Necmettin Erbakan Üniversitesi

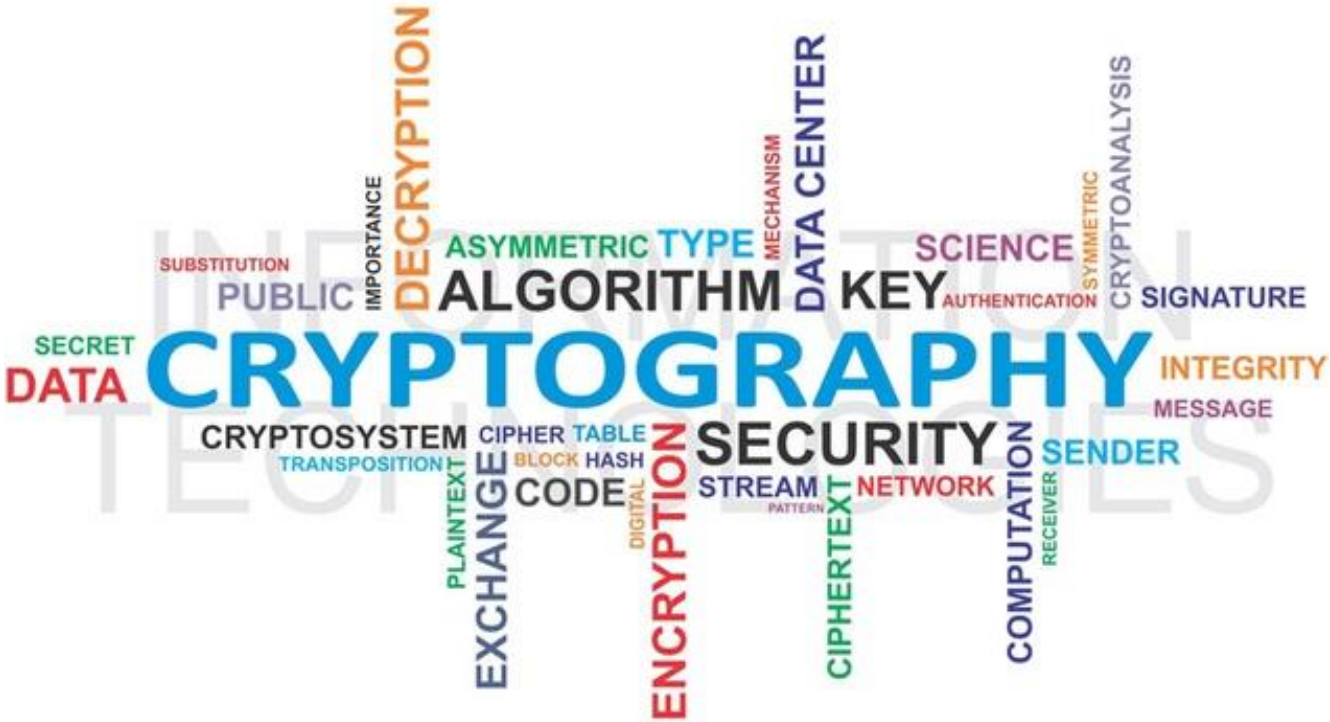
Bilgi Güvenliği
2022-2023 Güz Dönemi

Dr. Alperen Eroğlu
aeroglu@erbakan.edu.tr

Hafta-3

Siber Güvenliğin Temelleri – 1

(Şifre Bilim(Kriptografi), Kullanılan Teknikler)



https://www.enisa.europa.eu/news/enisa-news/cryptographic-tools-are-important-for-civil-society-and-industry

Hafta -3

Siber Güvenliğin Temelleri – 1

(Şifre Bilim(Kriptografi), Kullanılan Teknikler)

- Şifre Bilim Tarihçesi
- Şifre Bilim
- Şifre Bilimde Kullanılan Teknikler ve Algoritmalar
  - Asimetrik Algoritmalar
  - Simetrik Algoritmalar
  - Hibrit Yaklaşımlar

Hafta -3

Siber Güvenliğin Temelleri –II

(Şifre Bilim(Kriptografi), Kullanılan Teknikler)

- Anahtarlar
- Şifreleme Algoritmaları
  - Sezar Şifreleme Yaklaşımı
  - Sezar Açık Anahtar Şifreleme Yaklaşımı
  - Polialfabetik Şifreleme Yaklaşımı
  - Vernam (One-time Pad) Şifreleme Yaklaşımı
  - DES (Data Encryption Standard) Algoritması
  - RSA (Rivest, Shamir ve Adleman) Algoritması
  - AES Algoritması

Hafta -3

Siber Güvenliğin Temelleri –II

(Şifre Bilim(Kriptografi), Kullanılan Teknikler)

- Özetleme (Hashing) Algoritmaları
- Şifre Bilim Standartları
- Steganografi
- Kuantum Şifreleme
- Güvenlik Protokolleri
  - PGP
  - SSL/TLS
  - SSH
  - S/MIME
  - IPSec
  - Kerberos
- Elektronik İmza (E-İmza)

Şifre Bilim Tarihçesi

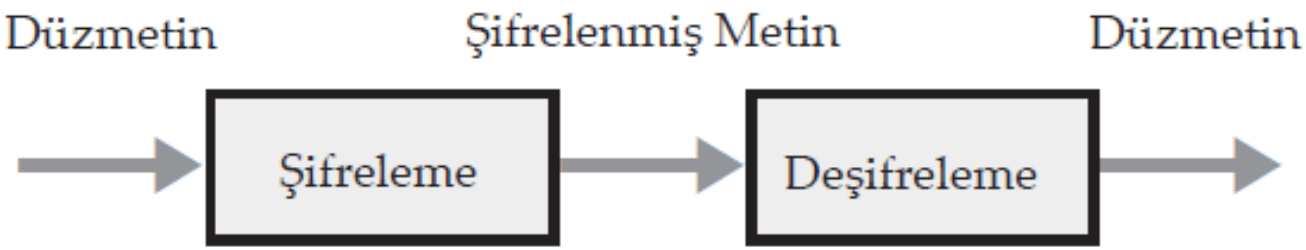
- M.Ö. 100-44 yılları arasında sunulan Sezar yaklaşımı, birçok bilim insanının da teyit ettiği gibi kullanılan ilk şifreleme yaklaşımlarındandır.
- ...
- 1970'lerde IBM ile başlayan çalışmalar, ABD Federal Bilgi İşleme Standardının (USA Federal Information Processing Standard) benimsenmesiyle, DES (Data Encryption Standard) veri şifrelemede bir standart olarak kabul edilmiştir.
- 1976 yılında Diffie-Hellman tarafından geliştirilen açık anahtarlı şifreleme yaklaşımı,
- 1978'de Ronald L. Rivest, Adi Shamir ve Leonard M. Adleman: RSA algoritmasını buldular.
- 1991'de Phil Zimmerman: PGP sistemini geliştirdi ve yayınladı.
- 1995'te SHA-1 (Secure Hash Algorithm) özet algortiması NIST tarafından standart olarak yayınlandı.
- 2001'de NIST'in yarışmasını kazanan Belçikalı Joan Daemen ve Vincent Rijmen'e ait Rijndael algoritması, AES (Advanced Encryption Standard) adıyla standart haline getirildi.

Şifre Bilim

- Verilerin güvenli olarak bir ortamdan diğerine aktarılmasında veya saklanmasında **matematiksel yaklaşımlar** sıkça kullanılmaktadır. Şifreleme bilimi **(kriptoloji)**, kriptografi ve kripto analiz olmak üzere iki alanı kapsayan bilim dalıdır. **Kriptografi;** matematik, elektronik, optik, bilgisayar bilimleri gibi birçok disiplini içeren özelleşmiş bir bilim dalıdır. Kabaca, belgelerin veya bilgilerin şifrelenmesi ve şifrelerinin çözülmesi için kullanılan yöntemlere verilen genel addır. Bir başka ifadeyle, üçüncü şahıslar tarafından algılanamayacak veya öğrenilemeyecek farklı bir forma veriyi işleyerek dönüştürme işlemidir.

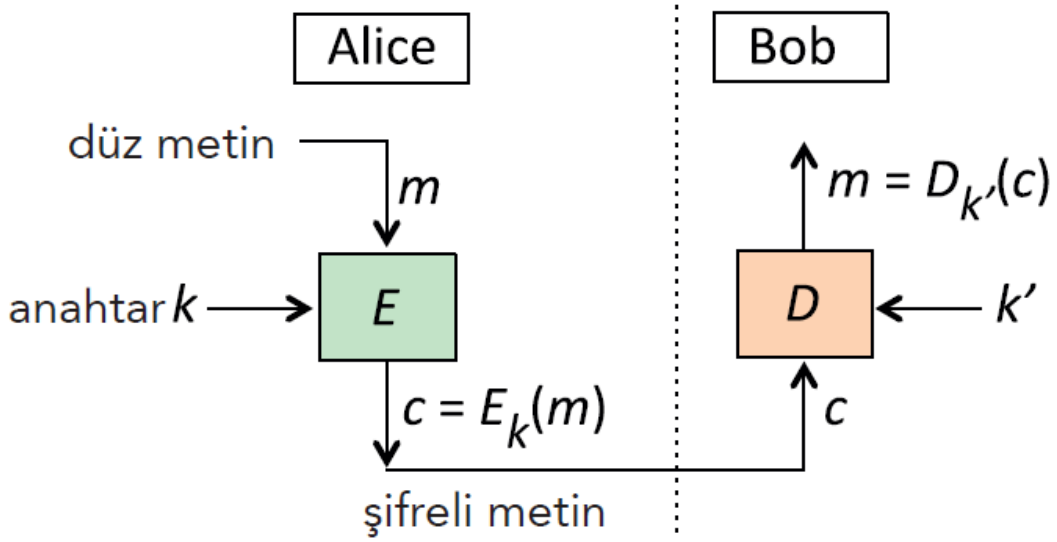
Şifre Bilim

Matematiksel temele dayanan bu bilimde, matematiksel fonksiyonlar, şifreleme (**encryption**) ve şifre çözme (deşifre - **decryption**) için kullanılır. ***Şifreleme***, düzmetni (**plaintext**) anlaşılamayacak bir forma dönüştürme işlemidir. Bu işlem, matematiksel bir fonksiyon ve bir anahtar veya anahtar çiftinin biri kullanılarak yapılır. **Deşifreleme** ise, şifrelenmiş mesajı (**ciphertext**), şifrelemede kullanılan fonksiyonun tersini ve bir anahtar veya anahtar çiftinin diğerini kullanarak düzmetine dönüştürme işlemi olarak tarif edilebilir.



Şifreleme ve Deşifreleme (Şifre Çözme) İşlemleri

Şifreleme ve Şifre Çözme (Genel Kavramlar)



$$c = E_k(m); \qquad m = D_{k'}(c)$$

Şifre Bilim

Kriptoanaliz ise; kriptografik sistem mekanizmalarını ve yaklaşımlarını inceleme ve çözme bilimidir. Şifrelenmiş verileri çözmek veya onları anlamlı hale getirme yaklaşımlarını içerirler.

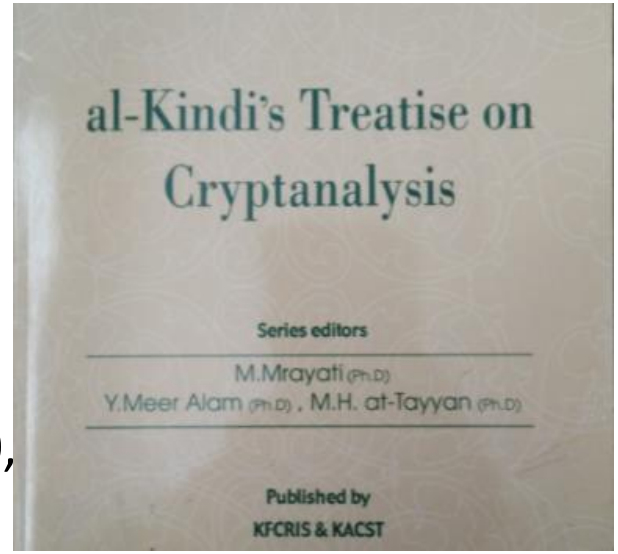
Ortaya konan bir şifreleme sistemini inceleyerek, zayıf ve kuvvetli yönlerini ortaya çıkarmak için kullanılabileceği gibi, şifrelerin çözülmesi için de kullanılabilir.

İşlemler sırasında, yoğun **istatistik, matematik ve bilgisayar gücüne** ihtiyaç vardır.

Kriptoloji = Kriptografi + Kriptanaliz

İlk Kriptanaliz Kitabı

- Bilinen en eski kriptanaliz kitabı El Kindi tarafından yazılmıştır,
- MS 801 ile MS 873 yılları arasında yaşamıştır.
- El-Kindi'nin kitabının ana konuları kriptanaliz yöntemleri, şifrelerin kriptanalizi ve Arapça'nın frekans analizidir.
- El-Kindi'nin ilgili el yazması eseri İstanbul'daki eski bir kütüphanede bulunmuştur.
- Uluslararası Kriptolojik Araştırmalar Birliği bülteni Vol. 20, No. 3, Güz 2003, El-Kindi'nin eserinin çevirisinin bir incelemesini içermektedir: http://www.iacr.org/newsletter/v20n3/newbooks.html



Şifre Bilim

Kriptoanaliz yöntemleri, **kaba kuvvet** ve **diferansiyel kriptoanaliz** olmak üzere ikiye ayrılır. ***Kaba kuvvet***, bir şifreleme algoritması tarafından kullanılan bir anahtarı veya anahtar çiftini, **tüm anahtarları tek tek veya belirli bir mantık çerçevesinde deneyerek**, kullanılmış olan şifreleme anahtarını bulma yaklaşımı iken, *diferansiyel* ***kriptoanaliz***; bilinen **açık şifreli mesaj çiftleri arasındaki farkların hesaplanması** temeline dayanır.

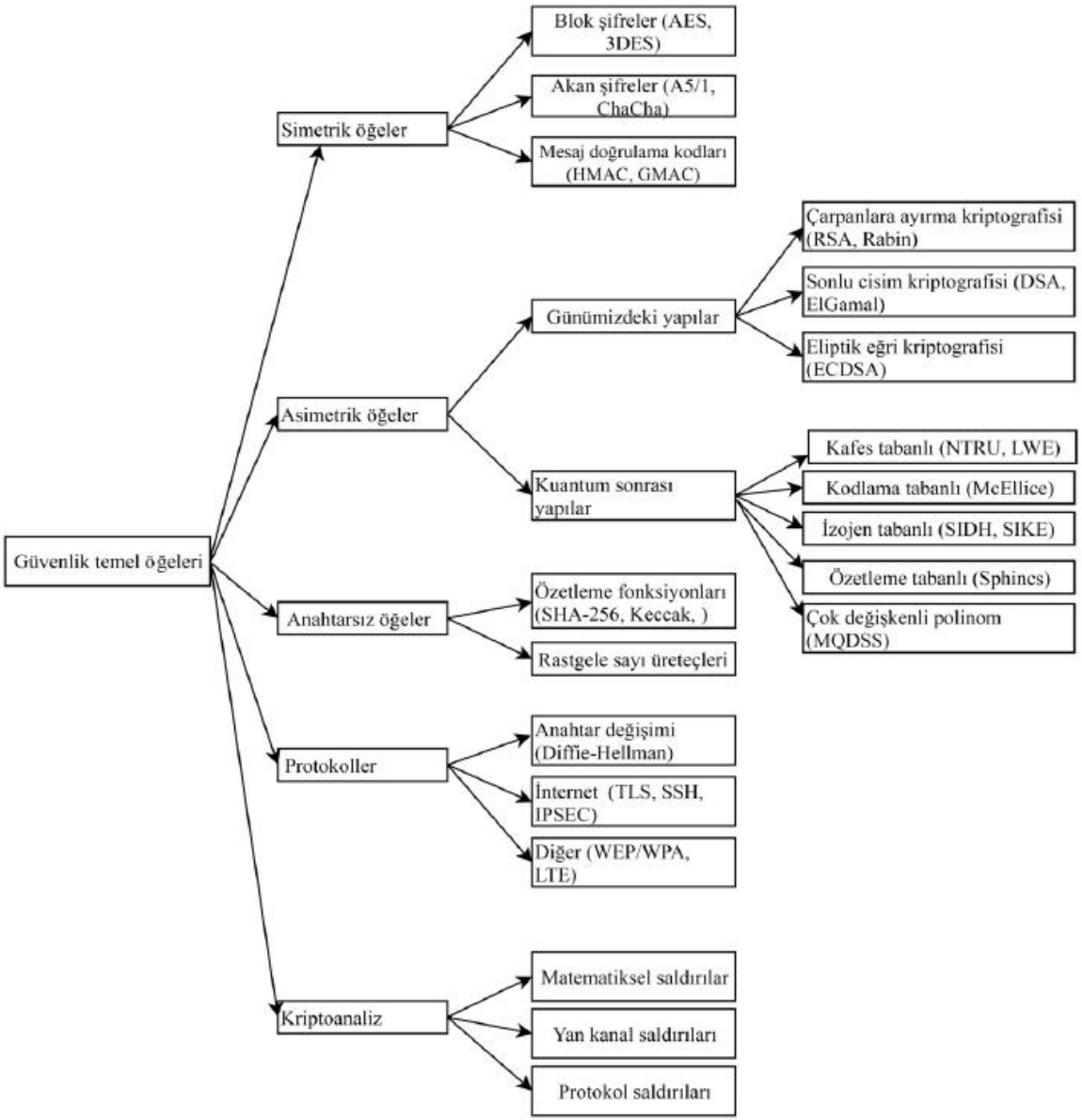
Genel (Kapsamlı) Anahtar Arama

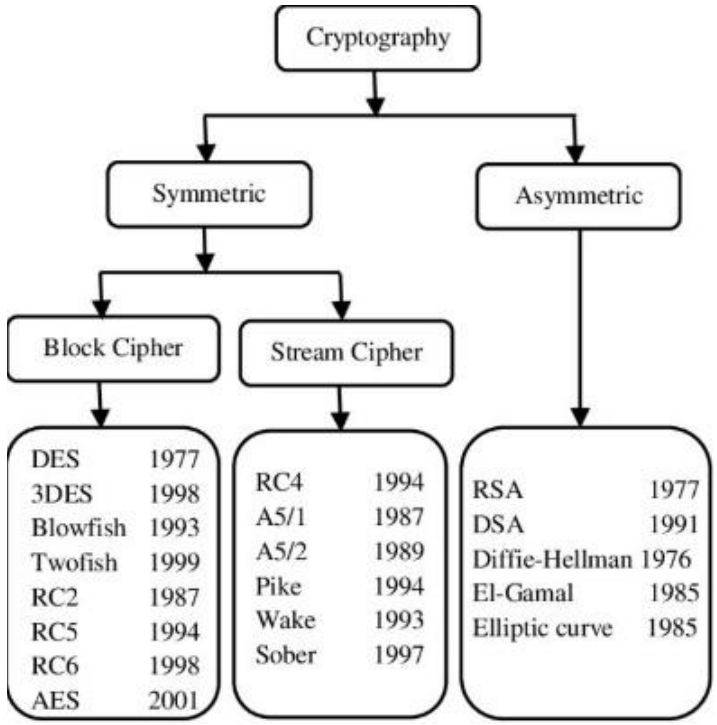
- E ve D algoritmalarının kritik bir özelliği, *m*'yi *k* olmadan *c*'den elde etmenin mümkün olmamasıdır.
- *k* bilgisi olmadan bir saldırganın, bir şifreli metin *c*'yi elde ettiğinde yapabileceği en iyi şey, K anahtar uzayındaki tüm *k* anahtarlarını denemektir:
  - D'yi her k ile sırayla parametrelendirmek, her $D_k(c)$'yi hesaplamak ve anlamlı bir sonuç aramaktır (kapsamlı anahtar arama – exhaustive key search)
- Algoritmik zayıflık yoksa, algoritmik "kısayol" saldırıları yoktur ve tüm anahtar uzayı denenmelidir. Ortalama şansa sahip bir saldırganın, anahtar uzayının yarısını denedikten sonra doğru anahtara ulaşması beklenir.

Şifre Bilimde Kullanılan Teknikler ve Algoritmalar

Şifreleme ve şifre çözme işlemlerinde kullanılan birçok algoritma, teknik ve yaklaşım mevcuttur. Genel olarak değerlendirildiğinde, şifreleme yaklaşımları, kapalı anahtarlı ve açık anahtarlı olmak üzere ikiye ayrılır. ***Kapalı anahtarlı*** yaklaşımlar, ***simetrik*** yaklaşımlar olarak da bilinmektedir. Bu yaklaşımda, hem şifreleme hem de şifre çözme işlemi için **tek bir anahtar** kullanılır. En popüler kapalı anahtarlı şifreleme yaklaşımı veri şifreleme standardı olarak isimlendirilen **DES** (Data Encryption Standard)'dir. ***Açık anahtarlı*** yaklaşımlar, ***asimetrik*** yaklaşımlar olarak da bilinmektedir. Kullanıcı **bir çift anahtara** yani hem **açık** bir anahtara hem de **gizli** bir anahtara sahiptir. Bu anahtarlar, **özel** (private) veya **gizli**, ve **genel** (public) veya **açık** olarak da isimlendirilir. Açık (genel) anahtar, herkese açıkken, gizli (özel) anahtar ise, sadece kişiye özeldir. Şifreleme açık anahtarla yapılırken, şifre çözme işlemi gizli anahtarla yapılmaktadır. Bunun tersi de mümkündür. Açık anahtarlı şifreleme yaklaşımlarında en popüler yaklaşım, **RSA** (Rivest, Shamir ve Adleman'in baş harflerinden oluşmuştur)'dır.

Şifre Bilimde Kullanılan Teknikler ve Algoritmalar





Şekil 2.1. Güvenlik temel öğelerinin sınıflandırılması

Şifre Bilimde Kullanılan Teknikler ve Algoritmalar

Güvenlik Unsurları	Simetrik yaklaşımlar	Asimetrik yaklaşımlar
Gizlilik	Sağlar	Sağlar
Bütünlük	Sağlar	Sağlar
Kimlik doğrulama	-	Sağlar
İnkar edemezlik	-	Sağlar
Hesaplama hızı	Yüksek	Düşük
Güvenlik	Anahtar uzunluğuna bağlı	Anahtar uzunluğuna bağlı
Genel değerlendirme	Şifrelemede iyi sonuç veriyor.	Anahtar şifrelemede iyi sonuç veriyor.

Şifreleme Yaklaşımlarının Karşılaştırılması

Simetrik algoritmalar hızlı mesaj şifrelemede, **asimetrik şifreleme yaklaşımları** da yavaş oldukları için **anahtar şifrelemede** yüksek performans gösteren yaklaşımlardır. Genel olarak ise, asimetrik yaklaşımlar, hesaplama hızları düşük olsa da güvenlik unsurlarının tamamını desteklemeleri açısından çok önemlidir.

Asimetrik Algoritmalar

Açık anahtarlı algoritmalar olarak bilinmektedirler.

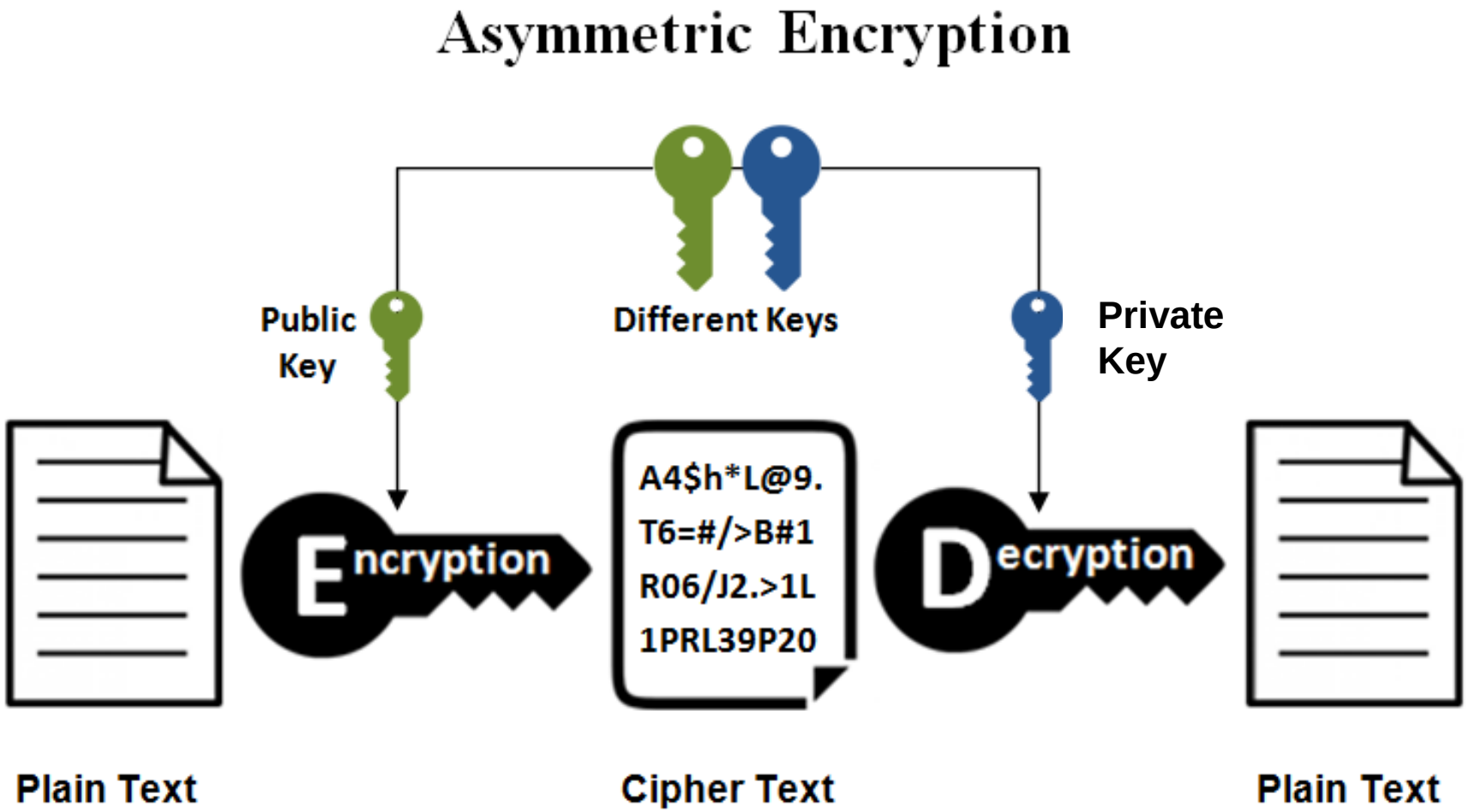
Bu algoritmalarda, şifreleme ve şifre çözme için farklı anahtar çiftleri kullanılmaktadır. Bu anahtarlar çift olarak üretilirler, tek yönlü çalışırlar, fakat birbirlerini tamamlarlar. Bu anahtar çiftinde, şifreleme anahtarı **açık anahtar** veya **genel anahtar** (public key), şifre çözme anahtarı ise **gizli anahtar** (secret key) veya **özel anahtar** (private key) olarak adlandırılır. Simetrik algoritmalardaki gizli anahtarlar ile karıştırılmaması için, gizli anahtar yerine özel anahtar teriminin kullanımı daha yaygındır.

Asimetrik Algoritmalar

Açık Anahtarlı Şifreleme ve Şifre Çözme İşlemi

Açık anahtar şifreleme işleminde, açık anahtarlarla şifrelenen düz metinler veya mesajlar, yalnız gizli anahtar kullanılarak deşifre edilebilir. Bu işlemi gösteren yaklaşım Şekil'de verilmiştir. Gizli anahtar sadece ait olduğu kişide bulunurken, açık anahtar çeşitli şekillerde insanlara iletilebilmektedir, yani açık olarak dağıtılmaktadır. Bu algoritmalara açık anahtarlı algoritmalar denmesinin sebebi, açık anahtarın herkese, yani genel kullanıma açık olmasıdır.

Asimetrik Algoritmalar



https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Asimetrik Algoritmalar

Farklı biri, bir bilgiyi şifrelemek için birinin genel anahtarını kullanırsa, sadece o ilgili birinin özel anahtarına sahip bir kişi, bu bilginin şifresini çözebilir. Bilgiler, genel anahtar ile şifrelenip özel anahtar ile çözülebileceği gibi, özel anahtarla şifrelenip genel anahtarla çözülebilirler.

RSA, açık anahtarlı şifreleme tekniğidir ve çoğunlukla tercih edilen bir yaklaşımdır.

Asimetrik Algoritmalar

Diğer bir açık anahtarlı şifreleme tekniği, ***Sayısal İmza Algoritması*** **(Digital Signature Algorithm-DSA)**'dır ve bu teknik imzalama için kullanılır. **Eliptik Eğri Şifreleme Sistemi (Elliptic Curve Crypto systems)** ise eliptik eğriler olarak bilinen matematiksel nesneler üzerine oluşturulmuş, şifrelemede kullanılan yaklaşımlardandır. **Diffie-Hellman Anahtar Anlaşması Protokolu (Diffie-Hellman Key Agreement Protocol)**, güvensiz bir kanalda gizli anahtar oluşturmada kullanılan diğer bir popüler açık anahtar şifreleme tekniğidir.

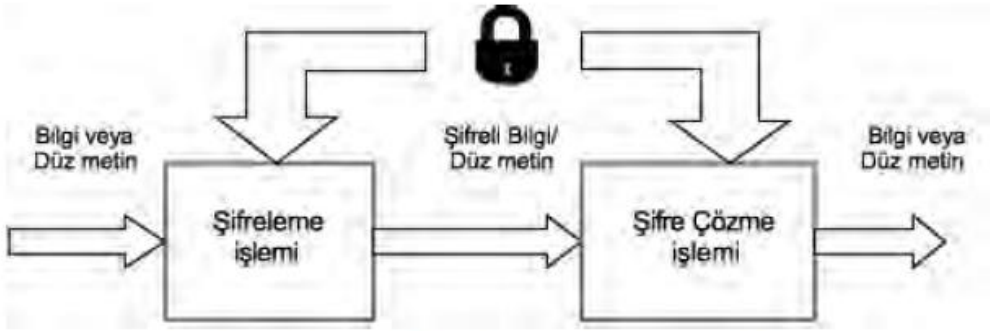
Simetrik Algoritmalar

Bu algoritmalar, *özel, tek veya gizli anahtarlı* geleneksel algoritmalardır ve çoğunda **şifreleme anahtarı ile şifre çözme anahtarı aynıdır**.

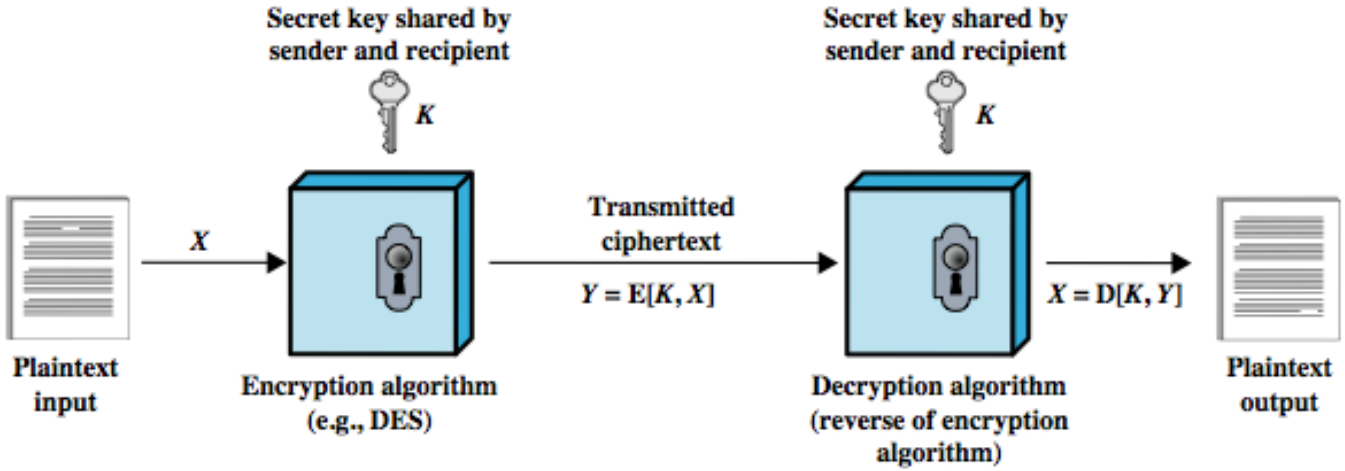
Güvenli bir iletişim için gönderici ile alıcı, bir gizli anahtar üzerinde uzlaşırlar. Seçilen gizli anahtar ile, mesajlar veya düz metinler şifrelenir veya şifrelenmiş mesajların, düz metinlerin şifreleri çözülebilir. Birbiri ile şifreli haberleşmek isteyen taraflar, seçilen gizli anahtarı paylaşmak zorundadırlar.

Simetrik Algoritmalar

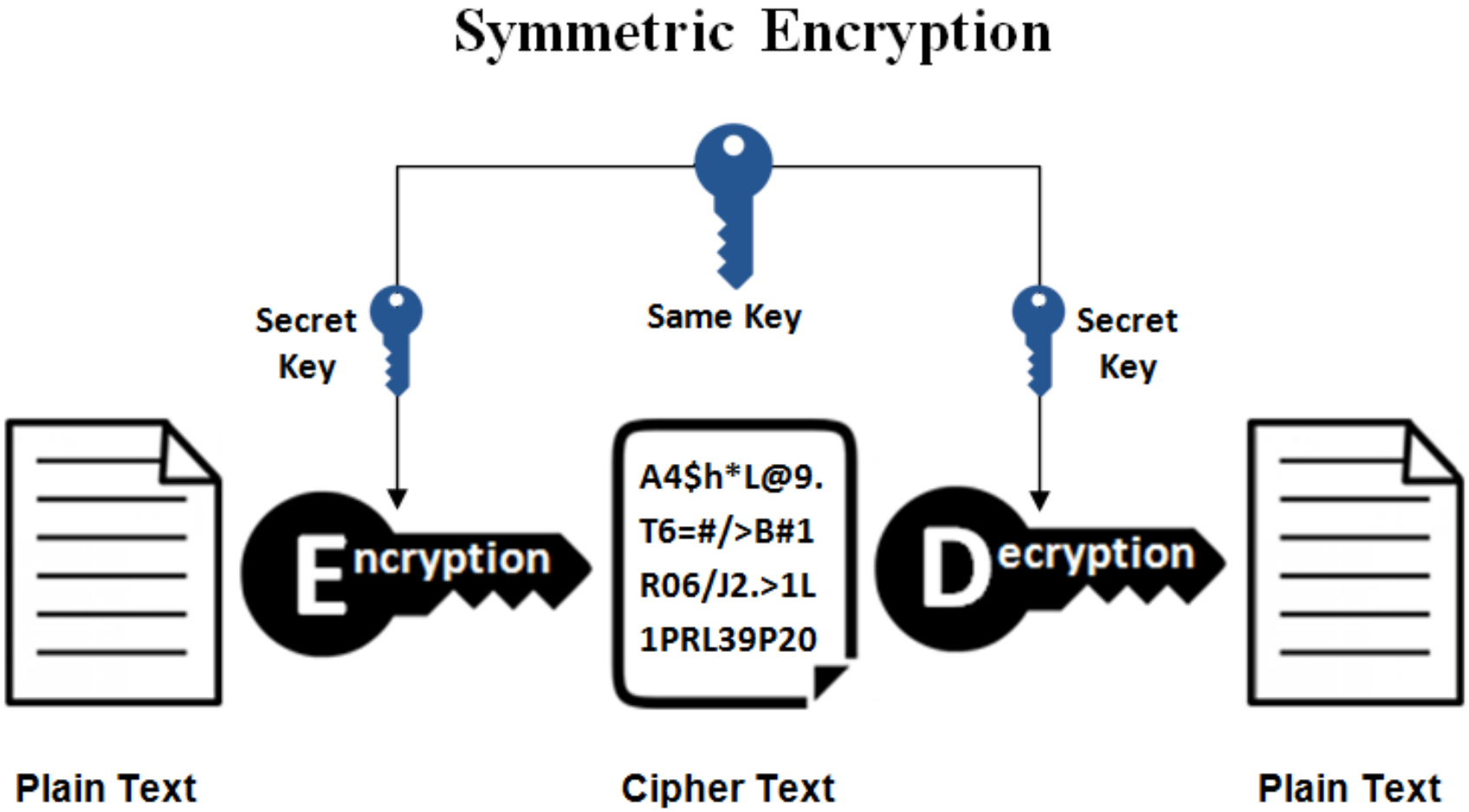
Simetrik algoritma yaklaşımının daha açık anlaşılması için şifreleme ve şifre çözme yaklaşımını detaylı gösteren blok çizim Şekil'de verilmiştir.



Tek Anahtarlı (Gizli) Şifreleme ve Şifre Çözme İşlemi



Simetrik Algoritmalar



https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Simetrik Algoritmalar

Anahtarın genel kullanıma sunulması, isteyen herkesin şifrelenmiş mesajları çözebileceği anlamına geldiği için, bu yaklaşımda anahtarlar gizli tutulmak zorundadır. Modern bilgisayarlar ile kullanılan anahtarın bulunabilmesi mümkün olduğundan, **simetrik algoritmalarda güvenlik anahtar uzunluğuyla doğru orantılıdır**. Günümüzde kabul edilebilir anahtar büyüklüğü en az 128 bit olup iletişimin gizli kalması için anahtarın da gizli tutulması şarttır.

DES ve **3DES** en çok kullanılan yaklaşımlardandır.

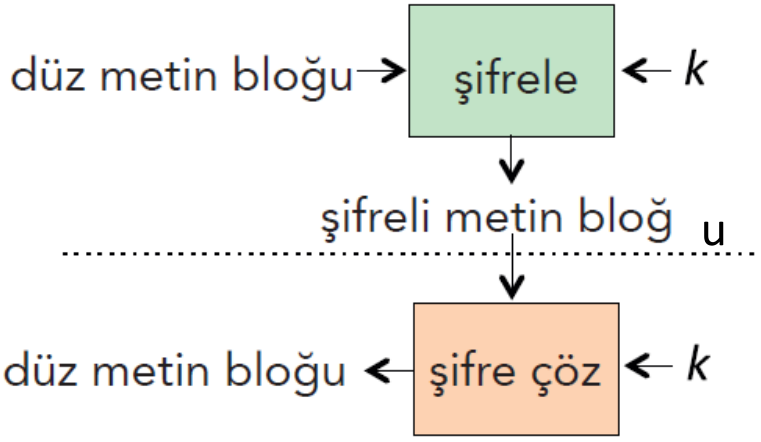
Akış Şifreleme (Stream Ciphers)

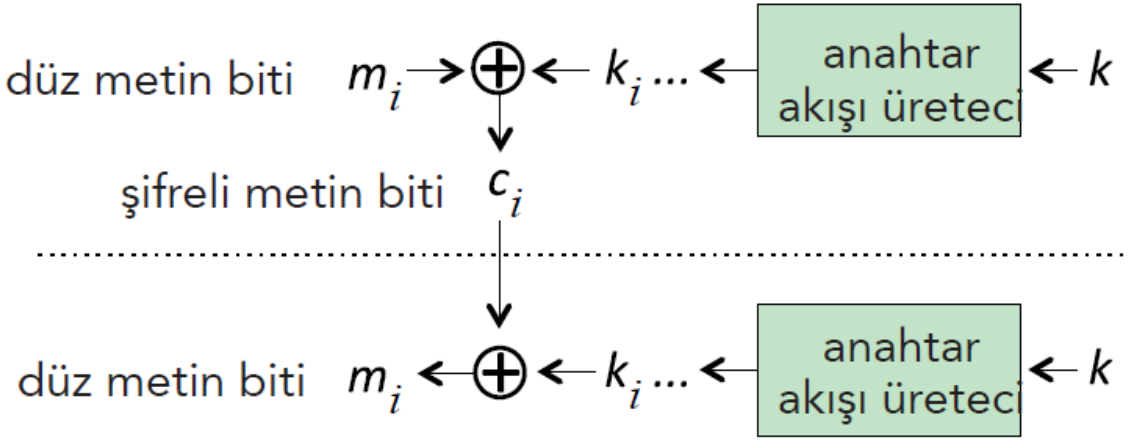
- Şifre çözme, şifreli metin ile aynı anahtar akışına XOR işlemi yapılmasını içerir.
- Blok şifremenin aksine, düz metin uzunluğunun belli bir uzunluğun (örnek: 128 bit) katı olması gibi bir gereklilik yoktur. Bu nedenle akış şifreleme, sırayla bir bit veya bir karakter şifrelemek gerektiğinde uygundur.
  - örneğin, uzak bir siteye gerçek zamanlı olarak gönderilen ve kullanıcı tarafından yazılan karakterler.
- Akış şifreleme, sabit boyutlu bir gizi (simetrik anahtar) saldırganlar için tahmin edilemeyen istenen uzunlukta bir gizli anahtar akışına (secret keystream) dönüştürür.

Blok Şifreleme

- İkinci bir simetrik şifreleme yöntemi olan blok şifreleme, düz metni sabit uzunlukta parçalar ve bloklar halinde işler.
- Her blok (örneğin bir grup ASCII kodlu karakter), anahtara bağlı olarak sabit bir dönüşümle şifrelenir.
- Kara kutu (giriş-çıkış) perspektifinden, bir blok şifrelemenin ana özellikleri blok uzunluğu (bit cinsinden blok boyutu) ve anahtar uzunluğu (bit cinsinden anahtar boyutu)'dur.
- Blok şifreleme kullanılırken, son düz metin bloğu blok uzunluğundan daha az bit içeriyorsa, "dolgu" karakterleri ile doldurulur.

Akış Şifreleme ve Blok Şifreleme





Mesaj Genişlemesi

- Simetrik şifreler tipik olarak uzunluğu korurlar, yani şifreli metin düz metinden daha fazla yer tüketmez, bu durumda yerinde şifreleme mümkündür (örneğin, bir depolama bağlamında, düz metin, ek bellek gerektirmeden şifreli metin ile değiştirilebilir).
- Bununla birlikte, çoğu zaman, bütünlük garantileri sağlamak için, şifreli metne, mesaj genişlemesini içeren bir kimlik doğrulama etiketi (authentication tag) eşlik eder.
- Ayrıca, ilgili parametreler için ek alan da gerekebilir (örneğin, IV'ler veya nonce değerleri).

Simetrik vs. Asimetrik Algoritmalar

Key Differences	Symmetric Encryption	Asymmetric Encryption
Size of cipher text	Smaller cipher text compares to original plain text file.	Larger cipher text compares to original plain text file.
Data size	Used to transmit big data.	Used to transmit small data.
Resource Utilization	Symmetric key encryption works on low usage of resources.	Asymmetric encryption requires high consumption of resources.
Key Lengths	128 or 256-bit key size.	RSA 2048-bit or higher key size.
Security	Less secured due to use a single key for encryption.	Much safer as two keys are involved in encryption and decryption.
Number of keys	Symmetric Encryption uses a single key for encryption and decryption.	Asymmetric Encryption uses two keys for encryption and decryption
Techniques	It is an old technique.	It is a modern encryption technique.
Confidentiality	A single key for encryption and decryption has chances of key compromised.	Two keys separately made for encryption and decryption that removes the need to share a key.
Speed	Symmetric encryption is fast technique	Asymmetric encryption is slower in terms of speed.
Algorithms	RC4, AES, DES, 3DES, and QUAD.	RSA, Diffie-Hellman, ECC algorithms.

https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Hibrit Yaklaşımlar

Simetrik algoritmaların hızlı olması, asimetrik algoritmaların güvenilir fakat yavaş olması ***Hibrid Kriptosistem*** adı verilen bir yapının ortaya çıkmasına sebep olmuştur.

Simetrik algoritmalarda en büyük problem anahtarın karşı tarafa iletimindedir. Bu yapı temelde bilginin simetrik bir algoritma ile şifrelenmesini, bu algoritmada kullanılan anahtarın da asimetrik bir algoritma ile şifrelenip gönderilecek bilgi ile birlikte iletilmesinde temel teşkil eder.

Böylelikle bilginin şifrelenmesi, simetrik algoritmadan dolayı hızlı olup, anahtarın iletimi de, asimetrik algoritmadan dolayı güvenli olacaktır. Bu yapıların ortak kullanılması ile hız ve güvenirlik bir arada sağlanabileceğinden, verimlilik artmaktadır. Bundan dolayı birçok işlemde, bu ve buna benzer yaklaşımlar tercih edilmekte ve geliştirilmektedir.

Anahtarlar (Keys)

Modern kriptolama yaklaşımları, anahtar tabanlıdır. Anahtarın güvenliğinin sağlanması, sistemin genel güvenliğinin sağlanması ile eş anlamlı sayılabilir. Dolayısıyla anahtarlar, kriptografik yaklaşımların temel yapı taşlarıdır ve güvenlik, anahtarın güvenliğine veya bit katarlarının uzunluğuna bağlıdır.

Şifrelemede Kullanılan Anahtar Örnekleri

= **110011111111111111111100000000001110001110000001**

(a) Şifrelemede Kullanılan 48 Bitlik Bir Anahtar

= 2489349e894859f45489450dab45454ca0908d8809

(b) Farklı Formda Bir anahtar Örneği

Anahtarlar

Anahtar uzunlukları farklılıklar göstersede, anahtarlar, büyük bir sayı kümesinden seçilmiş değerlerdir. Mesela; 48 bitlik bir anahtara örnek bir önceki Şekil'de verilmiştir. Burada anahtarlar bit olarak ifade edilebildiği gibi farklı bir formada da sunulabilir. Base64 buna bir örnek olarak verilebilir.

Anahtarların farklı uzunluklarda olabileceğini belirtmiştik.

Eğer 1024 bit uzunluğunda bir anahtar kullanılıyorsa, 2^{1024} farklı değer içerisinden seçilen bir sayının veya bu değerlerden birisinin anahtarınız olabileceğini hatırlatmakta fayda vardır.

Anahtarlar

Simetrik algoritmalarda, yetkilendirilmiş kişilerin değişiminde veya işten ayrılmasında yeni bir anahtar değişikliğine ihtiyaç duyulabilir.

Anahtarları ve anahtarın önemini anlamak için, anahtarlara farklı açılardan bakılmasında ve farklı değerlerle mukayese etmemizde fayda vardır.

Mesela; $2^{64}=10^{19}$ değerinde bir büyüklüğü ifade eder. 64 bitlik bir anahtar, 2^{64} farklı 1100111111111111 1111110000000000 1110001110000001 1000000011001101 oluşmaktadır. Bu bitleri, ikili taban yerine 16'lık veya farklı tabanlara göre ifade etmek de mümkündür.

Anahtarlar

Verilen bu sayıların onluk tabanda gerçek değerlerle ifade edilmesi, bu sayıların büyüklüğü hakkında bize fikir verecektir.

Evrenin yaşının 10^{10} yıl olduğu, dünyadaki atomların sayısının yaklaşık 2^{170} veya 10^{51} tane olduğu, genetik olarak bir kişinin var olma ihtimalinin 300 milyarda 1 veya 2^{40} olduğu, bir gün içinde yıldırım sonucu ölme ihtimalinin 9 milyarda 1 veya 2^{33} olduğu düşünülürse, anahtarların boyutları hakkında daha anlaşılabilir bir değerlendirme yapmak mümkün olabilecektir.

Anahtarlar

Anahtarları temel alarak, algoritmaları değerlendirdiğimizde, **simetrik** yaklaşımlarda **tek bir anahtar üretimi** yapılırken, asimetrik algoritmalarda, anahtarlar bir çift olarak üretilirler.

Anahtarlar

Simetrik bir algoritma için, **anahtarın alıcıya iletilmesi, mutlaka gizli bir yoldan yapılması gerekmektedir**. Burada iki kişi arasında yapılacak olan haberleşmelerde pek sıkıntı yoktur, fakat ikiden fazla kişi ile güvenli haberleşileceği zaman sıkıntılar oluşmaktadır. Bunun aşılması için bu yaklaşımda anahtar yönetimi gereklidir ve bu konu dikkat edilmesi gereken önemli bir hususdur. Bu yaklaşımda, her bir bilgisayar bir başka bilgisayarla, diğer bilgisayarlardan bağımsız bir iletim hattı oluşturmaktadır. N elemanlı bir ağda N'in 2'li kombinasyonu kadar iletim hattı oluşacağı dikkate alınırsa bu işin zorluğu da ortaya çıkar. Küçük bir ağ üzerinde bunun bir problem teşkil etmeyeceği düşünülebilir, fakat büyük veya dünya çapında bir ağ üzerinde düşünüldüğünde fiziksel olarak bu sayıda bir iletim hattı oluşturmak imkansızdır. Ayrıca, her bir eleman diğer bütün elemanların anahtarlarını depolamak zorundadır.

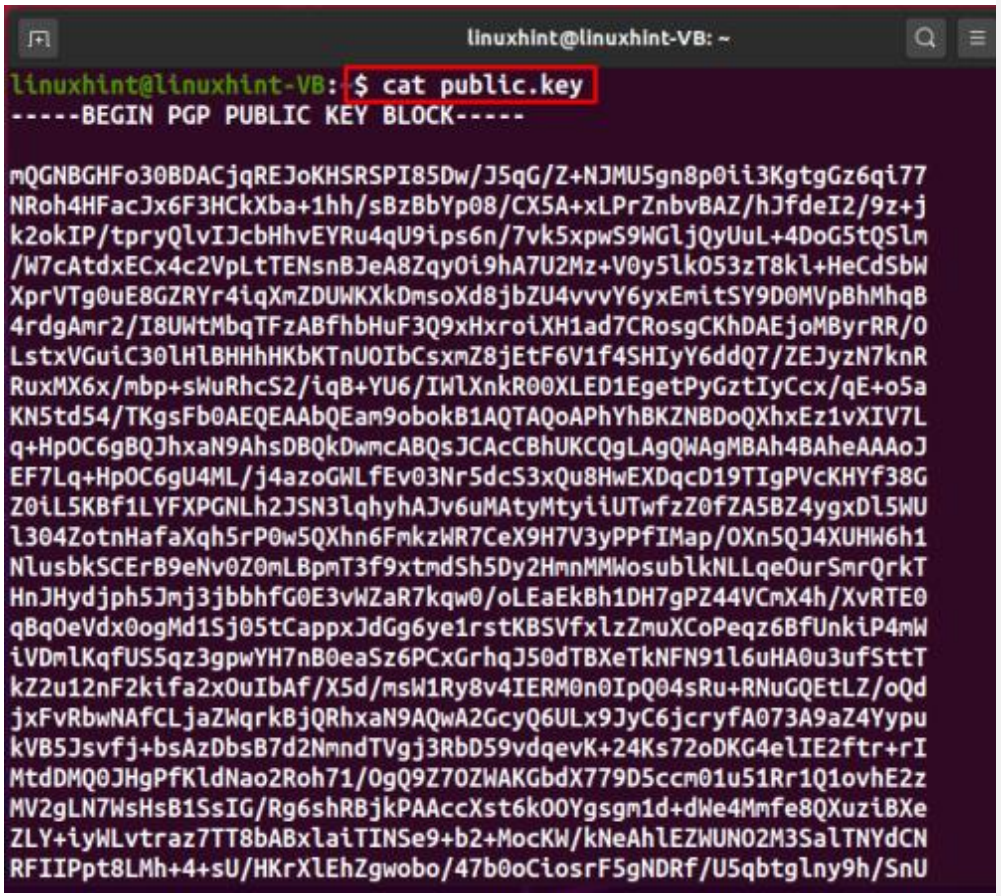
Anahtarlar

Simetrik algoritma anahtarlarının iletiminde, **TTP** (*trusted third party*), kullanılan yöntemlerden birisidir. Bu yöntemde, bütün kişi ve kurumlarca doğruluğu ve güvenirliği kabul edilen üçüncü bir ara yapı kullanılmaktadır. Gönderici herhangi bir alıcıya bilgi göndermek istediği zaman, bu ara yapıdan anahtar talebinde bulunur. TTP adı verilen bu yapı ise, göndericiye anahtar temin ederken, göndericinin bildirdiği alıcıya da aynı anahtarı ulaştırır. Ağa bağlı kullanıcılar anahtar teminini TTP yapısından elde ederler. Ancak bu yapının üstünlükleri olduğu kadar, dezavantajları da bulunmaktadır. Herhangi bir eleman ağdan atıldığında veya ağa eleman eklendiğinde bu yapının bundan etkilenmemesi, her bir elemanın sadece TTP'nin verdiği bir anahtarı depolamak zorunda olması, bilinen üstünlükleri iken, her bir bilgi iletiminde öncelikle, TTP ile iletişim kurulmak zorunda olması, TTP'de n adet anahtar depolanma zorunluluğu, TTP'nin tüm mesajları okuması ve TTP'nin anahtar iletiminde güvenliği sağlayamaması bilinen sakıncalarıdır.

Anahtarlar

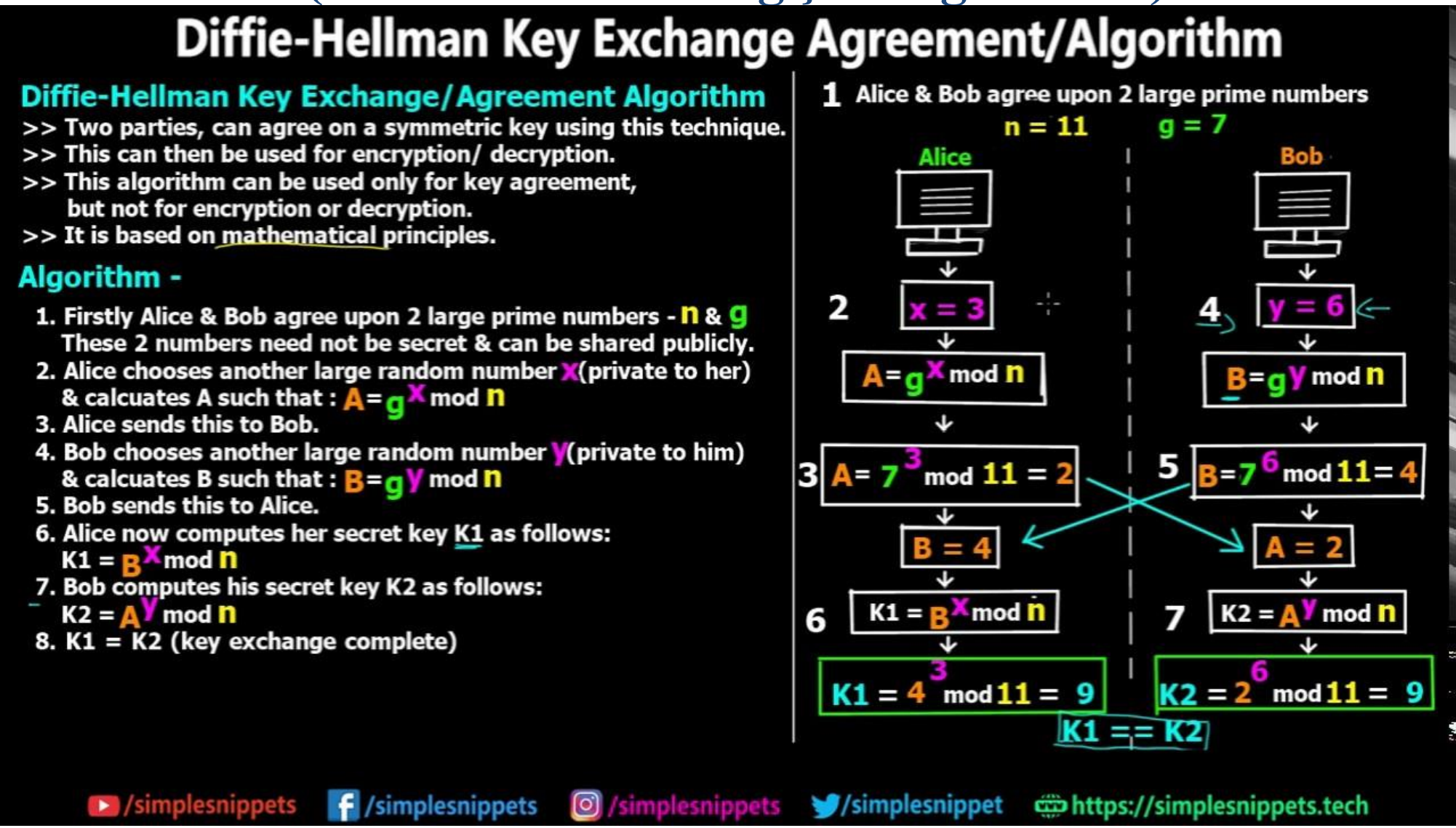
Asimetrik algoritma anahtarlarının iletiminde kullanılan diğer yöntemlerden biri **Genel Anahtar Tekniği**'dir. Bu yapıda mevcut iki anahtar bulunduğu için, genel anahtarlar her kullanıcının erişebileceği bir ortamda tutulurlar. Kişi_A kullanıcısı Kişi_B kullanıcısına bilgi göndereceği zaman, önce merkezden veya bilinen bir yerden Kişi_B kullanıcısının genel anahtarını temin eder. Daha sonra göndermek istediği bilgiyi bu anahtarla şifreleyip, Kişi_B'ye gönderir. Bu yapıda üçüncü bir ara yapıya gerek olmaması önemli bir üstünlüktür. Bu sayede, iletilecek bilginin üçüncü bir kişi tarafından okunma riski ortadan kaldırılmış ve çok sayıda anahtar depolama sıkıntısı giderilmiştir.

Anahtarlar (Örnek: Public and Private Keys)




```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAqwitjHs18lz19cGdvgne1ck8IYQUPyKAPtkPU3HZ+FwY3aTw
1IizXTH1QHXAMrpYF8MACk/lzC4aVlaUW6DxcXWyQnDkddJ8DKYgKxqE0m3Adtyy
XknNH1xWG7EDWXL5aysJ+kubtDqqhOHuMCPNbCNJ+zcnPsetccdNwL2prISFLUO5
LrLZ/NqHxXKPep5F6GrxRZj1DTMeQ7TUG+MawJG0vxN2GHdyU+CBx7nvQ2xI0nCL
mkVSFBsW1vrPlLPEVi7Dwh8oD5nNqslxitDBI+nTZbmx9iCFFjxfeGh6VryVRaGK
/31FH21rNMVh6Kk2HfK3j5MJZ5dft3gbPznZiQIDAQABAoIBABtnn49D6sfz10FS
jbj2kesFfIoORMQ8/fmUBB2lv3xJHX7eP+x+HudO6vIyK+K08wqTpzz/wl1uAbBV
3R21cxpv9mko96JdYJ0SPVNKw3+IMG+bO0VaY/CjdfSn71Z00rw2QDoHxWIiiFIU
dXrnMbIjEWacVsB7dDIn8jBw82/95N4n+9rhloNccH9jeCoRIgsLVbpu8tcHsSFN
Uk5SwNRfPYUoq7Q6jD6HNbeEtabyvJfumDbdiB8DusUW83RohKpNaP8+z1ZAMbUp
IySayM4ZNn79ZwGBFZXpe2Ib4MII8IYtxH0vd3zzMRfXf8nsWjuXCFueOVY93Xgn
+ejgYhUCgYEA0n0GvU7LxgIdlc6zi5BULV0ryBsWrQ2NRC+1HG4MlwoJpZs/VFTY
3XQN8qNaz9VvLdo6GVP0hIfFUvs6JA+MdqLMC6+i0cOfdMNs1APOCtQHXrSI0s+h
XrNFXHd0OyqG373Q9JNfcWDLHkaSGWpaQqX3AgJTNy7Dr8VJ8OlymlMCgYEA0APD
VZEf3uJP1HIN16FqGjKGDzVdcviW52OViKMPp39vH1eOMWSu1J9g8uG1wqDn+vGy
8cm/PQrv1+CvFGmhdooP34Z1pKXyTagUIVlTqeG90xsLnwlvZi9//PGEG7pxLejJ
L0DH+L3DoAMUECsgBLSt942gC3OfjGbFwAYBGTMCgYEAxnhTOX8pzwvBn7bmPuuZ
I6kdljJMoGIN2MRvLl5qCqTRUdDf1wG19rHuUOJMx3mFuqNxct5hyfFHUyZFvSjY
FikM4tv6V3XwTaXTYNoxlq40QM1T0gsrKmM5PKX596vyvtd5RpQLQ5m0DFkYe1R3
xS4+iStuEbNLmtoZDUrh37cCgYBiyna5q6vcOdU6C1ThpOp0OKyMioawNLnOePAq
rW6g2RfYZcfFU5DosCzmDSY6ohqqhqG6zVsCza/s8euUoToqxxUUzpIOuTVjhkDR
OdBPLUPu/7g8NsnuWP7LDZT1ak2YRSdPRs/yJYXD99JOf3y8X2cD3AI3jhknICQo
t3FMGwKBgDR7+ya7Tn8KZd19oANZjuqIuD9DFliTeIQc7fRcV1UDJxQaT7joWvSM
EexltK3KQc27rK1j77ED3maG9L19RP5SuFQVsK78pBosMNZxNfDp4wCtsjWicYcG
OG1Zr1QgVgoWerDjPYa9gLomCum+PNKNA7fTxqVqb8Z6957kTgFn
-----END RSA PRIVATE KEY-----
```

Anahtarlar (Örnek: Anahtar Değişim Algoritması)



Anahtarlar

Anahtar Uzunluğu (bit)	Sayı Değeri	10^6 şifre/s	10^9 şifre/s	10^{12} şifre/s
32	~4×10^9	36 dk	2.16 s	2.16 ms
40	~10^{12}	6 gün	9 dk	1 s
56	~7.2×10^{16}	1142 yıl	1 yıl 2 ay	10 saat
64	1.8×10^{19}	292 000 yıl	292 yıl	3.5 ay
128	1.7×10^{38}	5.4×10^{24} yıl	5.4×10^{21} yıl	5.4×10^{18} yıl

Farklı Anahtar Uzunluklarına Göre Şifre Kırma Zamanları

Anahtar uzunluğunun güvenliğe etkisini gösterme açısından literatürde verilen bir değerlendirme yaklaşımını yukardaki gibidir.

Anahtarlar

(a) akıllı çubuk

(b) akıllı kart

E-imza Taşıma Ortamları

Sorular

Bir sonraki ders Siber Güvenliğin Temelleri – II (Şifre Bilim (Kriptografi), Şifreleme Algoritmaları, Anahtarlar, Ciphers) konusuna giriş yapılacak.