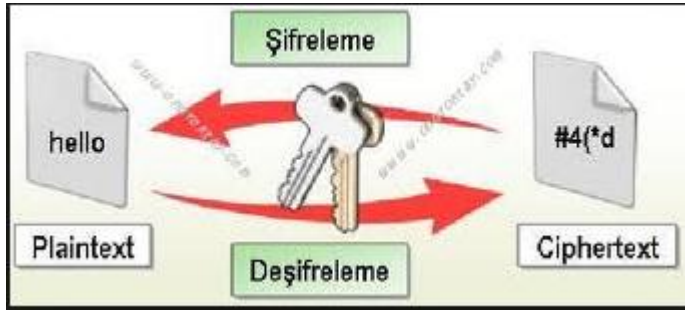
Kriptografi

Ayrık İşlemsel yapılar 14. hafta ders notu

Kriptografi Nedir?

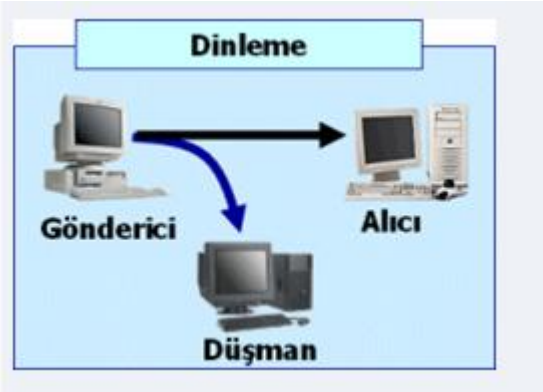
- Kriptografi şifreleme bilimi demektir.
- Teknolojinin hızlı bir şekilde gelişmesiyle askeri, elektronik, banka sistemleri ve daha bir çok yer kriptografi biliminin kullanım alanları haline gelmiştir.
- Günümüz sistemlerinde en önemli gereksinimlerden birisi bilgilerin sorunsuz bir şekilde taşınması ve gizliliktir.
- Verilerin güvenli bir şekilde yollanması ve karşı taraftan alınabilmesi için kriptografi bilimi aracılığıyla geliştirilen çeşitli şifreleme, anahtarlama ve çözümleme algoritmaları kullanılmaktadır.
- Şifreleme algoritması şifrelenecek metni ve şifreleme anahtarını girdi olarak alır. Çözümleme algoritması ise şifreleme algoritmasının ters yönünde çalışır.

Kriptografinin türkçe adı şifre yazımıdır. Kriptografi yunanca gizli anlamına gelen “kript” ve yazı anlamına gelen “graf” dan türetilmiştir. Kriptoloji ise şifre bilimidir. Kriptografi bilgi güvenliği ile uğraşır, Kriptoanaliz güvenli bilginin kırılması başka bir deyişle kriptografinin tam karşıtıdır. Kriptoanalistler genelde şifre çözmeye dayalı çalışırlar. Kriptoloji bir matematik bilimidir ve genelde sayılar teorisi üstüne kuruludur.

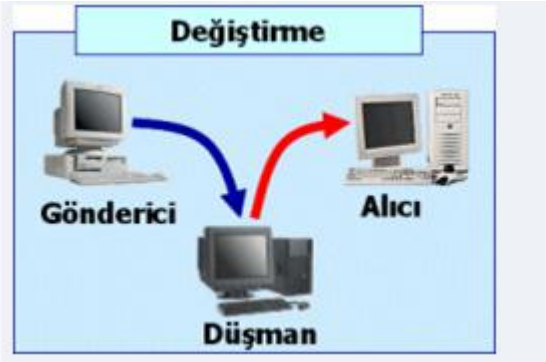


Amaçları

- Gizlilik ihlalini önlemek

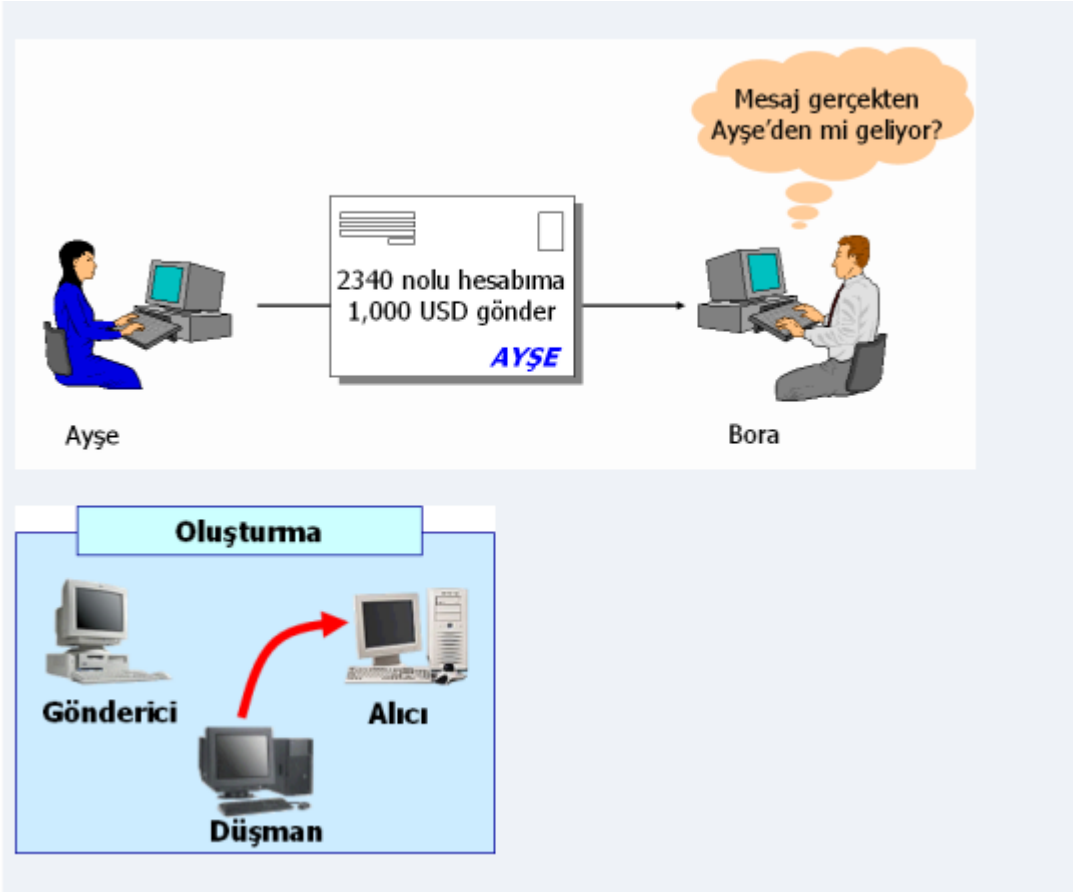


- Veri bütünlüğünü sağlamak



Haberleşmeye müdahale edip göndericinin mesajlarını değiştiren saldırgan, alıcıya giden mesajı istediği şekle sokabilir. Bu tehdit mesajın bütünlüğünü bozan değiştirme tehdidir.

- Kimlik Doğrulama İhlalini önlemek (Dijital imza kullanılır)



Kullanım Alanları

ATMlerde şifremizi girdikten sonra, şifre doğruluk kontrolü için telefon hatları üzerinden bankanın bilgisayarına yollanır. Bu yolculuk süresince şifrenin güvenliği sağlanmak zorundadır. Bu nedenle şifre şifrelenerek yollanır.

Televizyonda izlediğimiz şifreli tv kanallaındada kriptografi bilimi kullanılır. Uydu üzerinden yayın yapan bu tip kanallar gönderdikleri sinyalleri şifreler. Bu şifreyi çözmek için alıcıya(receiver) akıllı(smart) kart takılır. Kartın içindeki anahtar vasıtası ile şifre çözülür ve yayın normal olarak izlenir.

Bir başka iletişim tekniğini göz önüne alırsak, örneğin telsiz haberleşmelerinde de buna benzer sistemler kullanılmaktadır. Ses önce şifrelenir karşıya gönderilir orda şifre açılır ve ses araya başka bir kullanıcı girmeden güvenli bir şekilde teslim edilmiş olur.
E-imza
Dikkat edeceğimiz gibi kriptoloji iletişim materyallerinin kullanıldığı her alanda gizliliği sağlamak için kullanılmaktadır (ses, görüntü, metin v.s v.s).

Simetrik Şifreleme Algoritmaları

- Bu algoritmada şifreleme ve şifre çözmek için bir tane gizli anahtar kullanılmaktadır. 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. Asimetrik şifrelemeyle karşılaştırıldığında hız konusunda simetrik algoritmalar çok daha başarılıdır. 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.
- Örnek:DES, AES, Blowfish

Asimetrik Şifreleme Algoritmaları

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

Özel Anahtar kullanımı örnek

Durum: Barış elindeki çantanın Ayşe'ye güvenli bir biçimde iletilmesini ve çantanın yalnızca Ayşe tarafından açılmasını istiyor.Nasıl bir algoritma kullanılmalı?

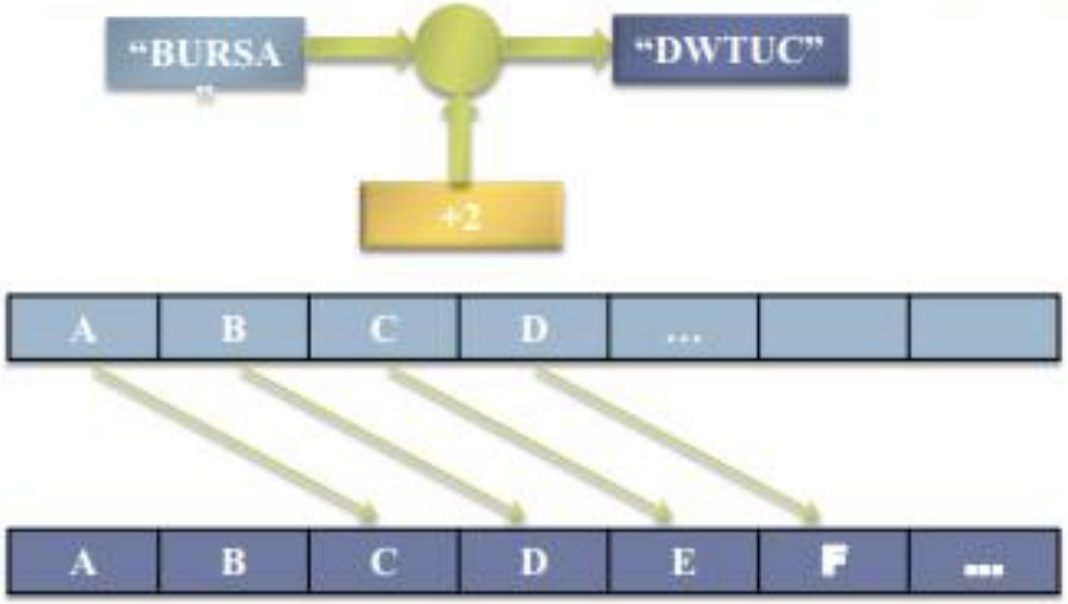
- Adım1 Barış elindeki çantaya sadece bir tane anahtarı olan bir kilit takar ve Ayşe'ye yollar. Buradaki anahtar Barış'ın özel anahtarıdır.
- Adım2: Ayşe de çantayı aldığı zaman kilidi açan anahtarı olmadığı için, anahtarı sadece kendinde olan başka bir kilit takar ve çantayı Barış'a geri yollar.
- Adım3: Barış çantayı aldığı zaman kendi takmış olduğu kilidi açar ve tekrar Ayşe'ye yollar.
- Adım4: Ayşe çantayı aldığında çantanın üzerinde sadece kendi takmış olduğu kilit vardır. Elindeki anahtarı kullanan Ayşe, çantayı açar ve Barış'ın göndermiş olduğu belgeleri sadece kendisinin almış olduğundan emin olur.

Sezar Şifreleme Algoritması

- İlk şifreleme algoritmalarından kabul edilen Sezar şifreleme algoritması (Caesar chiper), eski Roma İmparatoru Julius Caesar tarafından savaş zamanlarındaki bilgi gönderiminde kullanılmıştır.

Bu algoritmada; mesajdaki her karakter, başka (‘anahtar’ değeri kadar ötelenmiş) karakterle yer değiştirerek şifreli mesaj elde edilmektedir. Örneğin ROT13 olarak adlandırılan şifreleme yönteminde öteleme miktarı 13’tür

Sezar Şifreleme Algoritması



Eğer anahtar değeri 2 ise orijinal mesajdaki her harf, kendisinden iki sonraki harfle yer değiştirir. Yani orijinal mesajdaki "A"→"C", "B"→"D" olur.

RSA Algoritması

İlk defa 1977 yılında Ron Rivest, Adi Shamir ve Leonard Adleman tarafından oluşturulan RSA algoritması geliştiricilerinin soy isimlerinin ilk harfleriyle anılmaktadır.

Bir genel anahtarlı şifreleme tekniği olan RSA, çok büyük tamsayıları oluşturma ve bu sayıları işlemenin zorluğu üzerine düşünülmüştür. Anahtar oluşturma işlemi için asal sayılar kullanılarak daha güvenli bir yapı oluşturulmuştur. Anahtar oluşturma algoritması şu şekildedir:

- Alıcı P ve Q gibi çok büyük iki asal sayı seçer.
- Bu iki asal sayının çarpımı N = P.Q ve bu bir eksiklerinin φ(N)=(P-1)(Q-1) hesaplanır. (alıcı)
- 1'den büyük φ(N)'den küçük φ(N) ile aralarında asal bir E tamsayısı seçilir.(alıcı)
- Seçilen E tamsayısının mod φ(N)'de tersi alınır, sonuç D gibi bir tamsayıdır.(alıcı)
- E ve N tamsayıları genel anahtarı, D ve N tamsayıları ise özel anahtarı oluşturur.(alıcı)

Genel ve özel anahtarları oluşturduktan sonra; alıcı genel anahtarı halka açar. Yani bu sayıları herkes görebilir. Ancak özel anahtarı sadece alıcı bilir.

Şimdi bu alıcıya mesaj gönderelim.

Gönderen kişi halka açık olduğu için (N,e)'ye ulaşabilir.Ve bu genel anahtar ile göndereceği mesajı şifreler. Şifreleme işlemi şu şekilde yapılmaktadır:

Şifrelenecek bilginin sayısal karşılığının E'ninci kuvveti alınır ve bunun

mod N deki karşılığı şifrelenmiş metni oluşturmaktadır.

Genel anahtar ile şifrelenmiş bir metin ancak özel anahtar ile açılabilir. Bu yüzden şifrelenmiş metin, yine aynı yolla, şifrelenmiş metnin sayısal karşılığının D'ninci kuvveti alınır ve bunun mod N deki karşılığı orijinal metni oluşturur

Bu algoritmada iki asal sayının çarpımını kullanarak anahtar

oluşturulmasının sebebi, iki asal sayının çarpımını asal çarpanlarına ayırmak asal olmayan sayıları ayırmaktan daha zorlu olmasıdır.

Formül işleme koyulduğunda en çok zaman alan süreç, üst alma ve mod

bulma işlemleridir. Süreci hızlandırmak için E değerinin küçük ya da

hesaplanması kolay bir değer seçilebilir. Bu da yukarıda bahsettiğimiz gibi değerin küçüklüğü ve tekrarlı kullanılması güvenliği azaltmaktadır

RSA örnek:

1. İki farklı asal sayı seçelim. $p = 61$ ve $q = 53$ olsun.
2. $n = pq$ değerini hesaplayalım. 61 × 53 = 3233.
3. Totient değerini hesaplayalım. $\varphi(3233) = (61 - 1)(53 - 1) = 3120$.
4. 1 ile 3120 arasında 3120 ile aralarında asal olan bir e değeri seçelim. e değerini asal seçersek sadece 3120'nin böleni olup olmadığını kontrol etmemiz gerekir. $e = 17$ olsun.
5. d'yi e'nin mod $\varphi(n)$'deki çarpmaya gore tersi olarak hesaplayalım. $d = 2753$.

Ortak Anahtar: $(n = 3233, e = 17)$. Herhangi bir m mesajı için şifreleme fonksiyonu m^{17} (mod 3233).

Özel Anahtar: $(n = 3233, d = 2753)$. Herhangi bir c şifreli mesajı için şifre çözme fonksiyonu c^{2753} (mod 3233).

Örneğin $m = 65$'i şu şekilde şifreleriz: $c = 65^{17} \pmod{3233} = 2790$

$c = 2790$'ın şu şekilde şifresini çözebiliriz: $m = 2790^{2753} \pmod{3233} = 65$

RSA Örnek:

- Ayşe Barış'a FEDA sözcüğünü şifreli olarak göndermek istiyor.
- Barış gizli anahtarlar olan p ve q asalaarını 2 ve 11 seçsin.
- Buradaki N sayısı p.q=2.11=22 ve φ(N) sayısı ise (p-1).(q-1)=1.10 olacaktır.
- Sırada bir e sayısı belirlemek var. e=7 seçilsin. (N, e) ikilisini (22, 7) olarak duyurur.
- Ayşe bu ikiliye ulaşır ve göndereceği mesajı bu ikiliyi kullanarak şifreler. Aralarında aşağıdaki haerfleri aşağıdaki gibi kodlama konusunda anlaştıklarını varsayalım.

A	B	C	D	E	F	G	H	I	j	K	L	M	N	O	P	R	R	S	T	U	V	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

- Şimdi Ayşe bu sayıların 7. dereceden kuvvetlerini alarak mod 22'de hesaplasın.
- 6^7=8 mod22
- 5^7=3 mod22
- 4^7=16 mod22
- 1^7=1 mod 22

- Ayşe çıkan sonuçları (8-3-16-1) harflere çevirir ve HCPA şifremetnini Barış'a gönderir.
- Şifremetni alan Barış şifre çözme algoritmasını uygulamak için d sayısını hesaplamak zorundadır.
- e.d=1. mod φ(N) ➔ 7.d=1 mod(10)➔ d=3
- D=3 sayısını bulduktan sonra artık deşifre işlemini gerçekleştirebilir. Yapacağı şey şifremetni sayılara dönüştürüp her sayının 3. kuvvetini alarak mod 22'de hesaplamaktır.

- 8^3=6 mod 22
- 3^3=5 mod 22
- 16^3=4 mod22
- 1^3=1 mod 22

- Görüldüğü gibi Barış 6-5-4-1 sayılarını bularak FEDA sözcüğünü elde etmiş oldu.

- RSA algoritmasının en büyük dezavantajı; asimetrik bir şifreleme algoritması olması ve büyük sayılarla işlem yapması nedeniyle yavaş olmasıdır.

  Özellikle kablosuz ağ sistemlerinde bu algoritmanın kullanılması bazı sorunlara yol açabilir. Çünkü band genişliğini fazlaca tüketir ve sistemi yavaşlatarak performans düşüşüne neden olur.

- Büyük sayılarla işlem yapmak zor olduğu için güvenilirliği son derece yüksek olan bir şifreleme tekniğidir