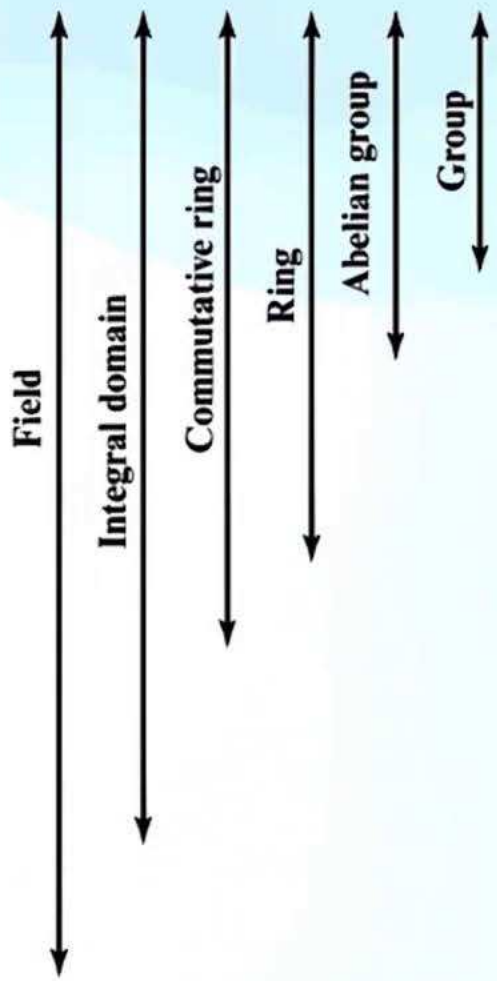
  (M7) Çarpımsal ters:

  F'deki her a için, 0 hariç, *F*'de $aa^{-1} = (a^{-1})a = 1$ olacak şekilde bir a^{-1} öğesi vardır.

- Özünde alan, kümeden ayrılmadan toplama, çıkarma, çarpma ve bölme işlemlerini yapabildiğimiz bir kümedir. Bölme şu kuralla tanımlanır: $a/b = a\,(b^{-1})$

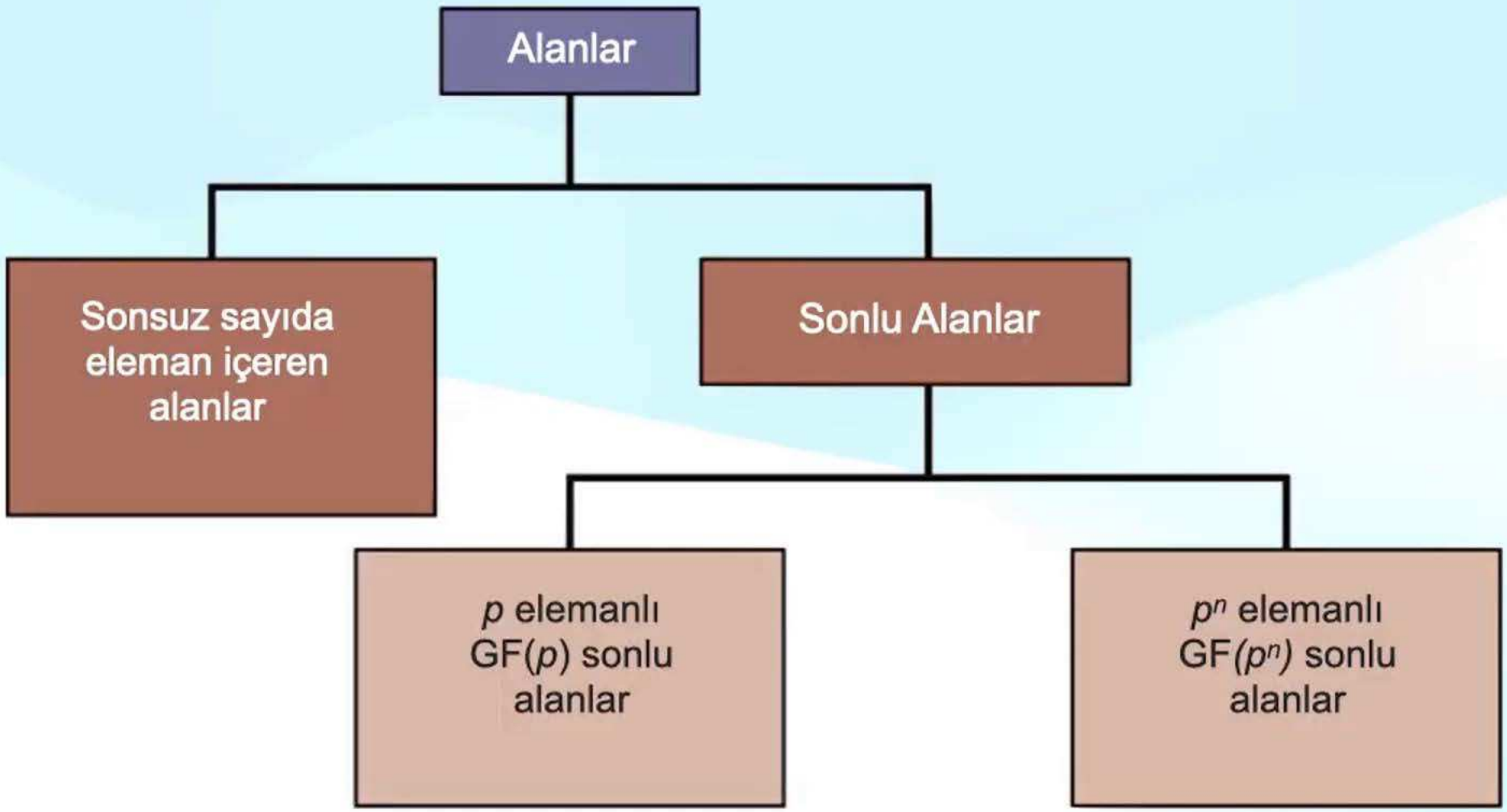
Bilinen alan örnekleri, ***rasyonel sayılar, gerçek sayılar*** *ve* ***karmaşık sayılardır***. *Tüm tam sayıların kümesinin bir alan olmadığına dikkat edin*, çünkü kümenin her öğesinin çarpımsal bir tersi yoktur.

Şekil 5.2 Grupların, Halkaların ve Alanların Özellikleri



(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Şekil 5.3 Alan Türleri



$GF(p)$ Formunun Sonlu Alanları

- Sonlu alanlar birçok şifreleme algoritmasında çok önemli bir rol oynar
- Sonlu bir alanın sırasının, n'nin pozitif bir tamsayı olduğu bir asal p^n'nin kuvveti olması gerektiği gösterilebilir.
  - p^n sırasının sonlu alanı genellikle $GF(p^n)$ olarak yazılır.
  - GF, sonlu alanları ilk kez inceleyen matematikçinin onuruna Galois alanını temsil eder.

Tablo 5.1 Aritmetik Modulo 8 ve Modulo 7(1/6)

(a) Toplama modül 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Tablo 5.1 Aritmetik Modulo 8 ve Modulo 7 (2/6)

(b) Çarpma modülü 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Tablo 5.1 Aritmetik Modulo 8 ve Modulo 7 (3/6)

(c) Toplamsal ve çarpımsal tersler modulo 8

w	0	1	2	3	4	5	6	7
$-w$	0	7	6	5	4	3	2	1
w^{-1}	—	1	—	3	—	5	—	7

Tablo 5.1 Aritmetik Modulo 8 ve Modulo 7 (4/6)

(d) Toplama modül 7

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Tablo 5.1 Aritmetik Modulo 8 ve Modulo 7 (5/6)

(e) Çarpma modülü 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Tablo 5.1 Aritmetik Modulo 8 ve Modulo 7 (6/6)

(f) Toplamsal ve çarpımsal tersler modulo 7

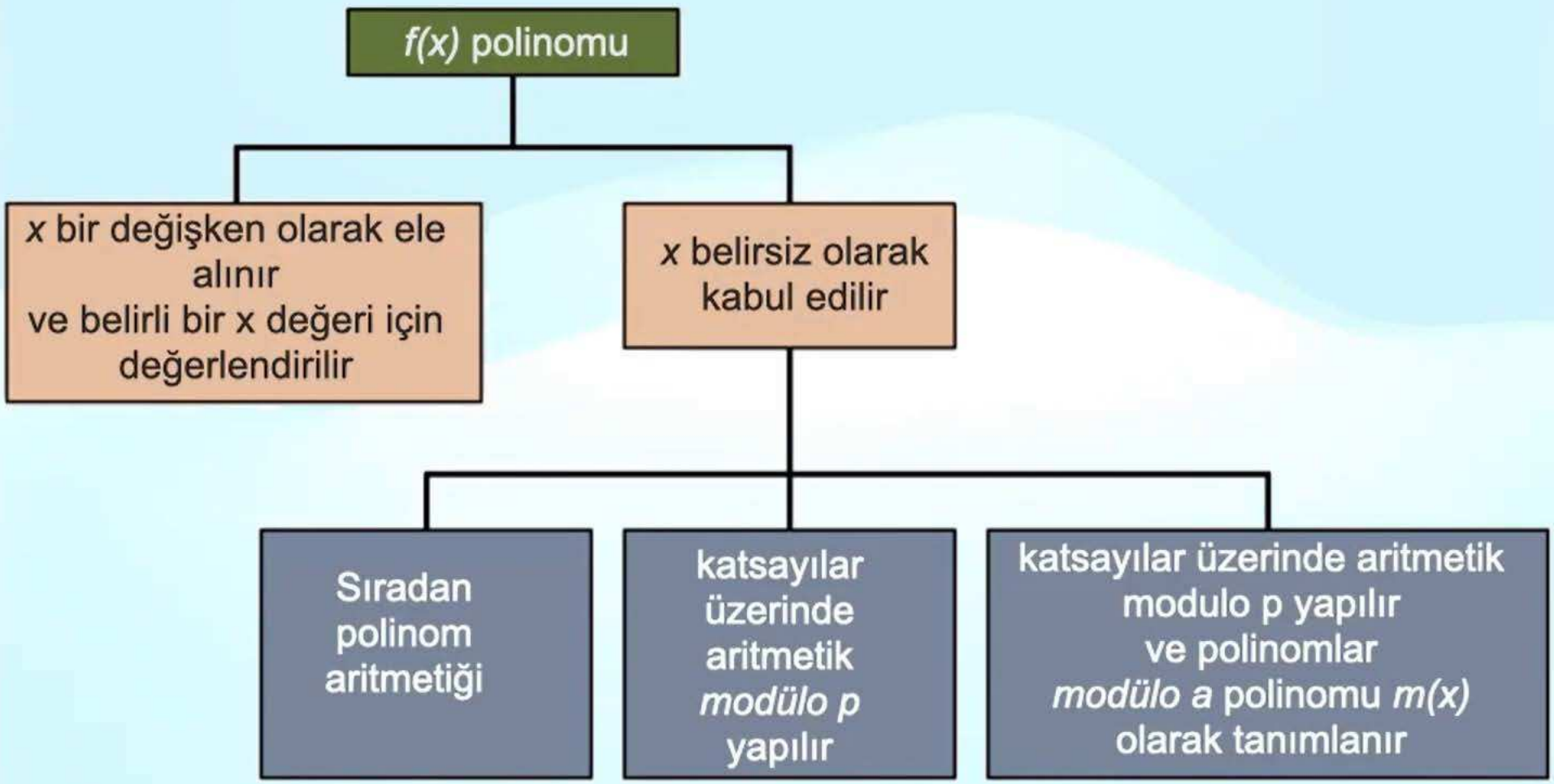
w	0	1	2	3	4	5	6
$-w$	0	6	5	4	3	2	1
w^{-1}	—	1	4	5	2	3	6

Bu bölümde, *p*'nin asal olduğu, *p* mertebesinden sonlu bir alanın nasıl oluşturulacağını gösterdik.

GF(p) aşağıdaki özelliklerle tanımlanır:

- 1. *GF(p)* *p* elemanlarından oluşur
- 2. + ve * ikili işlemleri set üzerinde tanımlanır. Toplama, çıkarma, çarpma ve bölme işlemleri kümeden ayrılmadan gerçekleştirilebilir. Kümenin 0 dışındaki her elemanının çarpımsal bir tersi vardır
- *GF(p)* elemanlarının $\{0, 1, \ldots, p-1\}$ tamsayıları olduğunu ve aritmetik işlemlerin toplama ve çarpma modu *p* olduğunu gösterdik.

Şekil 5.4 Polinom Aritmetiği



Şekil 5.5 Polinom Aritmetiğine Örnekler

$$
\begin{array}{rrrr}
x^3 & +x^2 & & +2 \\
+ & (x^2 & -x & +1) \\
\hline
x^3 & +2x^2 & -x & +3
\end{array}
$$

(a) Addition

$$
\begin{array}{rrrr}
x^3 & +x^2 & & +2 \\
- & (x^2 & -x & +1) \\
\hline
x^3 & & +x & +1
\end{array}
$$

(b) Subtraction

$$
\begin{array}{rrrrrr}
 & & x^3 & +x^2 & & +2 \\
 & & \times & (x^2 & -x & +1) \\
\hline
 & & x^3 & +x^2 & & +2 \\
 & -x^4 & -x^3 & & -2x & \\
x^5 & +x^4 & & +2x^2 & & \\
\hline
x^5 & & & +3x^2 & -2x & +2
\end{array}
$$

(c) Multiplication

$$
\begin{array}{r|rrrr}
 & & x & +2 & \\
\hline
x^2-x+1 & x^3 & +x^2 & & +2 \\
 & x^3 & -x^2 & +x & \\
\hline
 & & 2x^2 & -x & +2 \\
 & & 2x^2 & -2x & +2 \\
\hline
 & & & x &
\end{array}
$$

(d) Division

Z_p Katsayılı Polinom Aritmetiği

- Her farklı polinom, kümenin bir elemanı olarak kabul edilirse, bu küme bir halkadır.
- Bir alan içerisinde polinomlar üzerinde polinom aritmetiği yapıldığında, bölme işlemi mümkündür.
  - Not: Bu *kesin bölünmenin* mümkün olduğu anlamına gelmez.
- Alan olmayan bir katsayı kümesi üzerinden polinom bölme işlemi yapmaya çalışırsak, bölmenin *her zaman* tanımlı olmadığını görürüz.
  - Katsayı kümesi bir alan olsa bile, polinom bölümü mutlaka *kesin* değildir.
  - Kalanlara izin verildiği varsayımıyla, katsayı kümesi bir alan ise polinom bölmenin mümkün olduğunu söyleyebiliriz.

Polinom Bölümü

- Herhangi bir polinomu şu şekilde yazabiliriz:

$$f(x) = q(x)\, g(x) + r(x)$$

  - $r(x)$ kalan olarak yorumlanabilir
  - Yani $r(x) = f(x) \bmod g(x)$
- Eğer kalan <u>*yoksa*</u>, $g(x)$'in $f(x)$'i **böldüğünü** söyleyebiliriz.
  - $g(x) \mid f(x)$ şeklinde yazılır
  - $g(x)$'in $f(x)$'in bir **çarpanı** olduğunu söyleyebiliriz.
  - Veya $g(x)$, $f(x)$'in **bölenidir**.
- Bir F alanı üzerindeki bir $f(x)$ polinomu, ancak ve ancak $f(x)$, her ikisi de F üzerinde ve her ikisi de $f(x)$'in derecesinden daha düşük olan iki polinomun çarpımı olarak ifade edilemiyorsa **indirgenemez** olarak adlandırılır.
  - İndirgenemez bir polinom aynı zamanda **asal polinom** olarak da adlandırılır.

GF(2) Üzerinden Polinom Aritmetiği Örneği (1/2)

(a) Toplama

$$
\begin{array}{llll}
x^7 & +x^5 + x^4 + x^3 & & + x + 1 \\
 & & + (x^3 & + x + 1\ ) \\
\hline
x^7 & +x^5 + x^4 & &
\end{array}
$$

(b) Çıkarma

$$
\begin{array}{llll}
x^7 & +x^5 + x^4 + x^3 & & + x + 1 \\
 & & -(x^3 & + x + 1\ ) \\
\hline
x^7 & +x^5 + x^4 & &
\end{array}
$$

GF(2) Üzerinden Polinom Aritmetiği Örneği (2/2)

(c) Çarpma

$$
\begin{array}{rrrrrrrrrrr}
 & & & x^7 & & +x^5 & +x^4 & +x^3 & & +x & +1 \\
 & & & & & & & \times(x^3 & & +x & +1) \\
\hline
 & & & x^7 & & +x^5 & +x^4 & +x^3 & & +x & +1 \\
 & & x^8 & & +x^6 & +x^5 & +x^4 & & +x^2 & +x & \\
x^{10} & & +x^8 & +x^7 & +x^6 & & +x^4 & +x^3 & & & \\
\hline
x^{10} & & & & & & +x^4 & & +x^2 & & +1
\end{array}
$$

(d) Bölme

$$
\begin{array}{r|rrrrrrrr}
 & x^4 & +1 & & & & & & \\
\hline
x^3+x+1 & x^7 & & +x^5 & +x^4 & +x^3 & & +x & +1 \\
 & x^7 & & +x^5 & +x^4 & & & & \\
\cline{2-5}
 & & & & & x^3 & & +x & +1 \\
 & & & & & x^3 & & +x & +1 \\
\cline{5-9}
\end{array}
$$

Polinom En Büyük Ortak Bölen (OBEB)

- Aşağıdakiler doğruysa, *c(x)* polinomunun *a(x)* ve *b(x)* 'in en büyük ortak böleni olduğu söylenir:
  - *c(x)* hem *a(x)*'i hem de *b(x)*'i böler
  - *a(x)* ve *b(x)*'in herhangi bir böleni, *c(x)*'in bölenidir
- Eşdeğer bir tanım şudur:
  - ebob[*a(x), b(x)*] hem *a(x)*'i hem de *b(x)*'i bölen <u>maksimum</u> dereceli polinomdur
- Öklid algoritması, katsayıları bir alanın elemanları olan iki polinomun en büyük ortak bölenini bulmak için genişletilebilir.

Tablo 5.2 GF(2^3)'te Aritmetik (1/3)

(a) Toplama

		000	001	010	011	100	101	110	111
	+	0	1	2	3	4	5	6	7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

Tablo 5.2 GF(2^3)'te Aritmetik (2/3)

(b) Çarpma

		000	001	010	011	100	101	110	111
	×	0	1	2	3	4	5	6	7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	7	5
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

Tablo 5.2 GF(2^3)'te Aritmetik (3/3)

(c) Toplamsal ve çarpımsal tersler

w	$-w$	w^{-1}
0	0	–
1	1	1
2	2	5
3	3	6
4	4	7
5	5	2
6	6	3
7	7	4

Tablo 5.3 Polinom Aritmetik Modulo ($x^3 + x + 1$) (1/2)

(a) Toplama

		000	001	010	011	100	101	110	111
	+	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
000	0	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
001	1	1	0	$x + 1$	x	$x^2 + 1$	x^2	$x^2 + x + 1$	$x^2 + x$
010	x	x	$x + 1$	0	1	$x^2 + x$	$x^2 + x + 1$	x^2	$x^2 + 1$
011	$x + 1$	$x + 1$	x	1	0	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	x^2
100	x^2	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$	0	1	x	$x + 1$
101	$x^2 + 1$	$x^2 + 1$	x^2	$x^2 + x + 1$	$x^2 + x$	1	0	$x + 1$	x
110	$x^2 + x$	$x^2 + x$	$x^2 + x + 1$	x^2	$x^2 + 1$	x	$x + 1$	0	1
111	$x^2 + x + 1$	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	x^2	$x + 1$	x	1	0

Tablo 5.3 Polinom Aritmetik Modulo ($x^3 + x + 1$) (2/2)

(b) Çarpma

		000	001	010	011	100	101	110	111
	$\times$	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
010	x	0	x	x^2	$x^2 + x$	$x + 1$	1	$x^2 + x + 1$	$x^2 + 1$
011	$x + 1$	0	$x + 1$	$x^2 + x$	$x^2 + 1$	$x^2 + x + 1$	x^2	1	x
100	x^2	0	x^2	$x + 1$	$x^2 + x + 1$	$x^2 + x$	x	$x^2 + 1$	1
101	$x^2 + 1$	0	$x^2 + 1$	1	x^2	x	$x^2 + x + 1$	$x + 1$	$x^2 + x$
110	$x^2 + x$	0	$x^2 + x$	$x^2 + x + 1$	1	$x^2 + 1$	$x + 1$	x	x^2
111	$x^2 + x + 1$	0	$x^2 + x + 1$	$x^2 + 1$	x	1	$x^2 + 1$	x^2	$x + 1$

Tablo 5.4 Genişletilmiş Öklid $[(x^8 + x^4 + x^3 + x + 1), (x^7 + x + 1)]$

(Tablo 5.4 ders kitabının 138. sayfasında bulunabilir)

Başlangıç	$a(x) = x^8 + x^4 + x^3 + x + 1$; $v_{-1}(x) = 1$; $w_{-1}(x) = 0$ $b(x) = x^7 + x + 1$; $v_0(x) = 0$; $w_0(x) = 1$
İterasyon 1	$q_1(x) = x$; $r_1(x) = x^4 + x^3 + x^2 + 1$ $v_1(x) = 1$; $w_1(x) = x$
İterasyon 2	$q_2(x) = x^3 + x^2 + 1$; $r_2(x) = x$ $v_2(x) = x^3 + x^2 + 1$; $w_2(x) = x^4 + x^3 + x + 1$
İterasyon 3	$q_3(x) = x^3 + x^2 + x$; $r_3(x) = 1$ $v_3(x) = x^6 + x^2 + x + 1$; $w_3(x) = x^7$
İterasyon 4	$q_4(x) = x$; $r_4(x) = 0$ $v_4(x) = x^7 + x + 1$; $w_4(x) = x^8 + x^4 + x3 + x + 1$
Sonuç	$d(x) = r_3(x) = \gcd(a(x), b(x)) = 1$ $w(x) = w_3(x) = (x^7 + x + 1)^{-1} \bmod (x^8 + x^4 + x^3 + x + 1) = x^7$

Hesaplamalı Hususlar

- Katsayılar 0 veya 1 olduğundan, bit dizesi gibi herhangi bir polinomu temsil edebilirler.
- Toplama, bu bit dizelerinin XOR'u olur
- Çarpma kaydırma ve XOR'dur
  - cf uzun çarpma yöntemi
- Modulo indirgeme, en yüksek kuvveti tekrar tekrar indirgenemez polinomun geri kalanıyla değiştirerek yapılır (ayrıca kaydırma ve XOR)

Üreteç Kullanma

- q mertebesinden sonlu bir F alanının g **üreteci** (q eleman içerir), ilk $q-1$ kuvvetleri F'nin sıfır olmayan tüm elemanlarını oluşturan bir elemandır.
  - F'nin elemanları 0, g^0, g^1, ..., g^{q-2}'den oluşur
- Bir polinom $f(x)$ tarafından tanımlanan bir F alanını düşünün
  - F'de bulunan bir b elemanına, eğer $f(b) = 0$ ise, polinomun **kökü** denir.
- Son olarak, indirgenemez bir polinomun kök g'sinin, bu polinom üzerinde tanımlanan sonlu alanın bir *üreteci* olduğu gösterilebilir.

Tablo 5.5 $x^3 + x + 1$ kullanarak $GF(2^3)$ için Üreteç

Güç Gösterimi	Polinom Gösterimi	İkili Gösterim	Ondalık (Hex) Gösterimi
0	0	000	0
$g^0 (= g7)$	1	001	1
g^1	g	010	2
g^2	g^2	100	4
g^3	$g + 1$	011	3
g^4	$g^2 + g$	110	6
g^5	$g^2 + g + 1$	111	7
g^6	$g^2 + 1$	101	5

Tablo 5.6 GF(2^3) Polinom için Üreteç Kullanan Aritmetik ($x^3 + x + 1$) (1/2)

(a) Toplama

		000	001	010	100	011	110	111	101
	+	0	1	g	g^2	g^3	g^4	g^5	g^6
000	0	0	1	g	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$
001	1	1	0	$g + 1$	$g^2 + 1$	g	$g^2 + g + 1$	$g^2 + g$	g^2
010	g	g	$g + 1$	0	$g^2 + g$	1	g^2	$g^2 + 1$	$g^2 + g + 1$
100	g^2	g^2	$g^2 + 1$	$g^2 + g$	0	$g^2 + g + 1$	g	$g + 1$	1
011	g^3	$g + 1$	g	1	$g^2 + g + 1$	0	$g^2 + 1$	g^2	$g^2 + g$
110	g^4	$g^2 + g$	$g^2 + g + 1$	g^2	g	$g^2 + 1$	0	1	$g + 1$
111	g^5	$g^2 + g + 1$	$g^2 + g$	$g^2 + 1$	$g + 1$	g^2	1	0	g
101	g^6	$g^2 + 1$	g^2	$g^2 + g + 1$	1	$g^2 + g$	$g + 1$	g	0

Tablo 5.6 GF(2^3) Polinom için Üreteç Kullanan Aritmetik ($x^3 + x + 1$) (2/2)

(b) Çarpma

		000	001	010	100	011	110	111	101
	×	0	1	g	g^2	g^3	g^4	g^5	g^6
000	0	0	0	0	0	0	0	0	0
001	1	0	1	g	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$
010	g	0	g	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$	1
100	g^2	0	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$	1	g
011	g^3	0	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$	1	g	g^2
110	g^4	0	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$	1	g	g^2	$g + 1$
111	g^5	0	$g^2 + g + 1$	$g^2 + 1$	1	g	g^2	$g + 1$	$g^2 + g$
101	g^6	0	$g^2 + 1$	1	g	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$

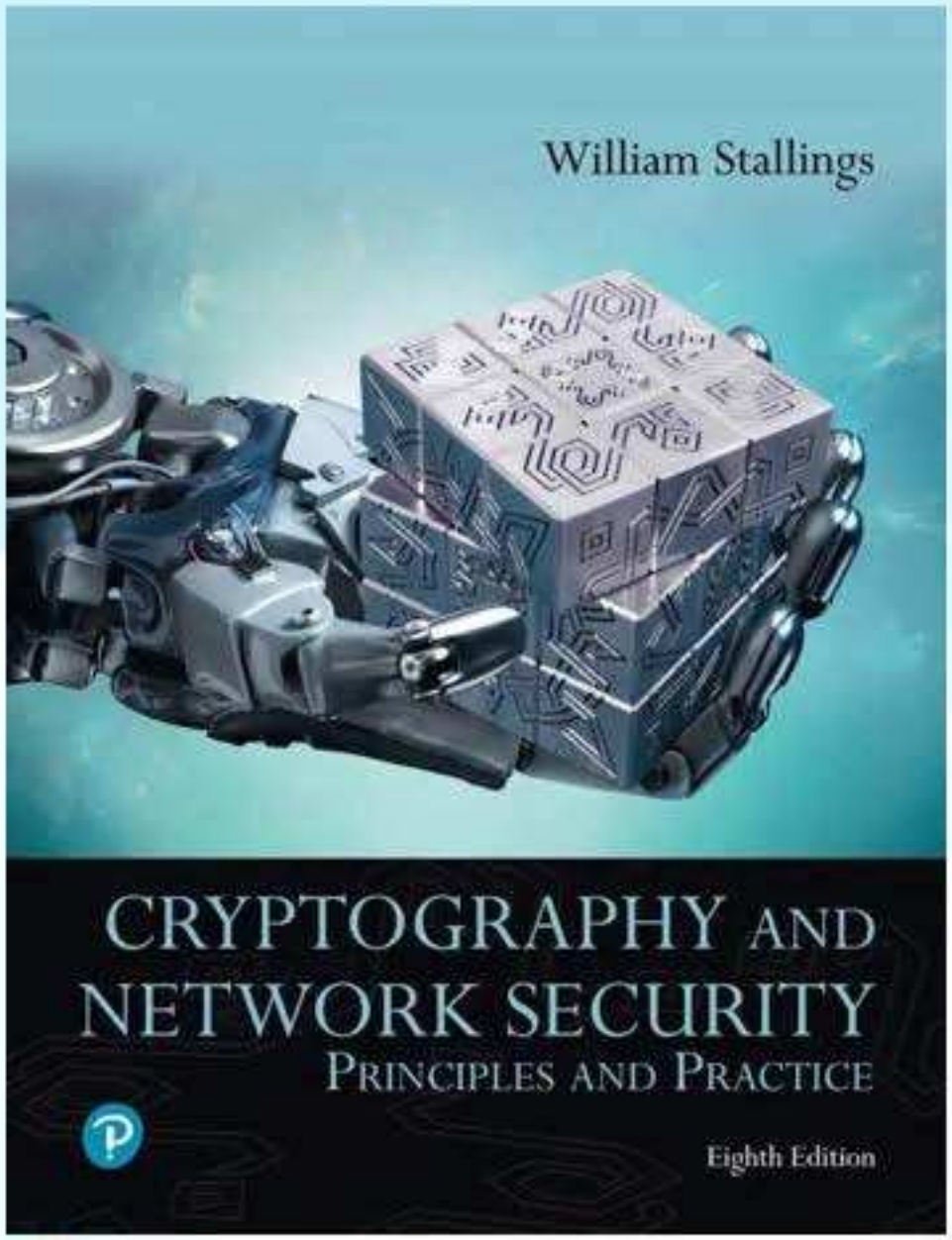
Özet

- Gruplar, halkalar ve alanlar arasında ayrım yapma
- GF(p) formunun sonlu alanlarını tanımlayın
- GF(2^n) formunun sonlu alanlarını tanımlayın
- Sıradan polinom aritmetiği, Z_p katsayılarla polinom aritmetik ve GF(2^n)'deki modüler polinom aritmetiği arasındaki farkları açıklar

Mod operatörünün iki farklı kullanımını açıklayın

Kriptografi ve Ağ Güvenliği: İlkeler ve Uygulamalar

Sekizinci Baskı



Bölüm 6

Gelişmiş Şifreleme Standardı

Pearson

Telif Hakkı © 2020 Pearson Education, Inc. Tüm Hakları Saklıdır.

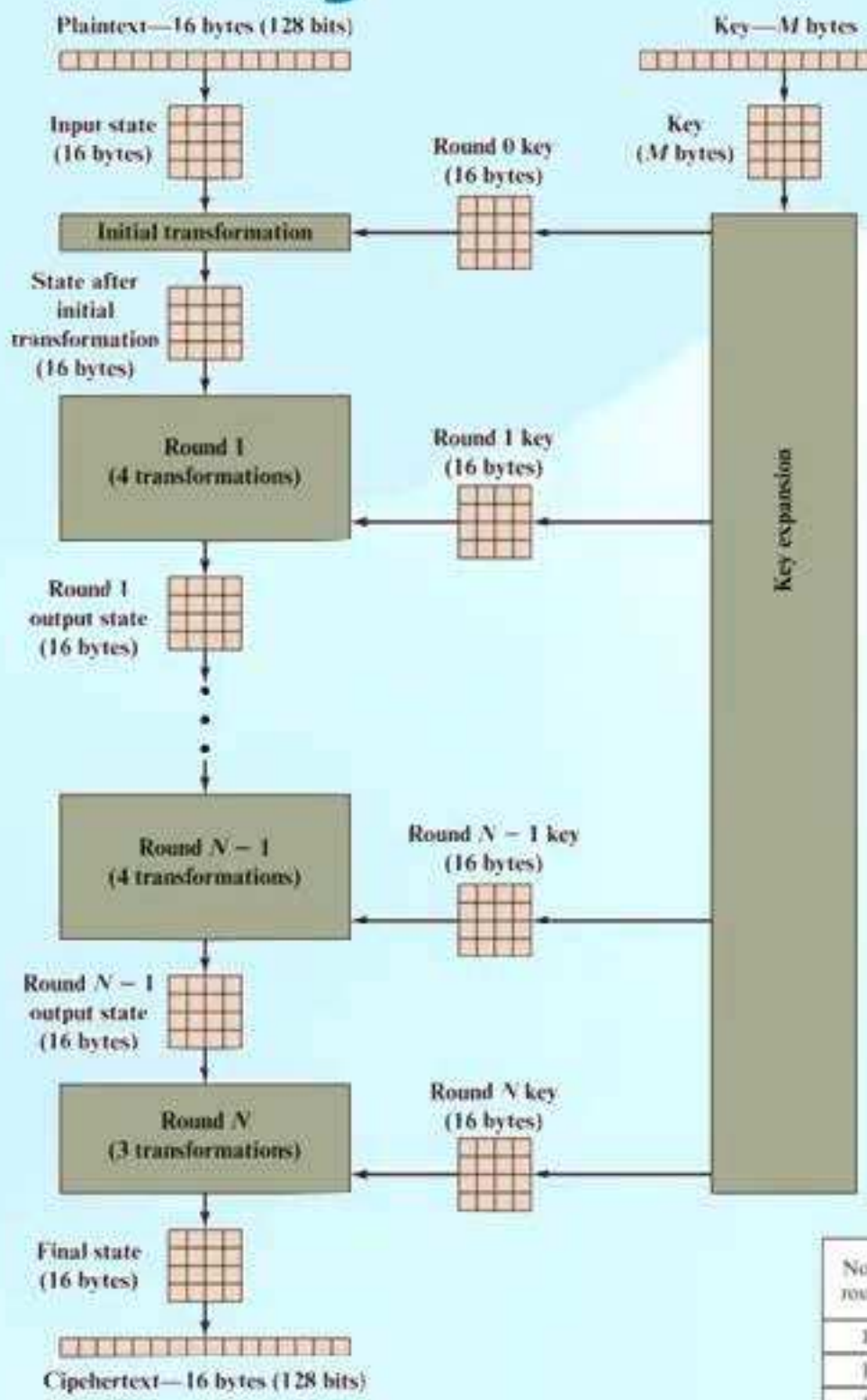
Sonlu Alan Aritmetiği (1/2)

- Gelişmiş Şifreleme Standardında (AES) tüm işlemler 8 bitlik baytlarda gerçekleştirilir
- Toplama, çarpma ve bölme aritmetik işlemleri sonlu alan $GF(2^8)$ üzerinde gerçekleştirilir.
- Alan, kümeden ayrılmadan toplama, çıkarma, çarpma ve bölme yapabildiğimiz bir kümedir.
- Bölme aşağıdaki kuralla tanımlanır:
  - $a/b = a\ (b^{-1})$
- Sonlu bir alana bir örnek (sonlu sayıda elemana sahip olan), tüm tamsayılardan oluşan Z_p kümesidir $\{0, 1, \ldots\ldots, p - 1\}$, burada p bir asal sayıdır ve aritmetik *modülo p*

Sonlu Alan Aritmetiği (2/2)

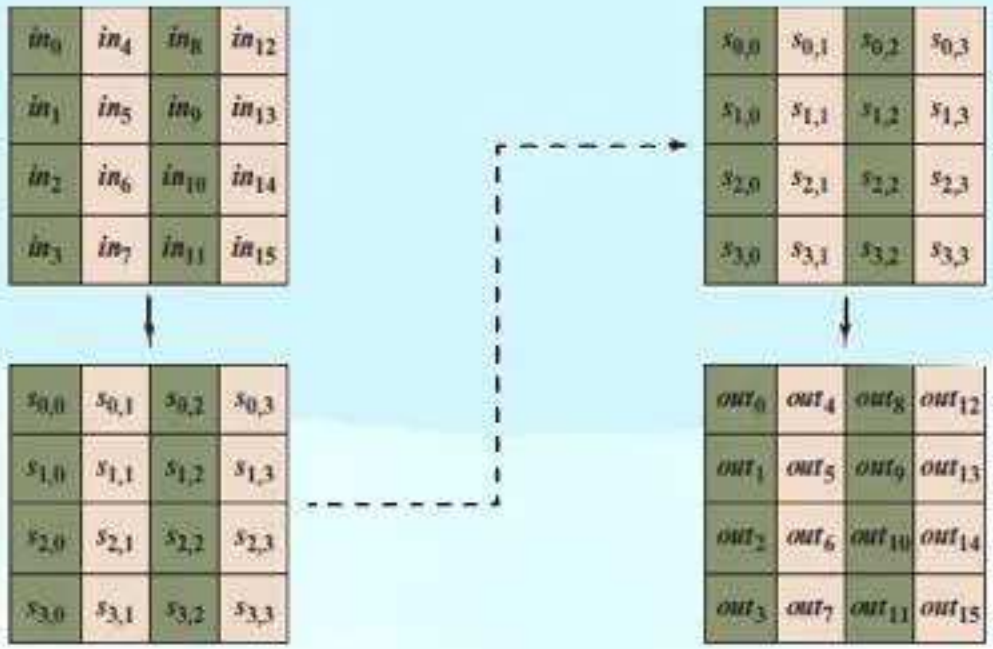
- Algoritmada kullanılan işlemlerden biri bölme ise o zaman bir alan üzerinden tanımlı aritmetik çalışmamız gerekir.
  - Bölme, sıfır olmayan her elemanın çarpımsal bir tersi olmasını gerektirir
- Kolaylık ve uygulama verimliliği için, boşa giden bit kalıpları olmadan belirli sayıda bit'e tam olarak uyan tamsayılarla çalışmak istiyoruz.
  - *0* ile 2^n-1 aralığındaki, n bitlik bir kelimeye uyan tamsayılar
- Modüler aritmetik kullanan Z_{2^n} gibi tamsayıların kümesi bir alan değildir
  - Örneğin, 2 tamsayısının Z_{2^n}'de çarpımsal tersi yoktur, yani *b* tamsayı yoktur, öyle ki `2b mod 2^n = 1`
- 2^n öğe içeren sonlu bir alan, $GF(2^n)$ olarak adlandırılır.
  - $GF(2^n)$'deki her polinom, `n-bit`lik bir sayı ile temsil edilebilir.

Şekil 6.1 AES Şifreleme İşlemi



No. of rounds	Key Length (bytes)
10	16
12	24
14	32

Şekil 6.2 AES Veri Yapıları



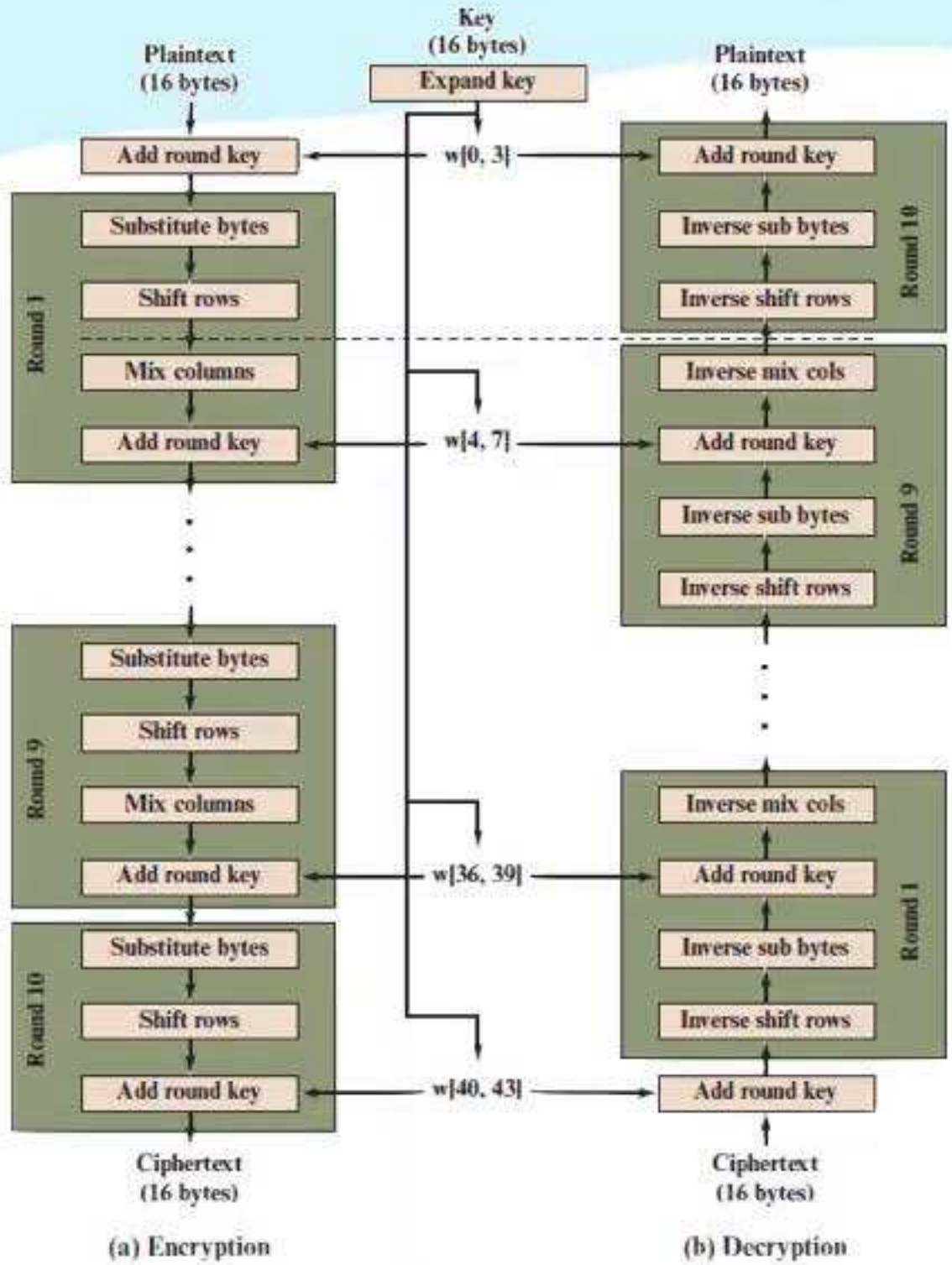
(a) Input, state array, and output

(b) Key and expanded key

Tablo 6.1 AES Parametreleri

Anahtar Boyutu (kelime/bayt/bit)	4/16/128	6/24/192	8/32/256
Şifresiz Metin Blok Boyutu (kelime/bayt/bit)	4/16/128	4/16/128	4/16/128
Tur Sayısı	10	12	14
Tur Anahtar Boyutu (kelime/bayt/bit)	4/16/128	4/16/128	4/16/128
Genişletilmiş Anahtar Boyutu (kelime/bayt)	44/176	52/208	60/240

Şekil 6.3 AES Şifreleme ve Şifre Çözme



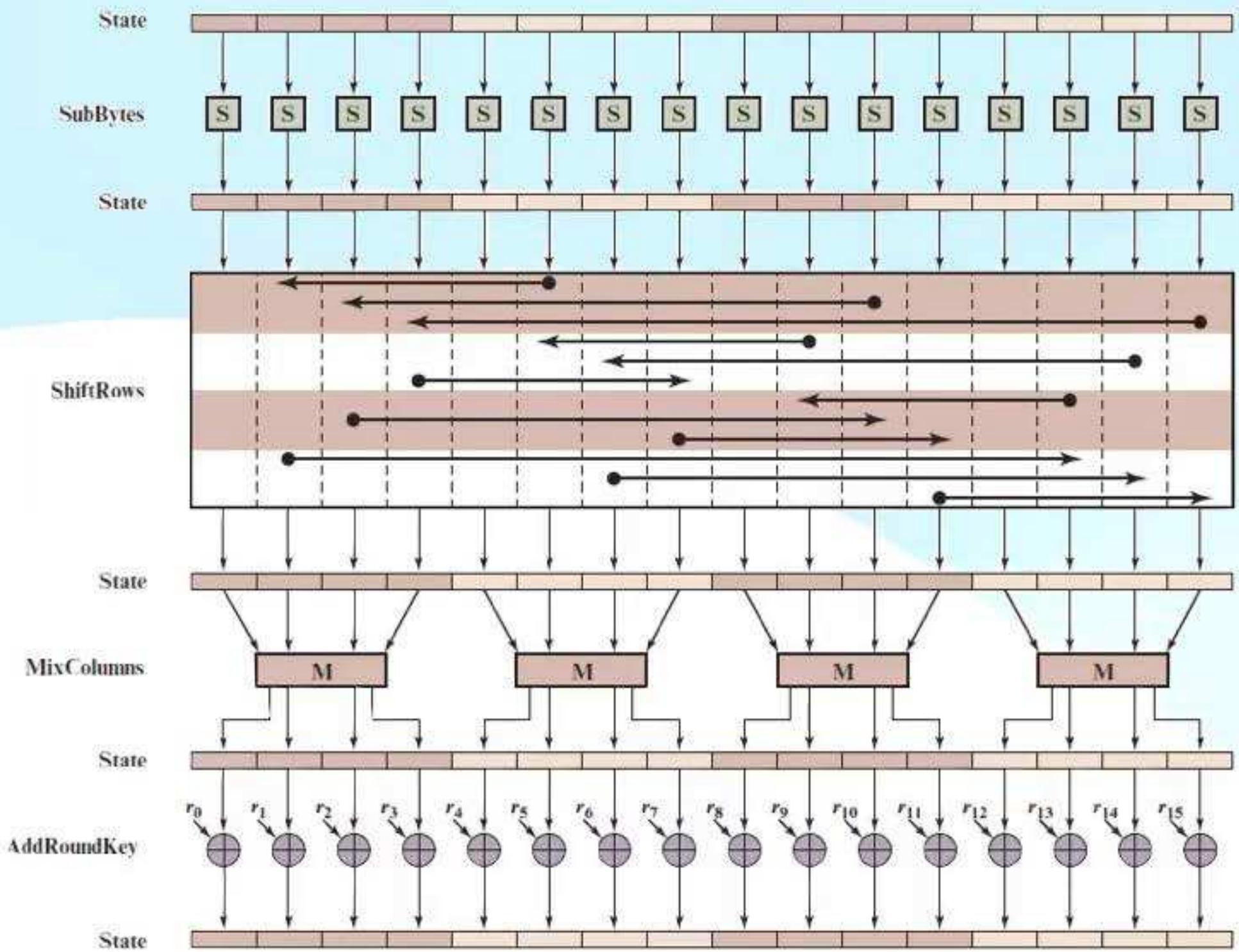
Detaylı Yapı (1/2)

- Değiştirme ve permütasyon kullanarak tüm veri bloğunu her turda tek bir matris olarak işler
- Girdi olarak sağlanan anahtar, kırk dört 32-bitlik sözcük dizisine genişletilir, `w[i]`
- Dört farklı aşama kullanılır:
  - **BaytlarıDeğiştir** - bloğun bayt bayt ikamesini gerçekleştirmek için bir S-box kullanır
  - **SatırlarıKaydır** - basit bir permütasyon
  - **SütunlarıKarıştır** – $GF(2^8)$ yerine aritmetik kullanan bir ikame
  - **TurAnahtarEkle** - genişletilmiş anahtarın bir kısmı ile mevcut bloğun basit bir bit düzeyinde XOR'u

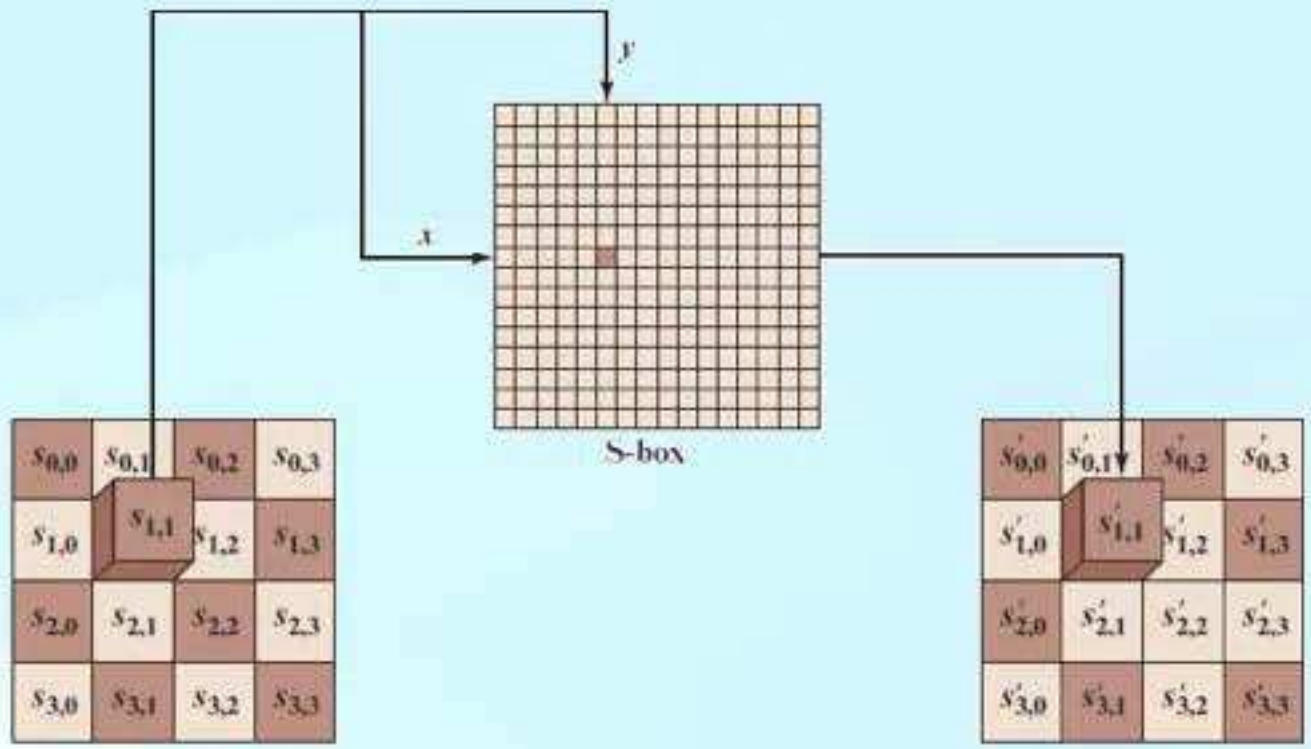
Detaylı Yapı (2/2)

- Şifre, ”Tur Anahtar Ekle" aşamasıyla başlar ve biter
- Şifreyi, bir bloğun XOR şifrelemesinin (”Tur Anahtar Ekle"), ardından bloğun şifrelenmesinin (diğer üç aşama), ardından XOR şifrelemesinin vb. dönüşümlü işlemleri olarak görüntüleyebilir
- Her aşama kolayca tersine çevrilebilir
- Şifre çözme algoritması, genişletilmiş anahtarı ters sırada kullanır, ancak şifre çözme algoritması, şifreleme algoritmasıyla aynı değildir.
- Durum hem şifreleme hem de şifre çözme için aynıdır
- Hem şifreleme hem de şifre çözmenin **son turu** yalnızca üç aşamadan oluşur

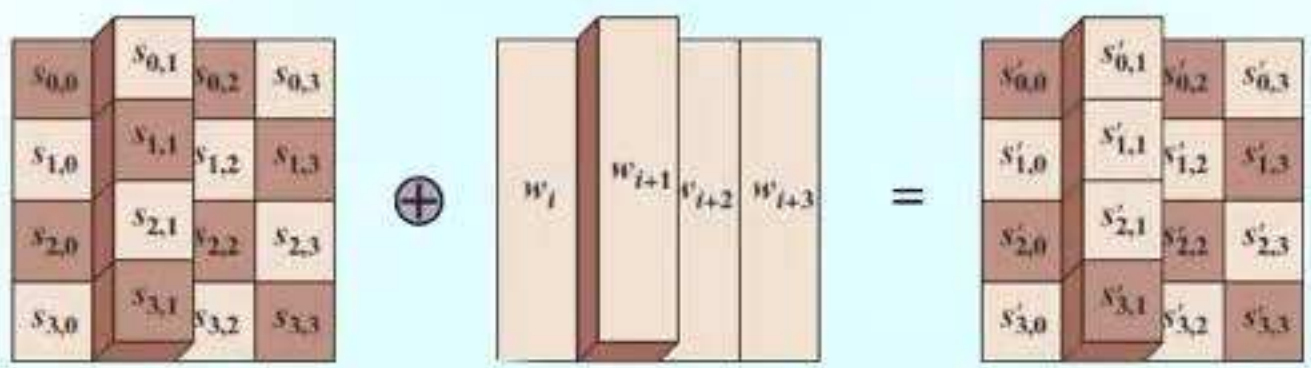
Şekil 6.4 AES Şifreleme Turu



Şekil 6.5 AES Bayt Düzeyinde İşlemler



(a) Substitute byte transformation



(b) Add round key transformation

Tablo 6.2 AES S-Kutuları (1/2)

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

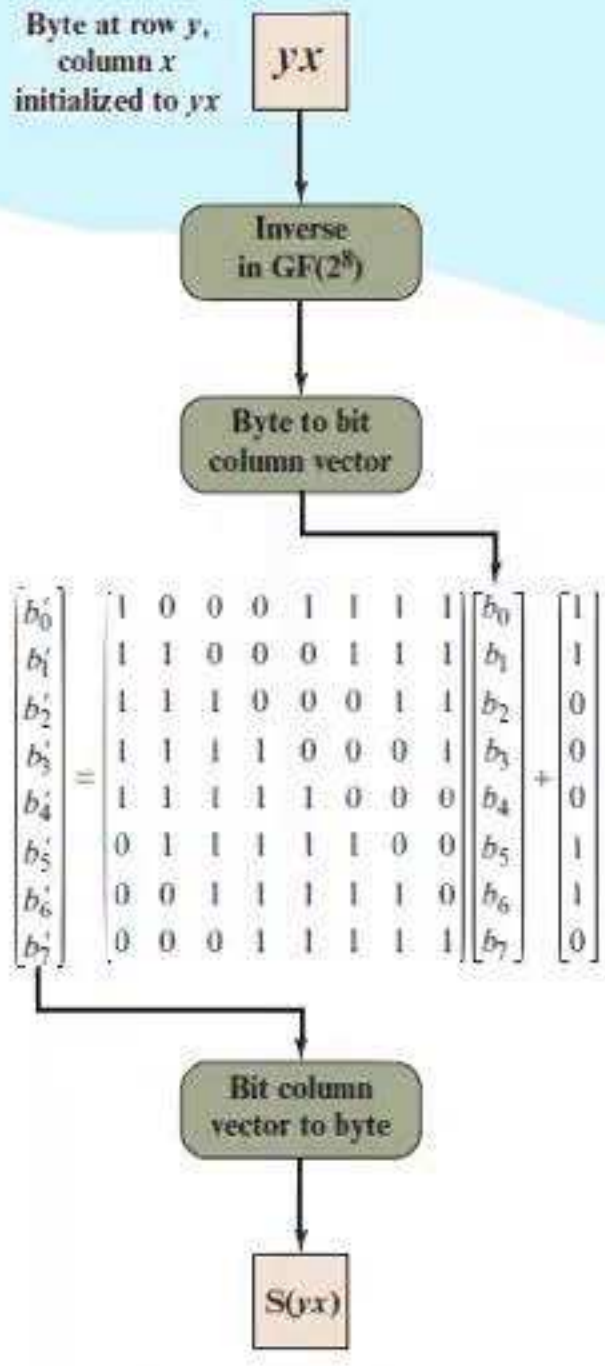
(a) S-box

Tablo 6.2 AES S-Kutuları (2/2)

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
	1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
	2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
	3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
	5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
	B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
	C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
	D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
	E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
	F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

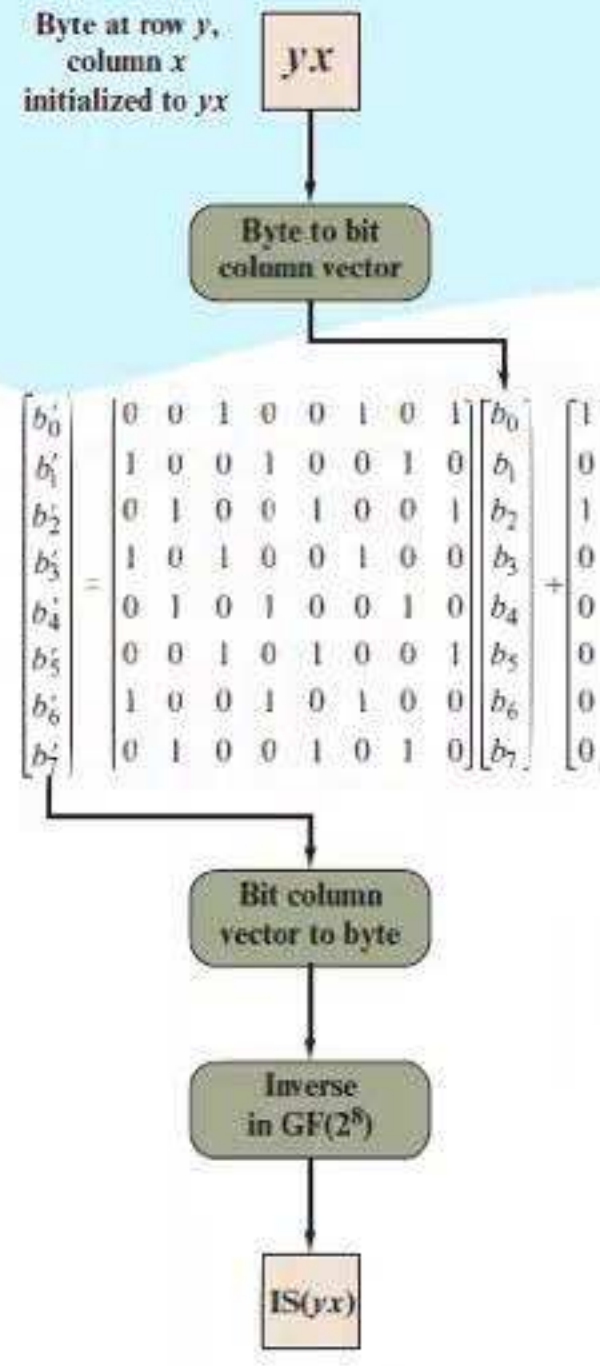
(b) Inverse S-box

Şekil 6.6 S-Box ve IS-Box Yapısı



$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

(a) Calculation of byte at row y, column x of S-box



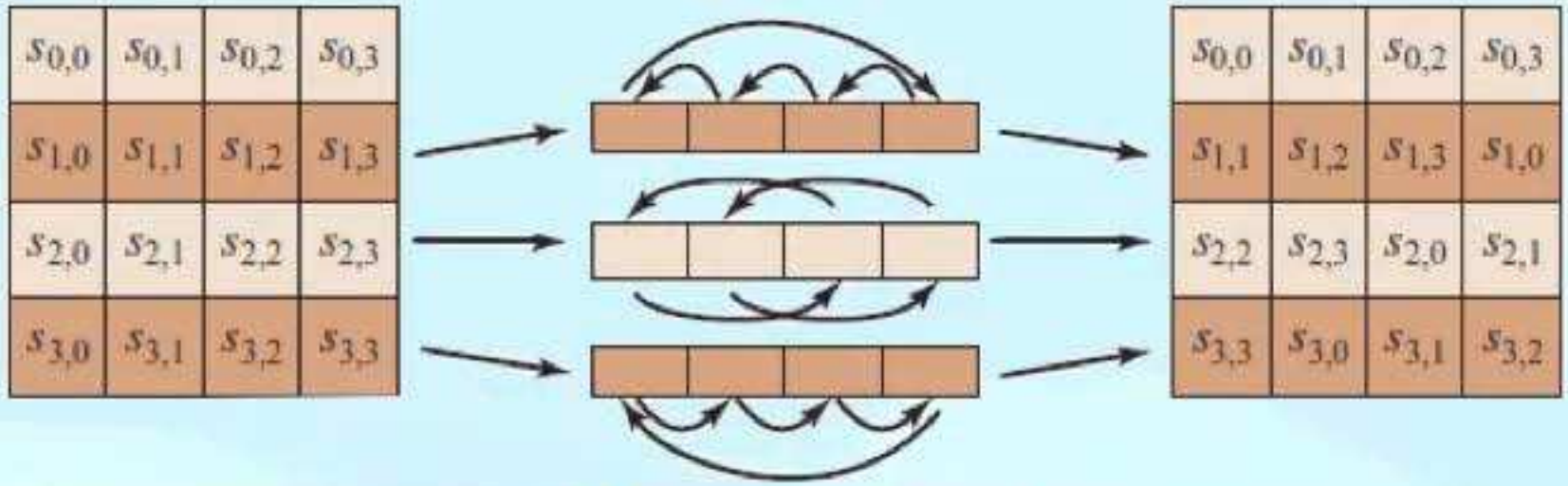
$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

(a) Calculation of byte at row y, column x of IS-box

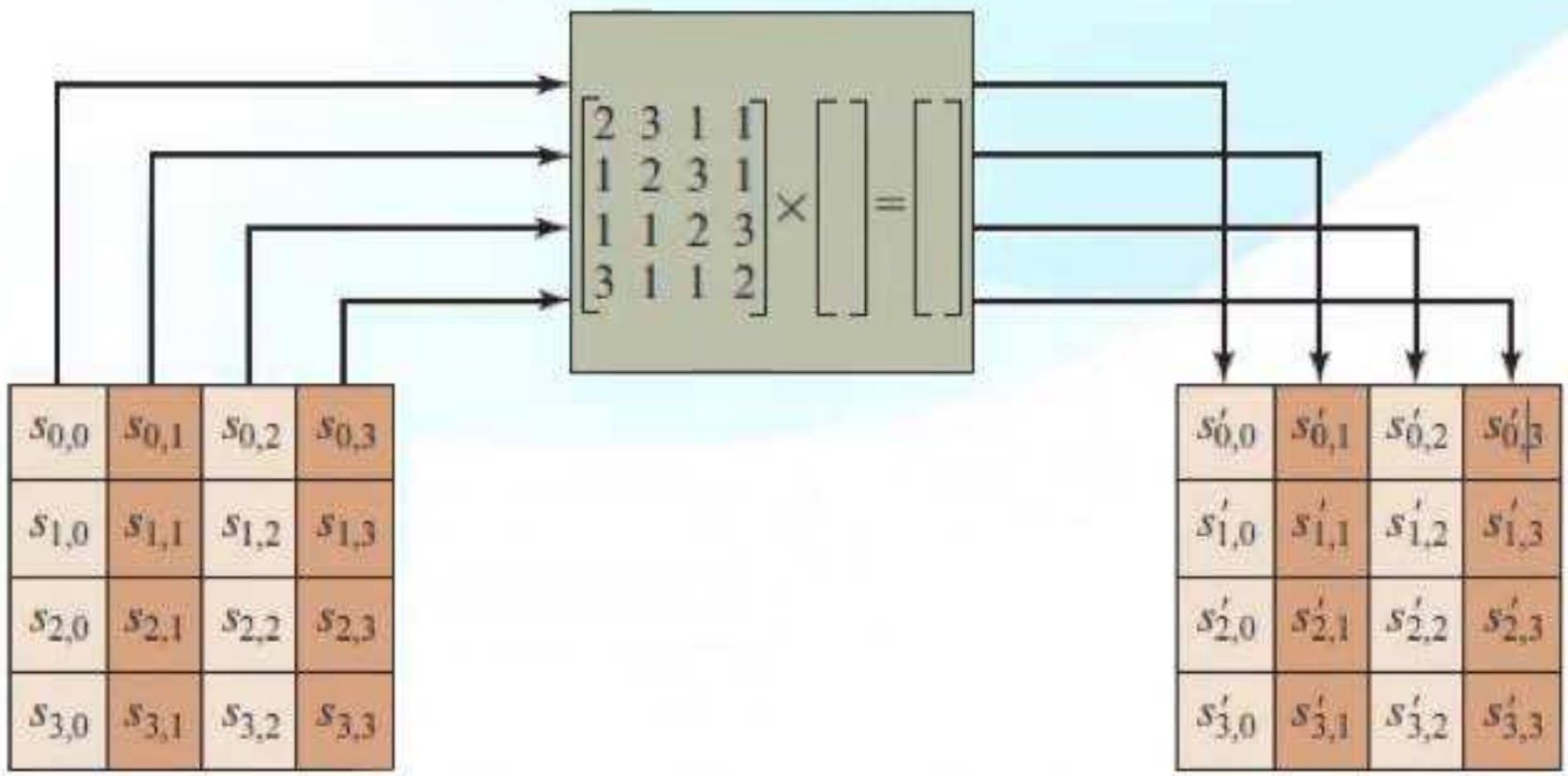
S-Box Mantığı

- S-box, bilinen kriptanalitik saldırılara karşı dayanıklı olacak şekilde tasarlanmıştır
- Rijndael geliştiricileri, girdi bitleri ile çıktı bitleri arasında düşük bir korelasyona sahip olan ve çıktının girdinin lineer bir matematiksel fonksiyonu olmadığı özelliği olan bir tasarım aradılar.
- Doğrusal olmama, çarpımsal tersin kullanılmasından kaynaklanmaktadır.

Şekil 6.7 AES Satır ve Sütun İşlemleri



(a) Shift row transformation



(b) Mix column transformation

SatırıKaydır Mantığı

- İlk göründüğünden daha önemli
- Durum, şifre giriş ve çıkışının yanı sıra, dört adet 4 baytlık sütundan oluşan bir dizi olarak değerlendirilir
- Şifrelemede, düz metnin ilk 4 baytı Durum'un ilk sütununa kopyalanır ve bu şekilde devam eder
- Tur anahtarı, Duruma sütun sütun uygulanır
  - Böylece, satır kaydırma tek bir baytı bir sütundan diğerine taşır, bu da 4 baytın katlarının doğrusal bir uzaklığıdır.
- Dönüşüm, bir sütunun 4 baytının dört farklı sütuna yayılmasını sağlar

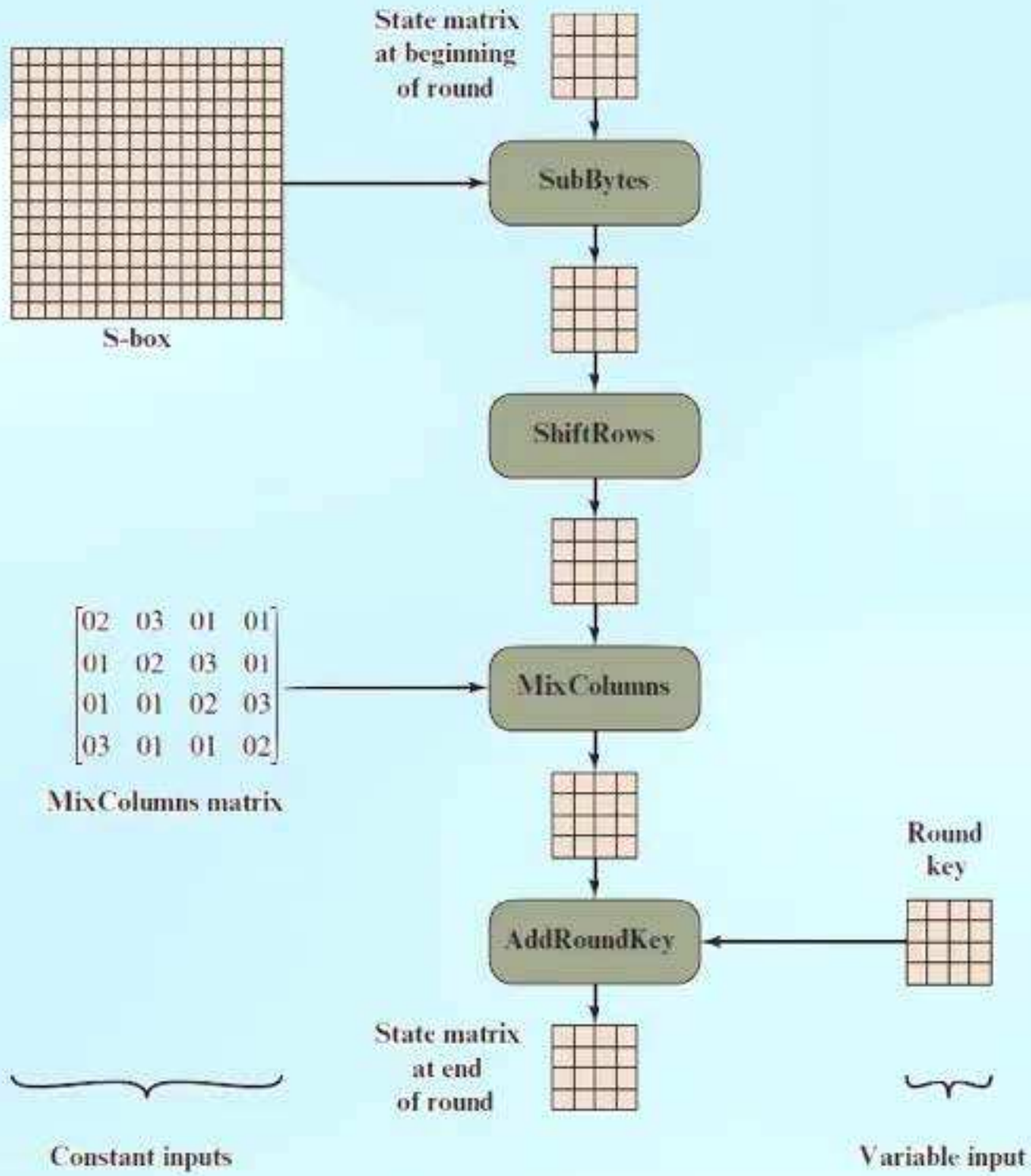
SütunlarıKarıştır Mantığı

- Kod sözcükleri arasındaki maksimum mesafeye sahip doğrusal bir koda dayalı bir matrisin katsayıları, her sütunun baytları arasında iyi bir karışım sağlar
- Satır kaydırma dönüşümüyle birleştirilmiş karma sütun dönüşümü, birkaç turdan sonra tüm çıkış bitlerinin tüm giriş bitlerine bağlı olmasını sağlar.

TurAnahtarEkle Dönüşümü

- 128 bitlik Durum, Tur anahtarın 128 biti ile bitsel olarak XORlanır
- İşlem, bir Durum sütununun 4 baytı ile Tur anahtarın bir sözcüğü arasında sütun yönünde bir işlem olarak görülür.
  - Bayt düzeyinde bir işlem olarak da görüntülenebilir
- Mantığı:
  - Mümkün olduğu kadar basittir ve Durum'un her parçasını etkiler
  - Tur anahtar genişletmenin karmaşıklığı ve AES'in diğer aşamalarının karmaşıklığı güvenliği sağlar

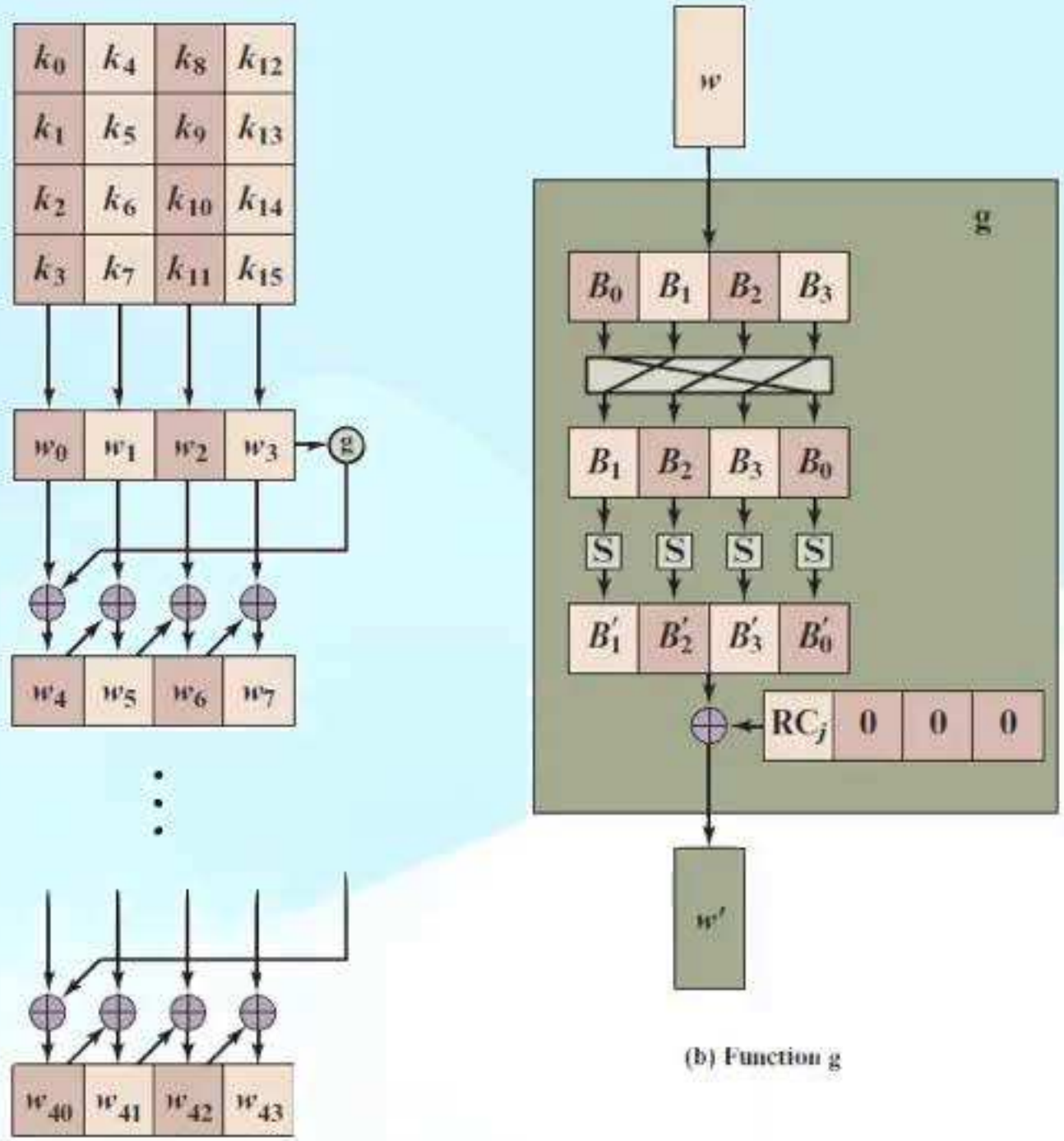
Şekil 6.8 Tek AES Turu için Girdiler



AES Anahtar Genişletme

- Girdi olarak dört kelimelik (16 bayt) bir anahtar alır ve 44 kelimelik (176) baytlık bir doğrusal dizi üretir
  - Bu, ilk TurAnahtarEkle aşaması ve şifrenin 10 turunun her biri için dört kelimelik bir tur anahtar sağlamak için yeterlidir.
- Anahtar, genişletilmiş anahtarın ilk dört sözcüğüne kopyalanır
  - Genişletilmiş anahtarın geri kalanı bir seferde dört kelimeyle doldurulur
- Eklenen her `w[i]` kelimesi hemen önceki kelimeye, `w[i - 1]` ve dört pozisyon geri, `w[i - 4]` kelimesine bağlıdır.
  - Dört durumun üçünde basit bir XOR kullanılır
  - `w` dizisindeki konumu 4'ün katı olan bir kelime için daha karmaşık bir fonksiyon kullanılır.

Şekil 6.9 AES Anahtar Genişletme



(a) Overall algorithm

(b) Function g

Anahtar Genişletme Mantığı (1/2)

- Rijndael geliştiricileri, genişletme anahtarı algoritmasını bilinen kriptanalitik saldırılara karşı dayanıklı olacak şekilde tasarladı.
- Tura bağımlı bir tur sabitin dahil edilmesi, tur anahtarların farklı turlarda üretilme yolları arasındaki simetriyi ortadan kaldırır.

Anahtar Genişletme Mantığı (2/2)

- Kullanılan belirli kriterler şunlardır:
  - Şifre anahtarının veya tur anahtarın bir parçasının bilinmesi, diğer birçok tur anahtar bitinin hesaplanmasını sağlamaz
  - tersine çevrilebilir bir dönüşüm
  - Çok çeşitli işlemcilerde hız
  - Simetrileri ortadan kaldırmak için tur sabitlerin kullanımı
  - Şifre anahtarı farklılıklarının tur anahtarlara yayılması
  - Yalnızca şifre anahtarı farklarından tur anahtar farklılıklarının tam olarak belirlenmesini yasaklamak için yeterli doğrusal olmama durumu
  - tanımlamanın basitliği

Tablo 6.3 Örnek Tur Anahtar Hesaplaması

Tanım	Değer
i (decimal)	36
temp = w[i − 1]	7F8D292F
RotWord (temp)	8D292F7F
SubWord (RotWord (temp))	5DA515D2
Rcon (9)	1B000000
SubWord (RotWord (temp)) ⊕ Rcon (9)	46A515D2
w[i − 4]	EAD27321
w[i] = w[i − 4] ⊕ SubWord (RotWord (temp)) ⊕ Rcon (9)	AC7766F3

Tablo 6.4 AES Örneği için Anahtar Genişletme (1/3)

Anahtar Kelimeler	Yardımcı Fonksiyon
w0 = 0f 15 71 c9	RotWord (w3) = 7f 67 98 af = x1
w1 = 47 d9 e8 59	SubWord (x1) = d2 85 46 79 = y1
w2 = 0c b7 ad d6	Rcon (1) = 01 00 00 00
w3 = af 7f 67 98	y1 ⊕ Rcon (1) = d3 85 46 79 = z1
w4 = w0 ⊕ z1 = dc 90 37 b0	RotWord (w7) = 81 15 a7 38 = x2
w5 = w4 ⊕ w1 = 9b 49 df e9	SubWord (x2) = 0c 59 5c 07 = y2
w6 = w5 ⊕ w2 = 97 fe 72 3f	Rcon (2) = 02 00 00 00
w7 = w6 ⊕ w3 = 38 81 15 a7	y2 ⊕ Rcon (2) = 0e 59 5c 07 = z2
w8 = w4 ⊕ z2 = d2 c9 6b b7	RotWord (w11) = ff d3 c6 e6 = x3
w9 = w8 ⊕ w5 = 49 80 b4 5e	SubWord (x3) = 16 66 b4 83 = y3
w10 = w9 ⊕ w6 = de 7e c6 61	Rcon (3) = 04 00 00 00
w11 = w10 ⊕ w7 = e6 ff d3 c6	y3 ⊕ Rcon (3) = 12 66 b4 8e = z3

Tablo 6.4 AES Örneği için Anahtar Genişletme (2/3)

Anahtar Kelimeler	Yardımcı Fonksiyon
w12 = w8 ⊕ z3 = c0 af df 39	RotWord (w15) = ae 7e c0 b1 = x4
w13 = w12 ⊕ w9 = 89 2f 6b 67	SubWord (x4) = e4 f3 ba c8 = y4
w14 = w13 ⊕ w10 = 57 51 ad 06	Rcon (4) = 08 00 00 00
w15 = w14 ⊕ w11 = b1 ae 7e c0	y4 ⊕ Rcon (4) = ec f3 ba c8 = 4
w16 = w12 ⊕ z4 = 2c 5c 65 f1	RotWord (w19) = 8c dd 50 43 = x5
w17 = w16 ⊕ w13 = a5 73 0e 96	SubWord (x5) = 64 c1 53 1a = y5
w18 = w17 ⊕ w14 = f2 22 a3 90	Rcon(5) = 10 00 00 00
w19 = w18 ⊕ w15 = 43 8c dd 50	y5 ⊕ Rcon (5) = 74 c1 53 1a = z5
w20 = w16 ⊕ z5 = 58 9d 36 eb	RotWord (w23) = 40 46 bd 4c = x6
w21 = w20 ⊕ w17 = fd ee 38 7d	SubWord (x6) = 09 5a 7a 29 = y6
w22 = w21 ⊕ w18 = 0f cc 9b ed	Rcon(6) = 20 00 00 00
w23 = w22 ⊕ w19 = 4c 40 46 bd	y6 ⊕ Rcon(6) = 29 5a 7a 29 = z6

Tablo 6.4 AES Örneği için Anahtar Genişletme (3/3)

Anahtar Kelimeler	Yardımcı Fonksiyon
w24 = w20 ⊕ z6 = 71 c7 4c c2	RotWord (w27) = a5 a9 ef cf = x7
w25 = w24 ⊕ w21 = 8c 29 74 bf	SubWord (x7) = 06 d3 bf 8a = y7
w26 = w25 ⊕ w22 = 83 e5 ef 52	Rcon (7) = 40 00 00 00
w27 = w26 ⊕ w23 = cf a5 a9 ef	y7 ⊕ Rcon(7) = 46 d3 df 8a = z7
w28 = w24 ⊕ z7 = 37 14 93 48	RotWord (w31) = 7d a1 4a f7 = x8
w29 = w28 ⊕ w25 = bb 3d e7 f7	SubWord (x8) = ff 32 d6 68 = y8
w30 = w29 ⊕ w26 = 38 d8 08 a5	Rcon (8) = 80 00 00 00
w31 = w30 ⊕ w27 = f7 7d a1 4a	y8 ⊕ Rcon(8) = 7f 32 d6 68 = z8
w32 = w28 ⊕ z8 = 48 26 45 20	RotWord (w35) = be 0b 38 3c = x9
w33 = w32 ⊕ w29 = f3 1b a2 d7	SubWord (x9) = ae 2b 07 eb = y9
w34 = w33 ⊕ w30 = cb c3 aa 72	Rcon (9) = 1B 00 00 00
w35 = w34 ⊕ w32 = 3c be 0b 3	y9 ⊕ Rcon (9) = b5 2b 07 eb = z9
w36 = w32 ⊕ z9 = fd 0d 42 cb	RotWord (w39) = 6b 41 56 f9 = x10
w37 = w36 ⊕ w33 = 0e 16 e0 1c	SubWord (x10) = 7f 83 b1 99 = y10
w38 = w37 ⊕ w34 = c5 d5 4a 6e	Rcon (10) = 36 00 00 00
w39 = w38 ⊕ w35 = f9 6b 41 56	y10 ⊕ Rcon (10) = 49 83 b1 99 = z10
w40 = w36 ⊕ z10 = b4 8e f3 52	
w41 = w40 ⊕ w37 = ba 98 13 4e	
w42 = w41 ⊕ w38 = 7f 4d 59 20	
w43 = w42 ⊕ w39 = 86 26 18 76	

Tablo 6.5 AES Örneği (1/2)

Tur Başlangıcı	AltBaytlardan Sonra	SatırlarıKaydırdıktan Sonra	SütunlarıKarıştırdıktan Sonra	TurAnahtarı
01 89 fe 76 23 ab dc 54 45 cd ba 32 67 ef 98 10				0f 47 0c af 15 d9 b7 7f 71 e8 ad 67 c9 59 d6 98
0e ce f2 d9 36 72 6b 2b 34 25 17 55 ae b6 4e 88	ab 8b 89 35 05 40 7f f1 18 3f f0 fc e4 4e 2f c4	ab 8b 89 35 40 7f f1 05 f0 fc 18 3f c4 e4 4e 2f	b9 94 57 75 e4 8e 16 51 47 20 9a 3f c5 d6 f5 3b	dc 9b 97 38 90 49 fe 81 37 df 72 15 b0 e9 3f a7
65 0f c0 4d 74 c7 e8 d0 70 ff e8 2a 75 3f ca 9c	4d 76 ba e3 92 c6 9b 70 51 16 9b e5 9d 75 74 de	4d 76 ba e3 c6 9b 70 92 9b e5 51 16 de 9d 75 74	8e 22 db 12 b2 f2 dc 92 df 80 f7 c1 2d c5 1e 52	d2 49 de e6 c9 80 7e ff 6b b4 c6 d3 b7 5e 61 c6
5c 6b 05 f4 7b 72 a2 6d b4 34 31 12 9a 9b 7f 94	4a 7f 6b bf 21 40 3a 3c 8d 18 c7 c9 b8 14 d2 22	4a 7f 6b bf 40 3a 3c 21 c7 c9 8d 18 22 b8 14 d2	b1 c1 0b cc ba f3 8b 07 f9 1f 6a c3 1d 19 24 5c	c0 89 57 b1 af 2f 51 ae df 6b ad 7e 39 67 06 c0
71 48 5c 7d 15 dc da a9 26 74 c7 bd 24 7e 22 9c	a3 52 4a ff 59 86 57 d3 f7 92 c6 7a 36 f3 93 de	a3 52 4a ff 86 57 d3 59 c6 7a f7 92 de 36 f3 93	d4 11 fe 0f 3b 44 06 73 cb ab 62 37 19 b7 07 ec	2c a5 f2 43 5c 73 22 8c 65 0e a3 dd f1 96 90 50
f8 b4 0c 4c 67 37 24 ff ae a5 c1 ea e8 21 97 bc	41 8d fe 29 85 9a 36 16 e4 06 78 87 9b fd 88 65	41 8d fe 29 9a 36 16 85 78 87 e4 06 65 9b fd 88	2a 47 c4 48 83 e8 18 ba 84 18 27 23 eb 10 0a f3	58 fd 0f 4c 9d ee cc 40 36 38 9b 46 eb 7d ed bd

Tablo 6.5 AES Örneği (2/2)

Tur Başlangıcı	AltBaytlardan Sonra	SatırlarıKaydırdıktan Sonra	SütunlarıKarıştırdıktan Sonra	TurAnahtarı
72 ba cb 04 1e 06 d4 fa b2 20 bc 65 00 6d e7 4e	40 f4 1f f2 72 6f 48 2d 37 b7 65 4d 63 3c 94 2f	40 f4 1f f2 6f 48 2d 72 65 4d 37 b7 2f 63 3c 94	7b 05 42 4a 1e d0 20 40 94 83 18 52 94 c4 43 fb	71 8c 83 cf c7 29 e5 a5 4c 74 ef a9 c2 bf 52 ef
0a 89 c1 85 d9 f9 c5 e5 d8 f7 f7 fb 56 7b 11 14	67 a7 78 97 35 99 a6 d9 61 68 68 0f b1 21 82 fa	67 a7 78 97 99 a6 d9 35 68 0f 61 68 fa b1 21 82	ec 1a c0 80 0c 50 53 c7 3b d7 00 ef b7 22 72 e0	37 bb 38 f7 14 3d d8 7d 93 e7 08 a1 48 f7 a5 4a
db a1 f8 77 18 6d 8b ba a8 30 08 4e ff d5 d7 aa	b9 32 41 f5 ad 3c 3d f4 c2 04 30 2f 16 03 0e ac	b9 32 41 f5 3c 3d f4 ad 30 2f c2 04 ac 16 03 0e	b1 1a 44 17 3d 2f ec b6 0a 6b 2f 42 9f 68 f3 b1	48 f3 cb 3c 26 1b c3 be 45 a2 aa 0b 20 d7 72 38
f9 e9 8f 2b 1b 34 2f 08 4f c9 85 49 bf bf 81 89	99 1e 73 f1 af 18 15 30 84 dd 97 3b 08 08 0c a7	99 1e 73 f1 18 15 30 af 97 3b 84 dd a7 08 08 0c	31 30 3a c2 ac 71 8c c4 46 65 48 eb 6a 1c 31 62	fd 0e c5 f9 0d 16 d5 6b 42 e0 4a 41 cb 1c 6e 56
cc 3e ff 3b a1 67 59 af 04 85 02 aa a1 00 5f 34	4b b2 16 e2 32 85 cb 79 f2 97 77 ac 32 63 cf 18	4b b2 16 e2 85 cb 79 32 77 ac f2 97 18 32 63 cf		b4 ba 7f 86 8e 98 4d 26 f3 13 59 18 52 4e 20 76
ff 08 69 64 0b 53 34 14 84 bf ab 8f 4a 7c 43 b9				

Tablo 6.6 AES'de Çığ Etkisi: Şifresiz Metindeki Değişim (1/2)

Tur		Bit Sayısındaki Fark
	0123456789abcdeffedcba9876543210 0023456789abcdeffedcba9876543210	1
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	657470750fc7ff3fc0e8e8ca4dd02a9c c4a9ad090fc7ff3fc0e8e8ca4dd02a9c	20
2	5c7bb49a6b72349b05a2317ff46d1294 fe2ae569f7ee8bb8c1f5a2bb37ef53d5	58
3	7115262448dc747e5cdac7227da9bd9c ec093dfb7c45343d689017507d485e62	59
4	f867aee8b437a5210c24c1974cffeabc 43efdb697244df808e8d9364ee0ae6f5	61
5	721eb200ba06206dcbd4bce704fa654e 7b28a5d5ed643287e006c099bb375302	68

Tablo 6.6 AES'de Çığ Etkisi: Şifresiz Metindeki Değişim (2/2)

Tur		Bit Sayısındaki Fark
6	0ad9d85689f9f77bc1c5f71185e5fb14 3bc2d8b6798d8ac4fe36a1d891ac181a	64
7	db18a8ffa16d30d5f88b08d777ba4eaa 9fb8b5452023c70280e5c4bb9e555a4b	67
8	f91b4fbfe934c9bf8f2f85812b084989 20264e1126b219aef7feb3f9b2d6de40	65
9	cca104a13e678500ff59025f3bafaa34 b56a0341b2290ba7dfdfbddcd8578205	61
10	ff0b844a0853bf7c6934ab4364148fb9 612b89398d0600cde116227ce72433f0	58

Tablo 6.7 AES'de Çığ Etkisi: Anahtardaki Değişim (1/2)

Tur		Bit Sayısındaki Fark
	0123456789abcdeffedcba9876543210 0123456789abcdeffedcba9876543210	0
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	657470750fc7ff3fc0e8e8ca4dd02a9c c5a9ad090ec7ff3fc1e8e8ca4cd02a9c	22
2	5c7bb49a6b72349b05a2317ff46d1294 90905fa9563356d15f3760f3b8259985	58
3	7115262448dc747e5cdac7227da9bd9c 18aeb7aa794b3b66629448d575c7cebf	67
4	f867aee8b437a5210c24c1974cffeabc f81015f993c978a876ae017cb49e7eec	63
5	721eb200ba06206dcbd4bce704fa654e 5955c91b4e769f3cb4a94768e98d5267	81

Tablo 6.7 AES'de Çığ Etkisi: Anahtardaki Değişim (2/2)

Tur		Bit Sayısındaki Fark
6	0ad9d85689f9f77bc1c5f71185e5fb14 dc60a24d137662181e45b8d3726b2920	70
7	db18a8ffa16d30d5f88b08d777ba4eaa fe8343b8f88bef66cab7e977d005a03c	74
8	f91b4fbfe934c9bf8f2f85812b084989 da7dad581d1725c5b72fa0f9d9d1366a	67
9	cca104a13e678500ff59025f3bafaa34 0ccb4c66bbfd912f4b511d72996345e0	59
10	ff0b844a0853bf7c6934ab4364148fb9 fc8923ee501a7d207ab670686839996b	53

AES Uygulaması

- AES şifre çözme şifresi, şifreleme şifresiyle aynı değil
  - Anahtar programların biçimi aynı olmasına rağmen, dönüşümlerin sırası farklılık gösterir.
  - Hem şifreleme hem de şifre çözme gerektiren uygulamalar için iki ayrı yazılım veya sabit yazılım modülünün gerekli olması dezavantajına sahiptir.
- Şifre çözme yapısını şifreleme yapısına uygun hale getirmek için iki ayrı değişikliğe ihtiyaç vardır.
- Şifre çözme turunun ilk iki aşamasının değiştirilmesi gerekir
- Şifre çözme turunun ikinci iki aşamasının değiştirilmesi gerekir

Ters SatırlarıKaydırma ve TersAltBaytları Değiştirme

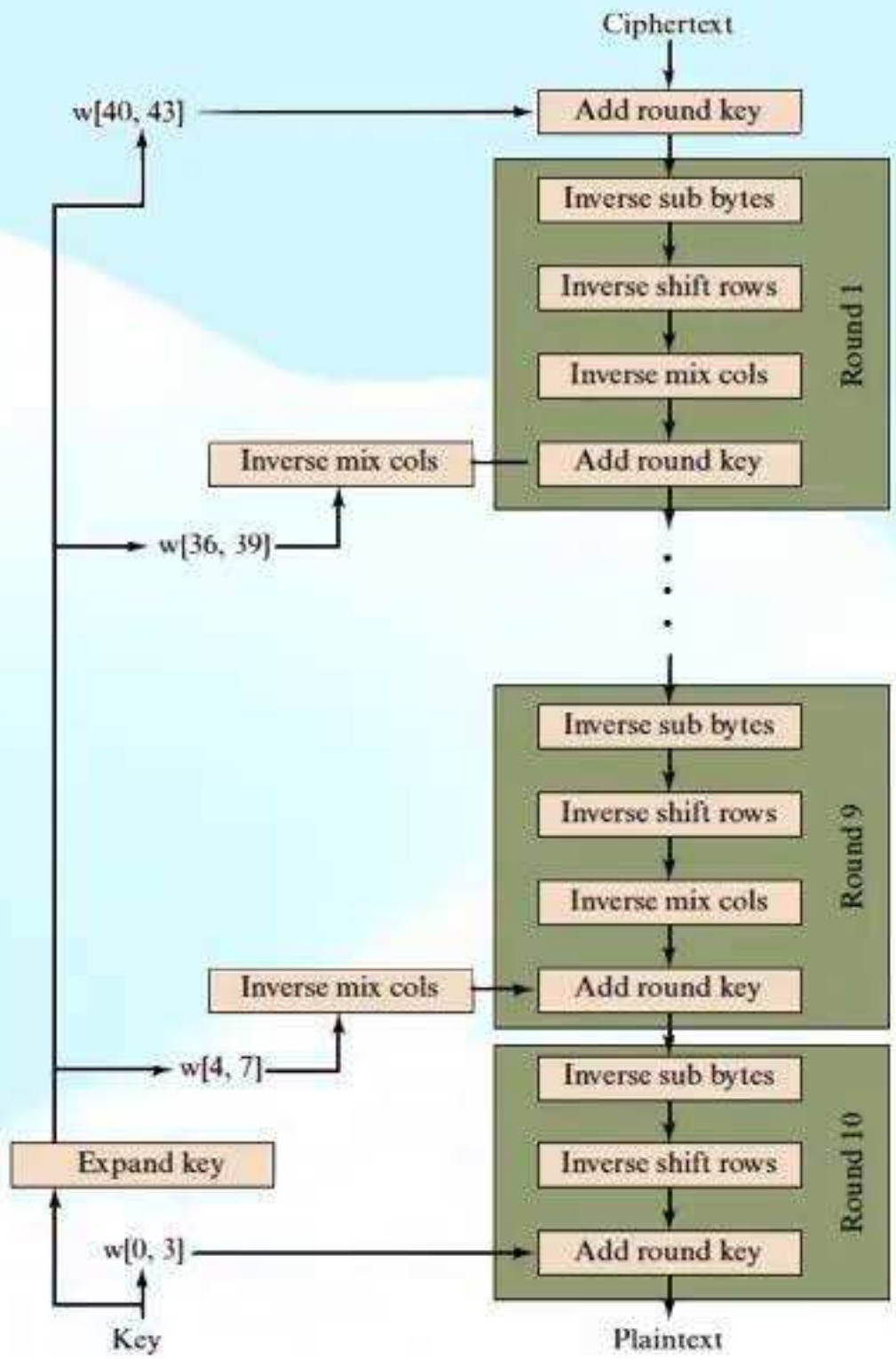
- SatırlarıTersÇevir, Durumdaki *bayt dizisini etkiler ancak bayt içeriklerini değiştirmez ve dönüşümünü gerçekleştirmek için bayt içeriklerine bağlı değildir.*
- TersAltBaytlar, Durumdaki *baytların içeriğini etkiler ancak bayt sırasını değiştirmez ve dönüşümünü gerçekleştirmek için bayt dizisine bağlı değildir.*

Böylece, bu iki işlem işe gidip gelir ve değiştirilebilir

TurAnahtarEkle ve TersSütunlarıKarıştır'ın Değiştirilmesi

- TurAnahtarEkle ve TersSütunlarıKarıştır dönüşümleri, Durumdaki bayt sırasını değiştirmez
- Anahtarı bir kelime dizisi olarak görürsek, hem TurAnahtarEkle hem de TersSütunlarıKarıştır her seferinde bir sütun Durum üzerinde çalışır.
- Bu iki işlem sütun girişine göre doğrusaldır.

Şekil 6.10 Eşdeğer Ters Şifre



Uygulama Yönleri (1/2)

- AES, 8 bitlik bir işlemcide çok verimli bir şekilde uygulanabilir
- ”TurAnahtarEkle", bayt bazında bir XOR işlemidir
- "SatırlarıKaydır" basit bir bayt kaydırma işlemidir
- "AltBaytlar", bayt düzeyinde çalışır ve yalnızca 256 baytlık bir tablo gerektirir
- ”SütunlarıKarıştır", $GF(2^8)$ alanında matris çarpımını gerektirir, bu da tüm işlemlerin baytlarda gerçekleştirildiği anlamına gelir

Uygulama Yönleri (2/2)

- 32 bit işlemcide verimli bir şekilde uygulayabilir
  - 32 bit kelimeleri kullanmak için adımları yeniden tanımlayın
  - 256 kelimelik 4 tabloyu önceden hesaplayabilir
  - Ardından, her turdaki her sütun, 4 tablo araması + 4 XOR kullanılarak hesaplanabilir.
  - Tabloları depolamanın maliyeti 4Kb
- Tasarımcılar, bu çok verimli uygulamanın, AES şifresi olarak seçilmesinde kilit bir faktör olduğuna inanıyor

Özet

- Gelişmiş Şifreleme Standardı'nın (AES) genel yapısına ilişkin bir genel bakış sunun
- AES'de kullanılan dört dönüşümü anlayın
- AES anahtar genişletme algoritmasını açıklayın
- GF(2^8)'de katsayılı polinomların kullanımını anlama