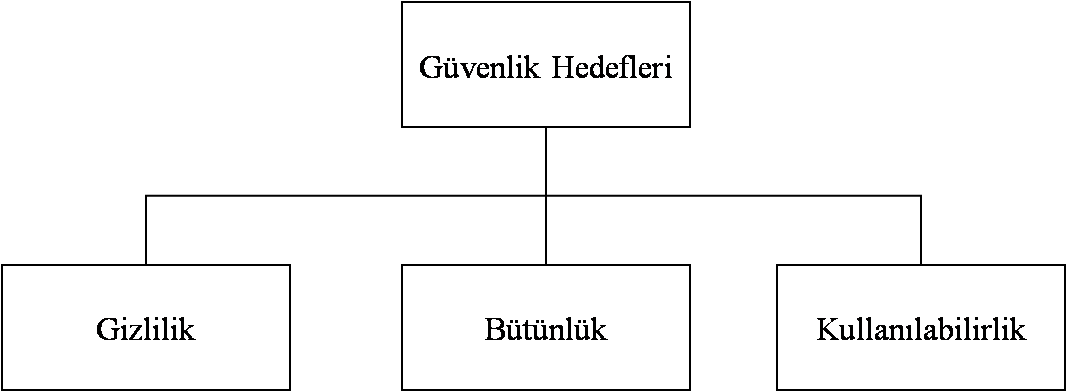
**DERS: Güvenlik Temelleri**



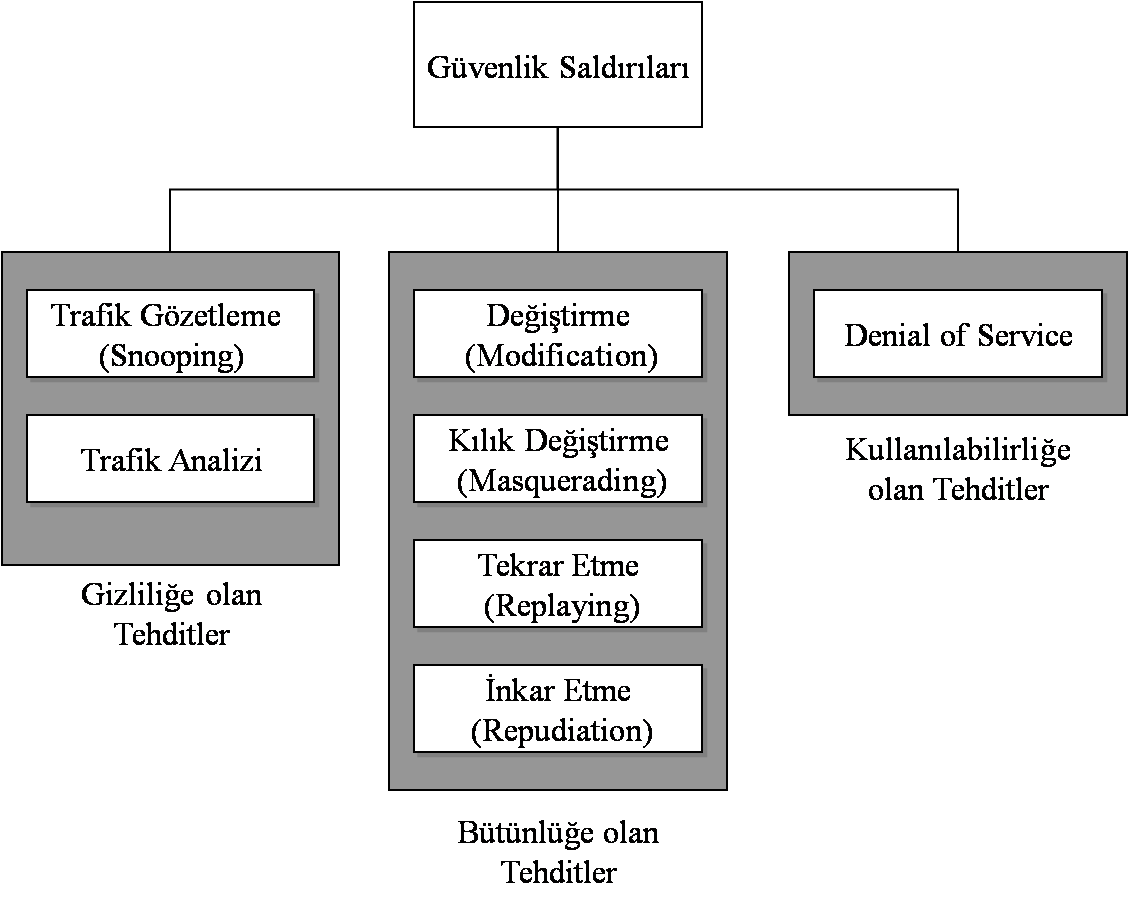
**Şekil 1.** Güvenlik Amaçlarının Sınıflandırılması

Üç önemli güvenlik amacı sırasıyla

**1-Gizlilik (Confidentiality):** Uzak bir bilgisayara depolanmak üzere bir bilgi parçası yollandığında ya da uzak bir bilgisayardan veri alındığında bu bilginin iletim sırasında gizlenmesi gerekir.

**2- Bütünlük (Integrity):** Bilginin zaman zaman değiştirilme ihtiyacı doğabilir. Bu değişiklikler yetkili (authorized) mekanizmalar tarafından gerçekleştirilmelidir.

**3-Kullanılabilirlik (Availability):** Bilgi güvenliğinin üçüncü parçası kullanılabilirliktir. Bir organizasyon tarafından yaratılan ve depo edilen bilgi, yetkili birimler tarafından kullanılabilir olmalıdır. Örneğin bir bankanın müşterisinin işlem yapmak için hesabına erişim yapamadığını düşünelim.



**Şekil 2.** Güvenlik Amaçları ile İlişkili Saldırıların Sınıflandırılması

**SALDIRILAR**

Yukarıda bahsedilen üç güvenlik amacı güvenlik saldırıları tarafından tehdit edilmektedir. İşte bu saldırılar literatürde farklı yaklaşımlara göre kategorilere sokulmaktadır. Burada ilk önce bu saldırılar güvenlik amaçlarına göre üç gruba ayrılacak daha sonra sistem üzerindeki etkilere göre iki geniş guruba bölünecektir.

**Gizliliği Tehdit Eden Saldırılar**

Yukarıdaki şekilden de görüldüğü gibi bilginin gizliliğini tehdit eden iki saldırı tipi mevcuttur.

1. **Trafik Gözetleme (Snooping):** Bu saldırı verinin yetkisiz olarak erişimi ya da elde edilmesi ile ilgilidir. Örneğin Internet yoluyla iletilen bir dosya gizli bir bilgi içerebilir. Yetkisiz bir birim iletimi ele geçirebilir ve içeriğini kendi faydası için kullanabilir. Trafik gözetlemeyi engellemek amacıyla verinin şifreleme teknikleri kullanılarak anlamsız hale getirilmesi yapılabilir.
2. **Trafik Analizi (Traffic Analysis):** Veri şifreleme her ne kadar veriyi elde eden için verinin anlaşılmaz hale gelmesini sağlasa da online trafiği izleyen bazı diğer tip verileri elde edebilir. Örneğin göndericinin ya da alıcının elektronik adresini (e-mail adresi) elde edebilir. Trafiği izleyen kişi istek ve cevap çiftlerini biriktirerek işlemin doğasını anlamsına yardım edebilir.

**Bütünlüğü Tehdit Eden Saldırılar**

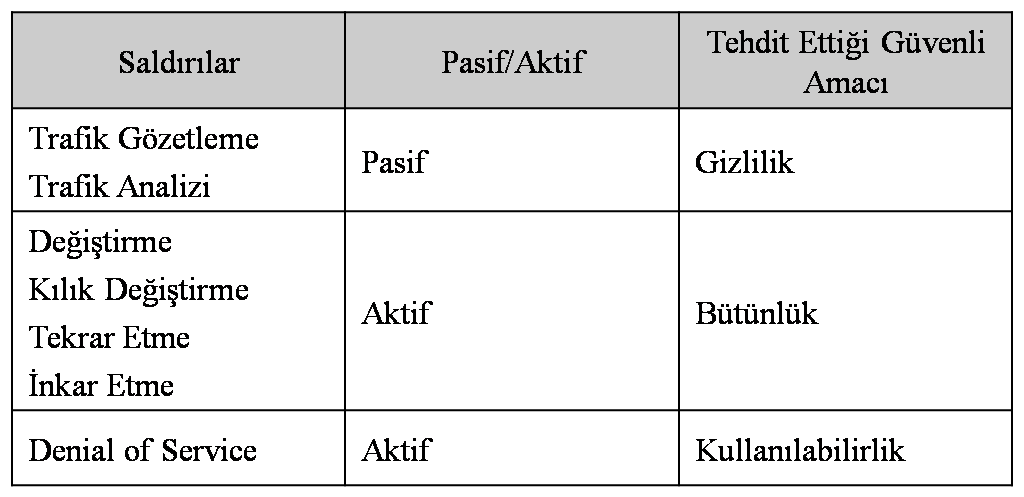
Verini bütünlüğünü tehdit eden bazı tip saldırılar vardır. Bunlar değiştirme (modification), kılık değiştirme (masquerading), Tekrar etme (replaying), inkar etme (repudiation).

1. **Değiştirme (Modification):** Bilgiye eriştikten ya da bilgiyi elde ettikten sonra saldırgan kendisine fayda sağlamak amacıyla bilgiyi değiştirebilir. Örneğin bir müşteri bankaya bazı işlemlerini yapmak için bir mesaj yollar. Saldırgan kendine fayda sağlamak amacıyla bu mesajı alır ve değiştirir. Not edilmelidir ki saldırgan sisteme zarar vermek için ya da kendi faydası için basitçe mesajı silebilir ya da geciktirebilir.
2. **Kılık Değiştirme (Masquerading):** Kılık değiştirme ya da kandırma (spoofing) saldırgan birisiymiş gibi davrandığında meydana gelir. Örneğin saldırgan bir müşterinin banka kartını ve PIN kodunu çalabilir ve müşteriymiş gibi davranabilir. Diğer bir örnek ise şöyle verilebilir. Bir kullanıcı bir banka ile bağlantıya geçmeyi dener. Fakat diğer bir site bankaymış gibi davranarak kullanıcıdan bazı bilgiler elde eder.
3. **Tekrar etme (Replaying):** Saldırgan kullanıcı tarafından yollanan mesajın bir kopyasını elde eder ve daha sonra onu tekrar etmeyi dener.
4. **İnkâr etme (Repudiation):** Bu saldırı tipi diğerlerinden biraz farklıdır. Çünkü iletişimde iki partiden biri tarafından gerçekleştirilir: gönderici ya da alıcı. Mesajı gönderen daha sonra mesajı gönderdiğini inkâr edebilir. Ya da alıcı daha sonra mesajı gönderdiğini inkâr edebilir. Gönderici tarafından inkâr etme bir banka müşterisinin üçüncü bir partiye banka aracılığıyla para göndermek istemesi ve daha sonra böyle bir istekte bulunduğunu inkâr etmesi şeklinde örneklenebilir. Yine alıcı tarafından inkâr etme bir kişi bir üreticiden bir ürün satın aldığında ve onu elektronik olarak ödeme yapmak istediğinde ortaya çıkabilir. Fakat daha sonra üretici ödemeyi aldığını inkâr ederek tekrar ödenmesini söylemesi şeklinde örneklenebilir.

**Kullanabilirliği Tehdit Eden Saldırılar**

Kullanılabilirliği tehdit eden sadece bir saldırıdan bahsedeceğiz.

1. **Dos Saldırısı (Denial Of Service):** Çok yaygın bir saldırıdır. Karşı sistemde çalışan servisin yavaşlamasını ya da topluca durmasını amaç edinir. Saldırgan bunu başarmak için birçok strateji kullanabilir. Örneğin saldırgan bir server’a (sunucu) birçok bogus (çalışmaz durumda) isteği gönderir ve böylece server aşırı yüklemeden dolayı çöker. Saldırgan bir server’ın bir istemciye (client) olan cevabını ele geçirebilir ve böylece istemciye sunucunun cevap vermediğine inandırabilir. Yine saldırgan istemcinin isteklerini ele geçirebilir ve böylece istemcinin birçok defa istek göndermesini sağlayarak sistemin aşırı yüklenmesine neden olabilir.

****

**Şekil 3.** Pasif ve Aktif Saldırıların Sınıflandırılması

**Pasif Saldırılara Karşı Aktif Saldırılar**

**Pasif saldırıda** saldırganın amacı sadece bilgiyi elde etmektir. Bunun anlamı saldırı veriyi değiştirmez ya da sisteme zarar vermez. Sistem normal işlemesine devam eder. Bununla beraber, saldırı göndericinin ya da alıcının mesajına zarar verebilir. Gizlilik güvenlik amacını tehdit eden saldırılar (Trafik gözetleme, Trafik Analizi) pasiftir. Bilginin ortaya çıkarılması göndericinin ya da alıcının mesajına zarar verebilir. Fakat sistem bundan etkilenmez. Bu nedenden dolayı gönderici ya da alıcı gizli bilgi akıtmasını keşfedene kadar bu saldırının anlaşılması zordur. Pasif saldırılar dolayısıyla verinin şifrelenmesi yoluyla engellenebilir.

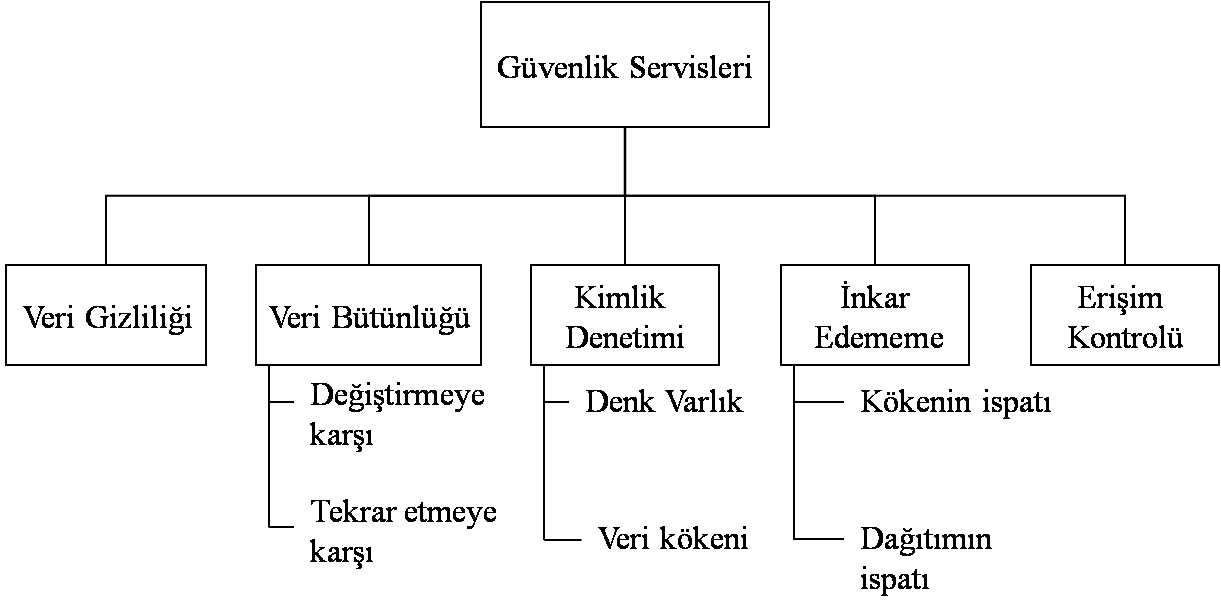
**Bir aktif saldırı** veriyi değiştirebilir ya da sisteme zarar verebilir. Bütünlüğü ve Kullanılabilirliği tehdit eden saldırlar aktif saldırılardır. Aktif saldırıları sezmek engellemekten daha kolaydır. Çünkü bir saldırgan birçok yolla saldırıları meydana getirebilir.

**Güvenlik Servisleri ve Mekanizmaları**

**ITU-T** ( International Telecommunication Union- Telecommunication Standardization Sector) bazı güvenlik servisleri ve mekanizmaları sağlamaktadır. Güvenlik servisleri ve mekanizmaları yakın olarak ilgilidir. Bir mekanizma ya da mekanizmaların bir kombinasyonu bir servis sağlamak için kullanılır. Buna ek olarak, bir mekanizma bir ya da daha fazla serviste kullanılabilir.

1. **Güvenlik Servisleri**

**ITU-T (X.800)** tanımladığımız güvenlik amaçları ve saldırılara ilişkin 5 servis tanımlamıştır. Şekil 4 bunu göstermektedir.



**Şekil 4.** Güvenlik Servisleri

Yukarıdaki servislerin bir ya da daha fazlasını güvenlik amaçlarının bir ya da daha fazlası ile ilişkilendirmek oldukça kolaydır. Buna ek olarak tanıtılan güvenlik saldırılarını önlemek amacıyla tasarlanmışlardır.

**Veri gizliliği (Data Confidentiality):** Veri gizliliği veriyi ortaya çıkarma saldırısından (disclosure attack) korumak için tasarlanmıştır. X.800 olarak tanımlanan servis çok geniştir ve bir mesajın tümünü ya da bir parçasının gizliliğini çevreler. Buna ek olarak trafik analizine karşı koruma sağlar.

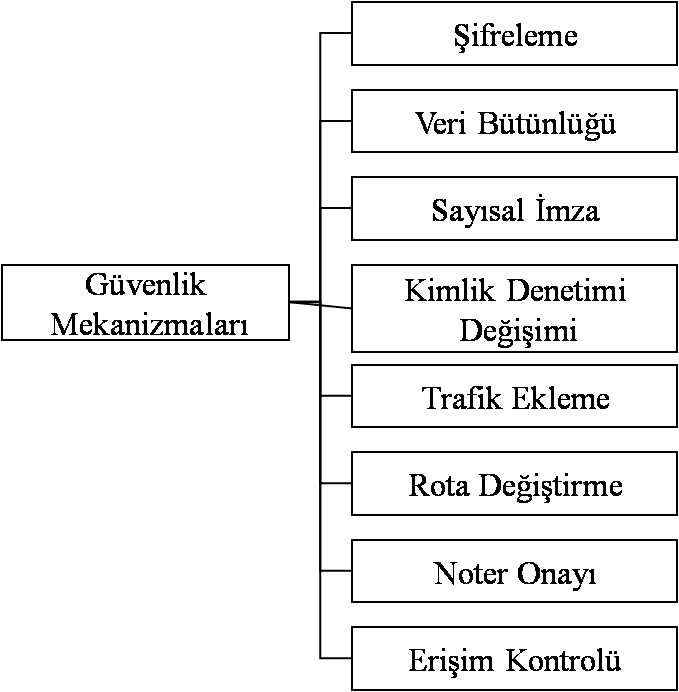
**Veri Bütünlüğü (Data Integrity):** Verinin değişimini, veriye eklemeyi ve bir düşman tarafından tekrar etmesini engellemek amacıyla tasarlanmıştır. Mesajın tümünü veya bir parçasını koruyabilir.

**Kimlik Denetimi (Authentication):** Bu servis hattın sonundaki partinin kimlik denetimini sağlar. Bağlantı tabanlı iletişimde bağlantı kurulması sırasında alıcının ya da göndericinin kimlik denetimini sağlar (Denk varlık kimlik denetimi-peer entity authentication). Bağlantısız iletişimde verinin kaynağının kimlik denetimini sağlar.

**İnkâr Edememe (Nonrepudiation):** İnkâr edememe servisi veriyi hem gönderenin hem de alıcının inkâr etmesine karşı korur. İnkâr edememe de kökenin ispatı ile verinin alıcısı daha sonra eğer gönderici reddederse kimliğini ispat edebilir. İnkâr edememe de dağıtımın ispatı ile verinin göndericisi istenen kullanıcıya verinin iletildiğini ispat edebilir.

**Erişim Kontrolü (Access Control):** Erişim kontrolü veriye yetkisi erişime karşı koruma sağlar. Tanımdaki erişim terimi çok geniştir ve okuma, yazma, değiştirme, programları çalıştırma ve bunun gibi kavramlarla ilişkilidir.

1. **Güvenlik Mekanizmaları**

****

**Şekil 5.** Güvenlik Mekanizmaları

**Şifreleme (Encipherment):** Şifreleme ya da veri gizleme gizliliği sağlar. Buna ek olarak diğer servisleri sağlamak için diğer mekanizmaları tamamlamak için de kullanılır. Bugünlerde şifreleme ve steganography teknikleri şifreleme için kullanılmaktadır.

**Veri Bütünlüğü (Data Integrity):** Veri bütünlüğü mekanizması veriye eklenen kısa bir kontrol değeridir. Bu değer veriden özel bir işlem ile üretilir. Alıcı veriyi alır ve bu değeri kontrol eder. Alıcı tarafta da bu kontrol değeri veri alındıktan sonra yaratılarak gelen kontrol verisi ile karşılaştırılır. Aynı ise verinin bütünlüğü sağlanır.

**Sayısal İmza (Digital Signature):** Sayısal imzada gönderen elektronik olarak veriyi imzalar. Alıcı da bu imzayı doğrular.

**Kimlik Denetimi Değiş Tokuşu (Authentication Exchange):** Kimlik denetimi değiş tokuşunda iki birim kendi kimliklerini ispatlamak için bazı mesajların değiş tokuşunu yapar. Örneğin bir birim bilmesi gereken bir sırrı bildiğini ispat edebilir.

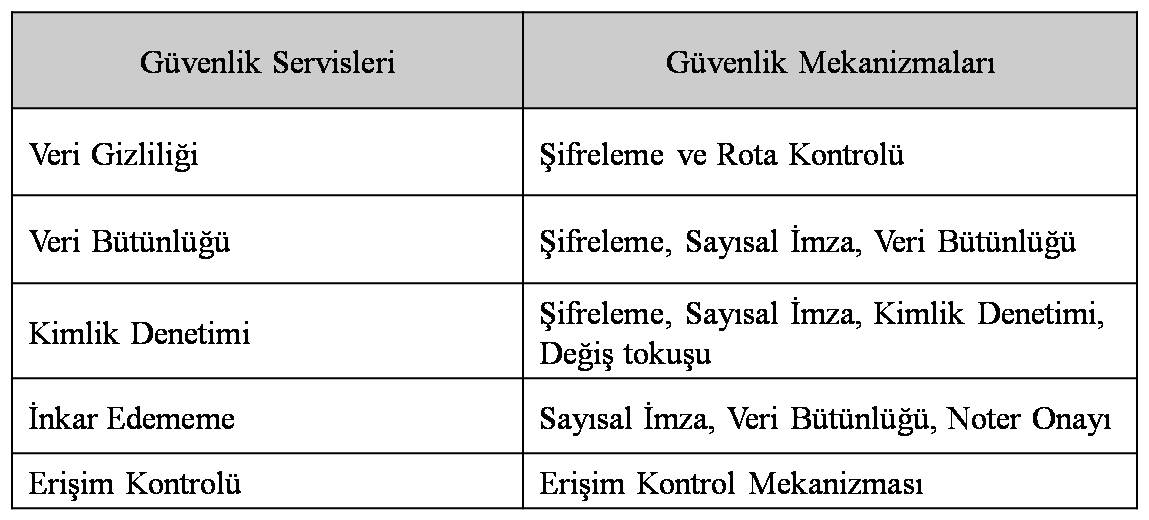
**Trafik Ekleme (Traffic Padding):** Trafik ekleme bazı işe yaramaz verinin (bogus data) veri trafiğine eklenmesi anlamına gelir. Bu yolla saldırganın trafik analizi kullanması engellenmeye çalışılır.

**Rota Kontrolü (Route Control):** Rota kontrolü farklı mevcut rotaların seçilmesi ve devamlı olarak değiştirilmesi anlamına gelir. Bu yolla saldırganın özel bir rotayı sürekli dinlemesi engellenmeye çalışılır.

**Noter Onayı (Notarization):** Noter onayı iki birim arasındaki iletişimin kontrolü içim güvenilir üçüncü bir partinin seçimi anlamına gelir. Bu örneğin inkar etmeyi engellemek için yapılır.

**Erişim Kontolü (Access Control):** Erişim kontrolü bir kullanıcının bir sistemin sahip olduğu kaynaklara ve veriye erişim hakkının olduğunu ispatlamak için kullanılan yöntemlerdir. PIN lerin ve şifrelerin doğrulanması bazı örneklerdir.

Servisler ve mekanizmalar arasındaki ilişki aşağıdaki tabloda verilmiştir.



**Teknikler**

Güvenlik amaçlarının uygulaması için bazı tekniklere ihtiyaç vardır. Biri genel olan kriptografi diğeri ise daha özel olan steganografidir. Kriptogafinin üç farklı mekanizması vardır. Bunlar simetrik şifreleme, asimetrik şifreleme ve hashing olarak özetlenebilir. **Simetrik şifreleme**, Alice güvenli olmayan bir kanaldan Bob’a bir mesaj yollar. Ancak düşman burda Eve olsun. Hattı dinlese bile mesajın içeriğini çözümleyemez. Ancak anahtara sahip olan Bob bu gelen mesajı açarak elde edebilir.

**Asimetrik şifrelemede** simetrik şifrelemedeki durumlar hemen hemen aynıdır. Farklılıklardan biri tek anahtarın yerine iki anahtar vardır: biri açık anahtar diğeri özel anahtar. Bob’a güvenli bir mesaj yollamak için Alice Bob’un açık anahtarını kullanarak mesajı şifreler ve Bob mesajı deşifrelemek için kendi özel anahtarını kullanır.

**Hashing** değişken uzunluktaki bir mesajdan sabit uzunlukta bir mesaj özetleme işidir. Mesaj özeti doğal olarak mesajdan oldukça küçüktür. Kullanışlı olması için mesaj ve mesaj özeti Bob’a yollanmalıdır. Hashing daha öncede söylendiği gibi veri bütünlüğünün sağlanması ile ilgili olarak kontrol değerleri sağlamak için kullanılır.

**Steganography** diğer yandan mesajı başka bir şeyi kullanarak gizlemektir.

**Örnek 1.** Aşağıdaki durumlar için güvenlik saldırılarını tanımlayınız.

1. Bir öğrenci profesörün odasına yarın olacak sınavın soruların kopyasını elde etmek için giriyor.
2. Bir öğrenci kullanılmış bir kitabı almak için 10 $ lık bir çek veriyor. Daha sonra anlıyor ki çek ten 100 $ alınmış
3. Bir öğrenci her gün diğer bir öğrenciye yüzlerce mail gönderiyor phony yollayarak.

**Cevap**

a şıkkında saldırı snooping-trafik gözetleme (bu örnekte depolanmış verinin gizliliğine olan saldırıdır) dir. Her ne kadar testin içeriği sınav günü gizli olmasa da test günüden önce gizlidir.

b şıkkında saldırı değiştirme (modification) saldırısıdır (verinin bütünlüğüne olan saldırıdır). Çekin değeri 10 $ dan 100 $ a değiştirilmiştir.

c şıkkında denial of service saldırısıdır. Kullanılabilirliğe karşı olan saldırıdır. Çok fazla sayıda mail yollamak server’ı çökertebilir ya da servisin çalışmasını durdurabilir.

**Örnek 2.** Aşağıdakilerden durumlardan hangilerinde gizlilik için kriptografi ya da steganography kullanılmıştır.

1. Bir öğrenci bir testin cevaplarını küçük bir kağıt parçasının üzerinde yazar ve onu kıvırıp kalemin içine koyar. Daha sonra diğer öğrenciye iletir.
2. Bir mesajı yollamak için casus mesajdaki her karaktere karşılık daha önce üzerinde anlaşılan bir sembol ile değiştirir.
3. Bir şirket kalpazanlıkları engellemek için çeklerinde özel bir mürekkep kullanır.
4. Bir mezun öğrenci tezini korumak için watermarks kullanır.

a şıkkında testin cevapları değiştirilmemiştir sadece gizlenmiştir (Steganography).

b şıkkında mesajdaki karakterler gizlenmemiştir. Sadece diğer karakterlerle değiştirilmiştir (Kriptografi).

c şıkkında özel mürekkep çek üzerindeki o anki yazıyı gizler (Steganography).

d şıkkı water Marks tezin o anki içeriğini gizler (Steganography).