Bilgi Güvenliği (Anahtarlama-Şifreleme Yöntemleri)

Günümüz sistemlerinde en önemli gereksinimlerden birisi bilgilerin sorunsuz bir şekilde taşınması ve gizliliktir. Verilerin güvenli bir şekilde yollanması ve karşı taraftan alınabilmesi için kriptografi bilimi aracılığıyla geliştirilen çeşitli şifreleme, anahtarlama ve çözümleme algoritmaları kullanılmaktadır. Şifreleme yöntemine, yetkili olmayan kişilerin çözme eğilimlerine dayanıklı, yetkili olanların ise bilgiyi gizlemeleri gerektiğinde eski haline dönüştürebilmelerinde kullanılabilen bir yaklaşım olarak başvurulur.

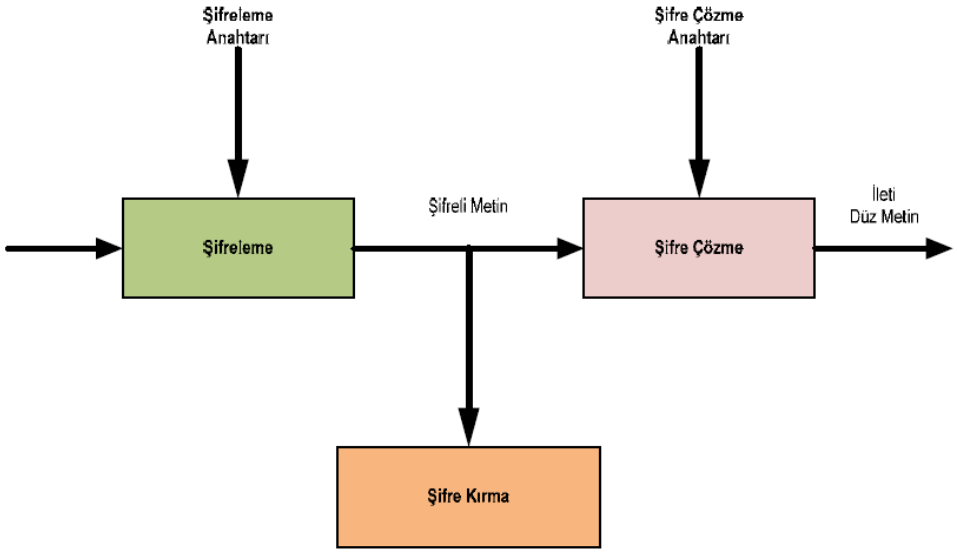
Bu genel olarak (cryptology) gizleme bilimidir. Bu sözcük Yunanca'da (Kryptos) saklı ve (logos) sözcüklerinden oluşur. Gizleme bilimi (cryptography) bilgi gizleme tekniklerini içine alır. Bu sözcük de Yunancadaki kryptos ve (graphein) yazmak sözcüklerinden oluşmaktadır.

Gizleme biliminin içinde ayrıca (cryptoanalysis) gizi kırma, yani şifrelenmiş metinden rakiplerin zekice şifreyi çözümlemeleri de yer almaktadır.

Şifreleme sürecinde sağlaması beklenen kriterler şu şekildedir:

- Şifrelenmiş mesaj, deşifre edildiğinde bilgi kaybı olmamalıdır.
- Şifreleme işlemlerinde güvenlik seviyesi mümkün olduğunca yüksek olmalıdır.
- İhtiyaç duyulan güvenlik seviyesine göre güvenlik seviyesi seçilebilmelidir.
- Şifrelenmiş mesaj ile düz metin arasındaki ilişki zor kurulmalıdır.
- Şifreleme işlemleri basitçe ve kolaylıkla gerçekleştirilebilmelidir.

Genel olarak işlem akışı aşağıdaki şekilde görülmektedir. Şifreleme algoritması şifrelenecek metni ve şifreleme anahtarını girdi olarak alır. Çözümleme algoritması ise şifreleme algoritmasının ters yönünde çalışır.



Genel olarak şifreleme yöntemlerini, algoritmalarına, anahtar sayısına veya mesaj tipine göre sınıflandırmak mümkündür.

Şifrelemenin tarihi gelişimine baktığımızda, şifreleme algoritmalarını gizli şifreleme algoritmalı ve açık şifreleme algoritmalı sistemler olmak üzere ikiye ayırabiliriz.

Gizli algoritmalı sistemlerde, şifreleme algoritması ve şifre çözme algoritması birbirinin tersidir. Öncelikle haberleşecek iki grup aralarında gizli bir algoritma tespit ederler. Eğer bu iki grup birbirleri ile yakın yerlerde değilse, güvenli bir iletişim kanalı veya güvenilir bir kurye ile bu algoritmayı birbirlerine ulaştırırlar. Bu sistemler, algoritmanın gizliliğinin sağlanması zorunluluğu nedeniyle sadece sınırlı kullanıma sahiptirler, yaygınlaşması ve standartlaşması oldukça zordur. Bu tür algoritmalara çoğunlukla kuşkuyla bakılmaktadır. Bu nedenle, gizli algoritmalı klasik şifreleme sistemleri, bankalar ve elektronik ticaret siteleri gibi uygulamalara uygun değildir.

Gizli algoritmalı klasik şifreleme algoritmaları günümüz modern şifreleme algoritmalarına temel teşkil etmiştir. Klasik şifreleme algoritmaları;

- Sezar Şifreleme Algoritması,
- Affine Şifreleme,
- Monoalfabetik Şifreleme ve
- Vigenere Şifreleme

olarak sıralanabilir.

Sezar Şifreleme Algoritması:

Bilinen en eski ve en basit şifreleme yöntemidir. Alfabede her bir harfin belirli sayıda karakter ötelenmesi ile şifreleme tablosu elde edilir. İngiliz alfabesinde yer alan 26 harfe sıfırdan başlayarak sırayla bir pozisyon sayısı atanır. Alfabenin ilk harfi “a” 0 ile son harfi “z” ise 25 ile eşlenir. Açık metinde yer alan her harfin pozisyon sayısı bulunur. Bu pozisyon sayılarının her biri 3 ile toplanır. Bu toplama işlemi sonucunda elde edilen sonuçların mod 26 işlemine göre sonuçları bulunur. Bulunan sayılar şifrelenmiş metinde yer alacak harflerin pozisyon sayılarıdır. Bu pozisyon sayılarına karşı gelen harfler belirlenerek şifreli metin elde edilir.

Affine Şifreleme:

Affine şifreleme yöntemi Sezar yönteminin geliştirilmesiyle elde edilmiştir. Şifreleme işlemi için açık metin belirlenen bir sayı ile çarpılır ve Sezar şifrelemesinde olduğu gibi öteleme miktarıyla toplanır.

Şifreleme fonksiyonu; y = a * x + b mod 26 ve

Çözme fonksiyonu; x = a -1 (y – b) mod 26'dır.

Çözme fonksiyonu için a değerinin mod 26 işleminde tersinin olması zorunludur. Dolayısıyla a değeri {1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 sayılarından biri olarak seçilmek zorundadır. Bu durumda Affine şifrelemesi için anahtar uzayı 12 × 26 = 312 farklı anahtardan oluşabilmektedir. Bu hesaplama İngiliz alfabesi dikkate alınarak yapılmıştır.

Monoalfabetik Şifreleme:

Monoalfabetik şifrelemede anahtar uzayını artırmak için alfabedeki her bir karakter başka bir karakter ile değiştirilerek şifreleme tablosu oluşturulur. Çözümleme ise bu işlemin tam tersi yapılarak elde edilir. Monoalfabetik şifreleme algoritması için uygulanan kaba kuvvet saldırısı ile korsan hiçbir sonuç elde edemez. Ancak bu kez de başka yöntemler kullanarak algoritmayı kırmaya çalışırlar. İngilizcede en sık kullanılan harf "e" dir. Dolayısıyla şifrelenmiş metinde en sık kullanılan karakteri tespit edip "e" karakteri ile yer değiştirilmesi durumunda birtakım çıkarımlar elde edilebilir. Buna ek olarak, dilin yapısıyla ilgili elde edeceği bilgiler yardımıyla, kaba kuvvet saldırısı ile kırılması imkânsız olan bir yöntemin çözülmesi mümkün hale gelebilmektedir.

Vigenere Şifreleme:

Vigenere şifreleme algoritması, monoalfabetik yöntemleri çözmekte kullanılan sıklık analizi saldırılarına karşı olan zafiyeti, şifrelenmiş metinde kullanılan her harfin neredeyse eşit sıklıkta kullanılmasıyla ortadan kaldırmıştır. Vigenere algoritmasında bir parola vardır. Parolanın açık metinden kısa olması halinde parola açık metin uzunluğunca tekrar edilir. Paroladaki her harf açık metindeki "A" karakterine karşılık gelir ve diğer karakterler Sezar şifrelemesinde olduğu gibi ötelenir. Bu yöntemin getirdiği en önemli farklılık açık metindeki bir karakterin birçok farklı karakter kullanarak şifrelenmiş metin oluşturmasıdır.

Anahtara Dayalı Şifreleme

Şifreleme algoritmalarının standart hale gelmesi için geniş bir kullanıma sahip olmaları gerekmektedir. Bu nedenle algoritması herkes tarafından bilinen sistemler tasarlanmıştır. Bu tür şifreleme sistemlerinde, metin sadece alıcı ile göndericinin bildiği bir anahtar kullanılarak bilinen bir şifreleme algoritması ile şifrelenir. Bu nedenle bu sistemlere anahtara dayalı şifreleme sistemleri denir. Modern şifreleme teknikleri anahtar altyapısına dayanan, açık algoritmalı sistemlerdir.

Açık algoritmalı sistemler için temel olarak iki çeşit şifreleme algoritması bulunmaktadır:

1. Simetrik Şifreleme
2. Asimetrik Şifreleme

Simetrik Şifreleme

Simetrik şifrelemede, şifreleme ve şifre çözmek için bir tane gizli anahtar kullanılmaktadır. Bu algoritmalara simetrik denmesinin nedeni, şifreleme ve çözme için tek ve aynı anahtarın kullanılmasıdır. Kullanılan anahtar başkalarından gizlidir ve şifreleme yapan ile şifrelemeyi çözecek kişilerde arasında anlaşılmış ortak bir anahtardır. Gönderilecek gizli metinle beraber üstünde anlaşılmış olan gizli anahtar da alıcıya gönderilir ve şifre çözme işlemi gerçekleştirilir.

Simetrik şifrelemenin en önemli avantajlarından birisi oldukça hızlı olmasıdır. Bununla birlikte simetrik algoritmayı içerdiği basit işlemlerden dolayı elektronik cihazlarda uygulamak çok daha kolaydır. Ayrıca, simetrik algoritmalarda kullanılan anahtarın boyu ve dolayısıyla bit sayısı çok daha küçüktür. Ancak, güvenli anahtar dağıtımı zordur ve kapasite sorunu bulunmaktadır. Kimlik doğrulama ve bütünlük ilkeleri hizmetlerini güvenli bir şekilde gerçekleştirmek de zordur.

Simetrik algoritmalar blok şifreleme ve dizi şifreleme olmak üzere ikiye ayrılmaktadır.

1. Blok Şifreleme Algoritmaları

Blok şifrelemede veri bloklar halinde işlenmektedir. Açık mesajın belirli uzunluklarda bloklara bölünmesi ile çalışır. Bu yönteme göre bölünen bütün bloklar ayrı ayrı şifrelenir ve sonuçta üretilen şifreli metin bu blokların dizilimi ile elde edilir. Bu algoritmalarda iç hafıza olmadığı için hafızasız şifreleme de denilmektedir. Bütünlük kontrolü gerektiren uygulamalarda genellikle blok şifreleme algoritmaları tercih edilir.

En ilkel uygulaması *vigenere şifreleme* yöntemiyledir. Örneğin şifrelenecek olan mesaj: “bilgigüvenliği” olarak kabul edilsin ve yöntemimizdeki blok uzunluğu 4 karakter olsun. Bu durumda bloklarımız:

1. bilg
2. igüv
3. enli
4. ği

şeklinde olacaktır. Şifreleme yöntemi her bloğu ayrı ayrı şifreleyecek ve çıkan sonuçları birleştirerek şifreli metni elde edecektir.

Blok şifreleme, dizi şifrelemeye göre daha avantajlıdır. Çünkü bloklardan karakterleri tahmin etmek daha güçtür.

Bazı blok şifreleme yöntemleri aşağıdaki şekilde sıralanabilir:

- *Hill Şifrelemesi*
  Her blok için verilen anahtar matris ile metindeki karakter değeri çarpılır. Elde edilen sonuçlar toplanarak yeni karakter elde edilir. Şifrenin açılması için matrisin tersinin bulunması gerekir. Tersi alınmış matris ile mesaj çarpılarak açık metin elde edilir.

- *Permütasyon Şifrelemesi*
  Basitçe bir metnin içinde bulunan harflerin verilen anahtar sıralamasına uygun şekilde yer değiştirmesi mantığına dayanan şifreleme yöntemidir. Yazılan metnin yeterli büyüklükte n x n'lik bir karenin satırlarına sırayla yazılması ve sütunların okunarak şifreli metnin oluşturulması esasına dayanır.

- *DES (Data Encryption Standard – Veri Şifreleme Standardı)*
  Şifrelemeyi metin uzunlukları belli olan bloklar halinde gerçekleştirir. DES algoritması aynı zamanda 64 bit uzunluğunda bir anahtar alır. Ancak bu anahtarın geçerli olan uzunluğu 56 bittir çünkü 8 bit partiy için harcanır. Her kullanımında o kullanıma özel yeni bir anahtar yaratması DES'in güçlü yanı olup, günümüz teknolojisi için algoritmasının yavaş ve 56-bit'lik anahtar uzunluğunun yetersiz kalması DES'in zayıf yönleridir. DES için zaman içinde bilgisayarların işlem hızının gelişmesi ile saldırılar kolay hale gelmiştir. 2000'li yılların başında kırılmasıyla günümüz teknolojisi için yetersiz kaldığı görülmüştür ve itibarını kaybetmiştir. DES'in daha zor saldırılır hale gelmesi için 168 bit anahtar uzunluğu kullanan üçlü DES (3DES) uygulaması geliştirilmiştir. SSH gibi günümüzde kullanılan çoğu uygulama DES şifrelemesinin 3 kere art arda yapılması şeklinde çalışan 3DES'i kullanmaktadır. 3DES için şifreleme işlemi 3 kere yapıldığından DES'e göre 3 kat daha yavaştır.

- *AES (Advanced Encryption Standard – Gelişmiş Şifreleme Standardı)*
  DES'e göre daha güvenli bir sistemdir. 128 bit, 192 bit ve 256 bit olmak üzere üç farklı anahtar uzunluğuna sahip olabilir. AES'in DES'in aksine donanımda ve yazılımda hızlı olması, daha kolay uygulanabilir olması ve çok daha az hafızaya gerek duyması güçlü yönleri olarak söylenebilir. AES, durum (state) denilen 4x4 sütun-öncelikli bayt matrisi üzerinde çalışır. Algoritma belirli sayıda tekrar eden girdi açık metni, çıktı şifreli metne dönüştüren özdeş dönüşüm çevrimlerinden (round) oluşmaktadır. Her çevrim, son

çevrim hariç, dört adımdan oluşmaktadır. Şifreli metni çözmek için bu çevrimler ters sıra ile uygulanır. Çevrimlerin tekrar sayıları 128-bit, 192-bit ve 256-bit anahtar uzunlukları için sırası ile 10, 12 ve 14'tür. AES en yaygın olarak kullanılan simetrik şifreleme algoritmasıdır.

- *Feistel Şifrelemesi*
  Adını, alman şifreleme uzmanı Horst Feistel'den alan şifreleme yönteminin en büyük avantajı şifreleme (encryption) ve açma (decryption) işlemlerinin çok benzer olması ve hatta bazı durumlarda aynı olmasıdır. Bu yapıda şifreleme ve açma arasındaki tek fark, anahtar sırasıdır ve bu durum kodlama çalışmasını ve yapılacak işi neredeyse yarıya indirmektedir. Bir feistel ağında temel olarak aşağıdaki 3 işlem çeşitli sıralar ile çeşitli miktarlarda tekrar etmektedir:
  1. Verinin bitlerinin yerinin değiştirilmesi
  2. Basit doğrusal olmayan fonksiyon icrası
  3. Doğrusal karıştırma (XOR)

- *BalonBalığı (Blowfish) Şifrelemesi*
  Feistel ağı kullanan bir blok şifreleme yöntemidir. Balonbalığı şifrelemesinde 16 adımdan oluşan feistel ağı kullanılmaktadır. Bu ağdaki mesaj boyutu 64bit ve anahtar boyutu 32 ile 448 bit arasında değişkendir. Hafıza gereksinimi sebebiyle akıllı kartlar gibi en küçük sistemlerde kullanılamaz. Yüksek şifreleme ve e-posta gibi rutin kullanıcı uygulamaları konusundaki etkinliğiyle başarılı bir algoritma olarak değerlendirilmektedir. Bu yöntemde kullanılan permütasyon dizileri ve yerine koyma kutuları Π pi sayısından elde edilen sayılar ile oluşturulmaktadır. Bilindiği kadarıyla Π pi sayısının tekrar etmeyen yapısından dolayı yöntemin güvenli olduğu düşünülebilir.

- *RC2*

  Daha sonra çıkan RC4, RC5 ve RC6 gibi şifrelemelerin ilkel versiyonudur. Basitçe 64 bitlik bir feistel ağı kullanarak 18 geçişte (round) değişken uzunluklu bir anahtar ile şifreleme yapmaktadır.

2. Dizi Şifreleme Algoritmaları

Dizi şifrelemede veri bir bit dizisi olarak alınmaktadır. Bir üreteç aracılığı ve anahtar yardımıyla istenilen uzunlukta kayan anahtar adı verilen bir dizi üretilir. Bu çeşit şifrelemede algoritmanın girdisi anahtardır. Algoritma, anahtardan rasgele olarak bir diziye çok benzeyen kayan anahtar dizisi üretir. Daha sonra, kayan anahtar dizisinin elemanları ile açık metin veya şifreli metin dizisinin elemanları ikili tabanda toplanarak şifreleme ve şifre çözme işlemi tamamlanır Kayan anahtar üretimi zamana bağlı olduğu için aynı zamanda hafızalı şifreleme de denilmektedir. Telsiz haberleşmesi gibi gürültülü ortamlarda ses iletimini sağlamak için genellikle dizi şifreleme algoritmaları kullanılır.

Asimetrik Şifreleme

Simetrik şifreleme algoritmalarında bulunan en büyük problem anahtar dağıtımıdır. Simetrik algoritma kullanan çok kullanıcılı bir sistemde anahtarın bütün kullanıcılara aynı anahtarın dağıtılması güvenlik açısından problemli olabilir. Her kullanıcıya farklı bir anahtar vermek ise sistemde birçok farklı anahtar olacağı için sıkıntılı olabilir. Bu sorunları çözüm getirmek için asimetrik şifreleme algoritmaları geliştirilmiştir.

Asimetrik şifreleme algoritmalarında anahtar ile şifre çözme anahtarı birbirinden farklıdır. Şifreleme yapan anahtara açık anahtar, şifreyi çözen anahtar ise özel anahtardır. Açık anahtarlar herkese dağıtılabilir, ancak hangi anahtarın kime ait olduğundan da emin olunmalıdır. Bu yüzden sertifikalar kullanılmaktadır. Sertifika açık anahtar ile sahibinin kimliği arasındaki bağlantının belgesidir. Özel anahtar ise sadece şifreyi çözecek kullanıcıda bulunur, açık anahtar ise gizli değildir. Bu yüzden asimetrik şifreleme güvenlik açısından simetriğe göre çok daha başarılıdır.

Az sayıda anahtar kullanarak simetrik şifreleme yapan çok kullanıcılı uygulamalarda ortaya çıkabilecek anahtar fazlalığı durumunu engeller. Bununla birlikte hız ve donanımsal uygunluk gibi konularda asimetrik şifreleme simetriğe göre geri planda kalmıştır.

Asimetrik algoritmaların güvenliğini sağlayabilmek için çok büyük asal sayılar kullanılmaktadır. Bu da zaman açısından çok büyük problemler getirmektedir. Asimetrik bir algoritmayı kullanan sistemler simetrik algoritmaları kullanan sistemlere göre çok daha yavaştır. Ayrıca asimetrik şifreleme algoritmalarının çok büyük sayılar kullanmasından dolayı donanımsal yapılara uyum sağlaması zor olmaktadır.

Kriptografinin ana ilkeleri olarak sayılan; bütünlük, kimlik doğrulama ve gizlilik hizmetinin güvenli bir şekilde sağlanabilir olması ve anahtarı kullanıcının belirleyebilmesi avantajlarına sahiptir. Ancak, şifrelerin uzunluğu sebebiyle algoritmaların yavaş çalışması ve anahtar uzunluklarının bazen sorun çıkarabiliyor olması gibi dezavantajları bulunmaktadır.

Günümüzde simetrik ve asimetrik şifreleme algoritmalarını birlikte kullanarak hem yüksek derecede güvenlik hem de yüksek hızlı sistemler şifrelenebilmektedir. Bu gibi sistemlere melez sistem adı verilir. Anahtar şifreleme, anahtar anlaşma ve sayısal imza işlemleri genellikle asimetrik şifrelemeyle, yığın veri işlemleri ve imzasız veri bütünlüğü korumaysa simetriklerle gerçekleştirilir.

Bazı asimetrik şifreleme yöntemleri aşağıdaki şekilde sıralanabilir:

- *DH (Diffie-Helman)*

  1976 yılında Diffie ve Helman tarafından bulunmuş ilk asimetrik şifreleme algoritmasıdır. DH iki katılımcının öncesinde herhangi bir bilgi alışverişi yapmadan güvenli olmayan bir kanal vasıtasıyla (güvenli bir şekilde) ortak bir şifrede karar kılmalarına yarayan bir

protokoldür. Algoritma anahtar değişimi ile asıl amacı, iki kullanıcının bir anahtarı güvenli bir şekilde birbirlerine iletmeleri ve daha sonrasında da bu anahtar yardımı ile şifreli mesajları birbirlerine gönderebilmelerini sağlamaktır. Diffie–Hellman algoritması oluşturularak simetrik şifreleme algoritmaları için büyük problemi olan gizli anahtarı koruma ve dağıtım büyük ölçüde aşılmıştır. Bununla birlikte Diffie-hellman algoritması sadece ortak gizli anahtarı belirlemekte kullanılmaktadır.

- *RSA (Rivest-Shamir-Adleman)*

1977 yılında R.Rivest, A.Shamir ve L.Adleman isminde üç bilim adamının oluşturduğu yeni asimetrik şifreleme algoritması RSA, anahtar dağıtımının yanında şifreleme ve şifre çözme işlemlerini de gerçekleştirmektedir. RSA, güvenilirliği çok büyük tam sayılarla işlem yapmanın zorluğuna dayanan bir şifreleme tekniğidir. Bir genel anahtarlı şifreleme tekniği olan RSA, çok büyük tamsayıları oluşturma ve bu sayıları işleminin zorluğu üzerine düşünülmüştür. Anahtar oluşturma işlemi için asal sayılar kullanılarak daha güvenli bir yapı oluşturulmuştur. Genel olarak RSA hem mesaj şifreleme hem de elektronik imza amacıyla kullanılan daha çok ticari uygulamalarda tercih edilen tam sayılar üzerinde en iyileştirme yapılarak oluşturulan değerlerden anahtarların üretildiği bir şifreleme teknolojisidir. RSA algoritmasında sistemin güvenilirliğinin yanı sıra hızının da yüksek olması için, kullanılacak anahtarın sayısal büyüklüğü önemlidir. Yeterli güvenilirlik derecesine ulaşmak için gerekli büyüklük Eliptik Eğri Şifreleme (ECC) Algoritması kullanılarak belirlenmektedir. RSA ile günümüzde 1024 bitlik bir anahtar (yaklaşık 300 basamaklı bir sayı) basit uygulamalar için yeterli bir şifreleme tekniği olarak kullanılabilir. RSA algoritması, bir şifreleme algoritması için oldukça basit bir algoritmadır. Buna karşın sürekli çok büyük asal sayı oluşturmak oldukça zor bir işlemdir.

RSA şifreleme sistemin oluşturulmasıyla birlikte asimetrik şifreleme algoritmalarının günümüzde daha yaygın olarak kullanılması sağlanmıştır.