Şifreleme Çeşitleri

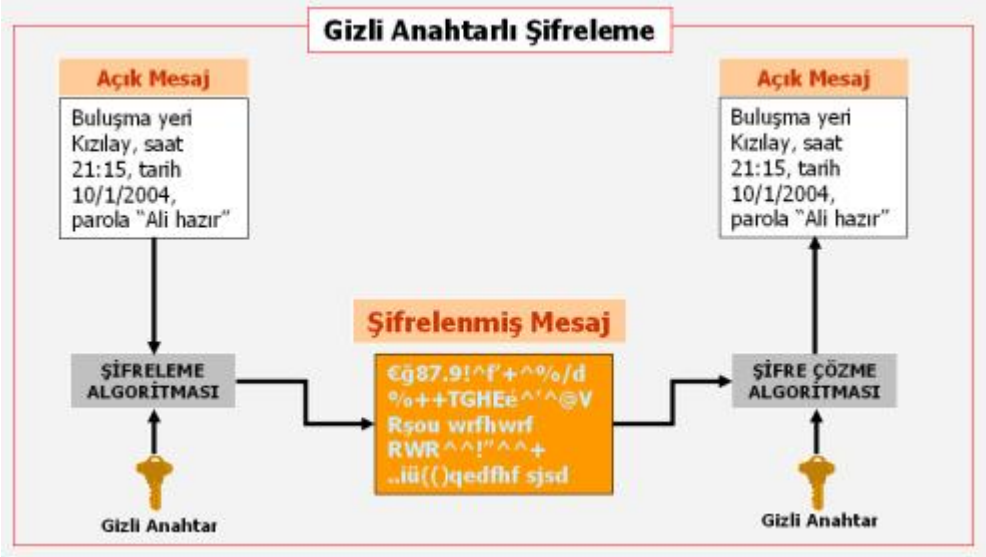
Tarafından: @ahmet sabri mert

Günümüz sistemlerinde en önemli gereksinimlerden birisi bilgilerin sorunsuz bir şekilde taşınması ve gizliliktir. Verilerin güvenli bir şekilde yollanması ve karşı taraftan alınabilmesi için çeşitli şifreleme, anahtarlama ve çözümleme algoritmaları kullanılmaktadır. Şifreleme algoritması şifrelenecek metni ve şifreleme anahtarını girdi olarak alır. Çözümleme algoritması ise şifreleme algoritmasının ters yönünde çalışır.

Günümüzde yaygın olarak kullanılan iki tür şifreleme vardır: simetrik ve asimetrik şifreleme. Aradaki fark, şifreleme ve şifre çözme için aynı anahtarın kullanılıp kullanılmamasından kaynaklanır.

Simetrik şifreleme:

Simetrik şifrelemede, şifreleme ve şifre çözme için aynı anahtar kullanılır. Bu nedenle, anahtarı gönderen ve alıcı arasında aktarmak için güvenli bir yöntemin düşünülmesi çok önemlidir.



Simetrik Şifreleme Şeması

Kuvvetli Yönleri;

- Algoritmalar olabildiğince hızlıdır.
- Donanımla birlikte kullanılabilir.
- Güvenlidir.

Zayıf Yönleri;

- Güvenli anahtar dağıtımı zordur.
- Kapasite sorunu vardır.
- Kimlik doğrulama ve bütünlük ilkeleri hizmetlerini güvenli bir şekilde gerçekleştirmek zordur.

DES (Data Encrytion Standard - Veri Şifreleme Standartı):

1970'lerde bir şifreleme standardı olarak kabul edilen DES şifrelemesinin artık tek başına güvenli olduğu düşünülmemektedir. Bir seferde yalnızca 56 bitlik veriyi şifreler ve piyasaya sürülmesinden kısa bir süre sonra kolayca saldırıya uğradığı anlaşıldı ve günümüzde kullanılmıyor.

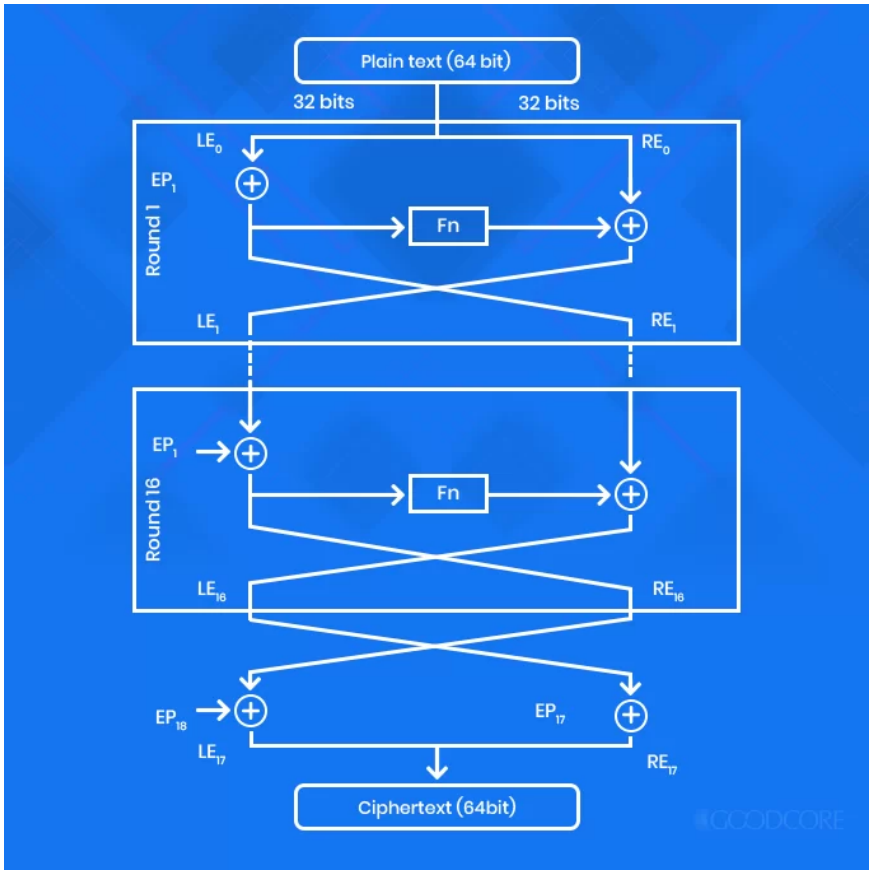
AES (Advanced Encrytion Standard - Gelişmiş Şifreleme Standartı):

En güvenli şifreleme türlerinden biri olan AES, hükümetler ve güvenlik kuruluşlarının yanı sıra günlük işletmeler tarafından sınıflandırılmış iletişimler için kullanılır.
AES, verileri ayrı veri bitleri yerine tek bir blokta şifrelemesi bakımından diğer şifreleme türlerinden farklıdır. Blok boyutları, her tür AES şifreli verinin adını belirler: AES-128, 128 bit boyutundaki blokları şifreler

AES-192, 192 bit boyutundaki blokları şifreler
AES-256, 256 bit boyutundaki blokları şifreler
Farklı blok boyutlarına sahip olmanın yanı sıra, her şifreleme yönteminin farklı sayıda turu vardır. Bu turlar, düz metin bir veri parçasını şifrelenmiş veriye veya şifreli metne dönüştürme işlemleridir. Örneğin, AES-128 10 tur kullanır ve AES-256 14 tur kullanır.

Blowfish:

DES'in yerini almak üzere tasarlanmış başka bir şifreleme algoritması olan Blowfish, 32 bit ile 448 bit arasında değişen bir anahtar uzunluğu üzerinde çalışan simetrik bir blok şifredir. Bir blok şifreleme olduğundan, şifreleme ve şifre çözme sırasında verileri veya bir mesajı sabit 64 bitlik bloklara böler.

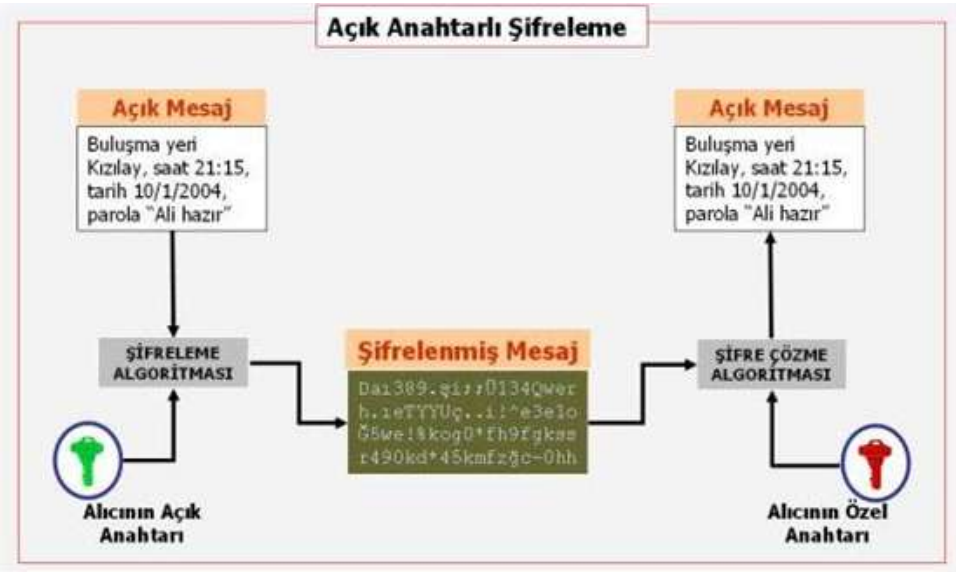


Blowfish Şifreleme Şeması

Asimetrik şifreleme:

Asimetrik şifrelemede bir anahtar çifti kavramını kullanır: şifreleme ve şifre çözme işlemi için farklı bir anahtar kullanılır. Anahtarlardan biri tipik olarak özel anahtar, diğeri ise genel anahtar olarak bilinir.

Özel anahtar sahibi tarafından gizli tutulur ve genel anahtar ya yetkili alıcılar arasında paylaşılır ya da genel olarak herkesin kullanımına sunulur.
Alıcının genel anahtarıyla şifrelenen verilerin şifresi yalnızca ilgili özel anahtarla çözülebilir. Bu nedenle veriler, verilere yetkisiz veya yasa dışı erişim riski olmadan aktarılabilir.



Asimetrik Şifreleme Şeması

Kuvvetli Yönleri;

- Kriptografinin ana ilkeleri olarak sayılan; bütünlük, kimlik doğrulama ve gizlilik hizmeti güvenli bir şekilde sağlanabilir.
- Anahtarı kullanıcı belirleyebilir.

Zayıf Yönleri;

- Şifrelerin uzunluğundan kaynaklanan algoritmaların yavaş çalışması.
- Anahtar uzunlukları bazen sorun çıkarabiliyor olması.

DH (Diffie-Helman):

1976 yılında Diffie ve Helman tarafından bulunmuş ilk asimetrik şifreleme algoritmasıdır. Ortak kanal üzerinden iletişim kuran iki tarafın İnternet üzerinden iletilmeden karşılıklı bir sır oluşturmasını sağlayan bir anahtar değişim protokolüdür. DH, ikisinin konuşmalarını veya verilerini simetrik şifreleme kullanarak şifrelemek ve şifresini çözmek için bir ortak anahtar kullanmasını sağlar.

RSA (Rivest-Shamir-Adleman):

1977 yılında oluşturulan RSA, anahtar dağıtımının yanında şifreleme ve şifre çözme işlemlerini de gerçekleştirmektedir. En iyi şifreleme algoritması olarak kabul edilir, 1024 bit üzerinde çalışır ve 2048 bit anahtar uzunluğuna kadar genişletilebilir. 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.

Referanslar

[1] Hp.com. 2022. *What Are the Different Types of Encryption?* | *HP® Tech Takes* . [online] Mevcut: <https://www.hp.com/us-en/shop/tech-takes/what-are-different-types-of-encryption> [Erişildi 16 Ağustos 2022].

[2] Allan, M., 2022. *6 Types of Encryption That You Must Know About!* . [online] GoodCore Blog. Mevcut: <https://www.goodcore.co.uk/blog/types-of-encryption/> [Erişildi 16 Ağustos 2022].

[3] Bidb.itu.edu.tr. 2022. *Şifreleme Yöntemleri* . [online] Mevcut: <https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/%C5%9Fifreleme-y%C3%B6ntemleri> [Erişildi 16 Ağustos 2022].

[4] Ico.org.uk. 2022. *What types of encryption are there?* . [online] Mevcut: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/what-types-of-encryption-are-there/#1> [Erişildi 16 Ağustos 2022].