

Ayrık İşlemsel Yapılar

HAFTA 14

Kriptoloji

Doç. Dr. Nilüfer YURTAY
Dr. Öğretim Üyesi Gülüzar ÇİT

İçerik

- ❑ Kriptoloji
- ❑ Kriptoanaliz
- ❑ Kriptografi
- ❑ Şifreleme Algoritmaları
 - ❑ Simetrik Şifreleme Algoritmaları
 - ❑ Asimetrik Şifreleme Algoritmaları

Kriptoloji

- ❑ Şifre bilimi
- ❑ Bilginin gizlenmesi veya ortaya çıkarılması ile ilgilenen matematik temelli bir bilim dalıdır.

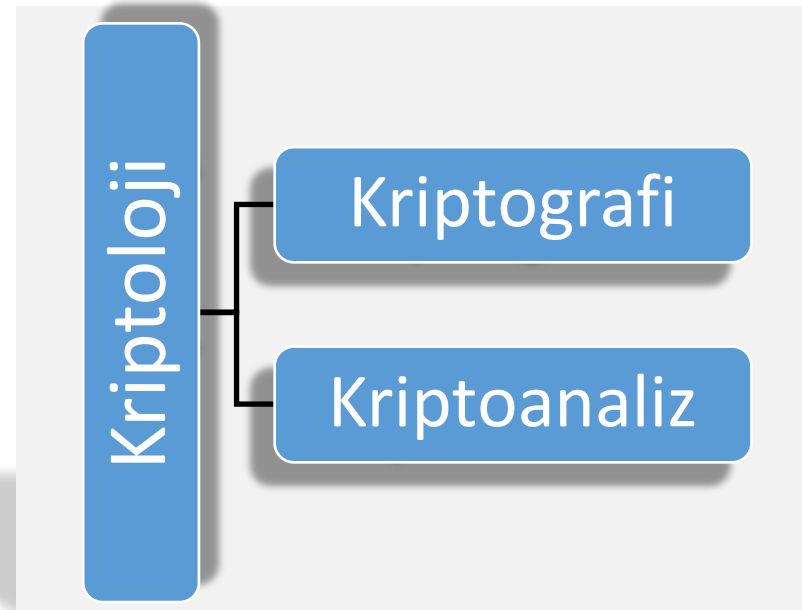


Kriptoloji

- ❑ Teknolojinin hızlı bir şekilde gelişmesiyle askeri, devlet, elektronik, banka sistemleri ve daha bir çok yer kriptoloji biliminin kullanım alanları haline gelmiştir.
- ❑ Günümüz elektronik sistemlerinin en önemli gereksinimlerinden birisi bilgilerin sorunsuz ve gizli bir şekilde taşınmasıdır.
- ❑ Verilerin güvenli bir şekilde gönderilmesi ve karşı taraftan alınabilmesi için geliştirilen çeşitli şifreleme, anahtarlama ve çözümleme algoritmaları kullanılmaktadır.

Kriptoloji

- ❑ Şifreleme algoritması şifrelenecek metni ve şifreleme anahtarını girdi olarak alır.
- ❑ Çözümleme algoritması ise şifreleme algoritmasının ters yönünde çalışır.



Kriptoloji



Kriptoanaliz

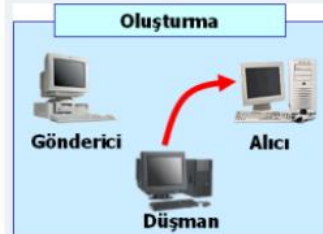
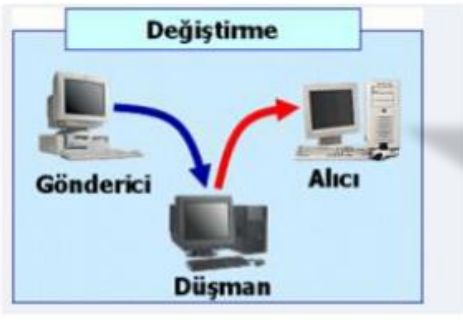
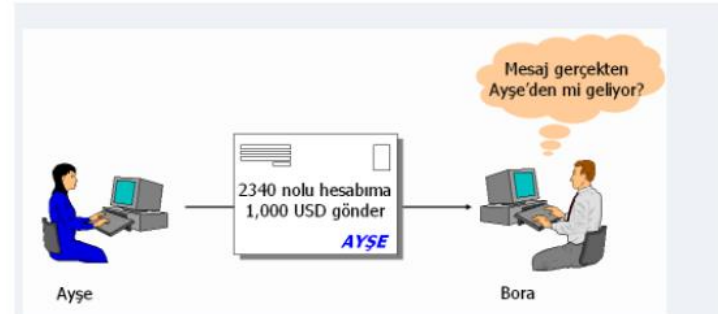
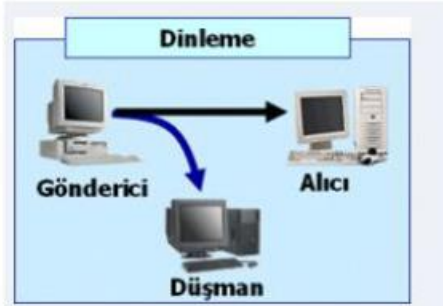
- ❑ Güvenli bilginin kırılması
- ❑ Kriptografinin tam tersi
- ❑ Kriptoanalistler genelde şifre çözmeye dayalı çalışırlar

Kriptografi

- ❑ Şifreleme bilimi
- ❑ Yunanca gizli anlamına gelen «**kript**» ve yazı anlamına gelen «**graf**» kelimelerinden türetilmiştir.
- ❑ Türkçe adı: «**şifre yazımı**»

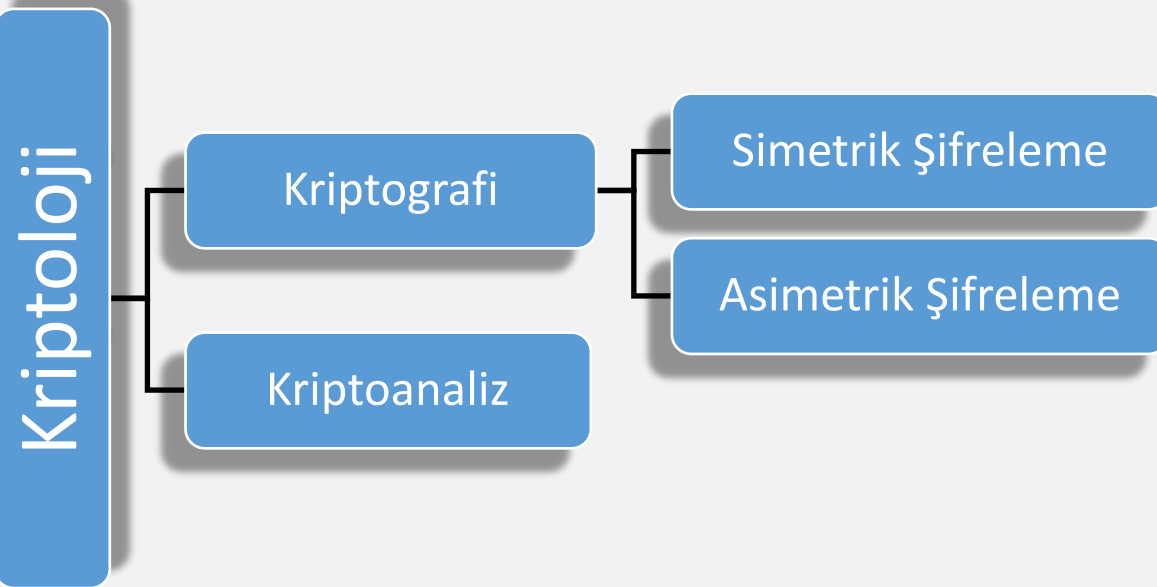
Amaçları

- ❑ Gizlilik ihlali önlemek
- ❑ Veri bütünlüğünü sağlamak
- ❑ Kimlik doğrulama ihlali önlemek (Dijital İmza)



Kullanım Alanları

- ☐ ATM
- ☐ Televizyon
- ☐ Telsiz haberleşme
- ☐ E-imza
- ☐ ...



Simetrik Şifreleme Algoritmaları

- ❑ Bu algoritmada şifreleme ve şifre çözmek için **gizli anahtar** kullanılmaktadır.
- ❑ Kullanılan anahtar başkalarından gizlidir ve şifreleme yapan ile şifrelemeyi çözecek kişiler arasında anlaşılmiş ortak bir anahtardır.
- ❑ Gönderilecek gizli metinle beraber üstünde anlaşılmiş olan gizli anahtar da alıcıya gönderilir ve şifre çözme işlemi gerçekleştirilir.

Simetrik Şifreleme Algoritmaları

- ❑ Simetrik şifrelemenin asimetrik şifrelemeye göre avantajları
 - ❑ Hızlı
 - ❑ İçerdiği basit işlemlerden dolayı elektronik cihazlarda uygulamak çok daha kolaydır.
 - ❑ Kullanılan anahtarın boyu ve dolayısıyla bit sayısı çok daha küçüktür.
- ❑ Örnek Simetrik Algoritmalar
 - ❑ DES, AES, Blowfish

Asimetrik Şifreleme Algoritmaları

- ❑ Simetrik şifreleme algoritmalarında bulunan en büyük problem anahtar dağıtımıdır.
 - ❑ Simetrik algoritma kullanan çok kullanıcıli 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 anahtar açık anahtar, şifreyi çözen anahtar ise özel anahtardır.
- ❑ Açık anahtarlar herkese dağıtılabılır, 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.

Asimetrik Şifreleme Algoritmaları

- ❑ Bu yüzden asimetrik şifreleme güvenlik açısından simetriğe göre çok daha başarılıdır. Az sayıda anahtar kullanarak simetrik şifreleme yapan çok kullanıcıli 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 Asimetrik Algoritma
 - ❑ RSA

Asimetrik Şifreleme Algoritmaları

❑ ÖRNEK:

❑ Özel Anahtar Kullanımı

❑ **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.

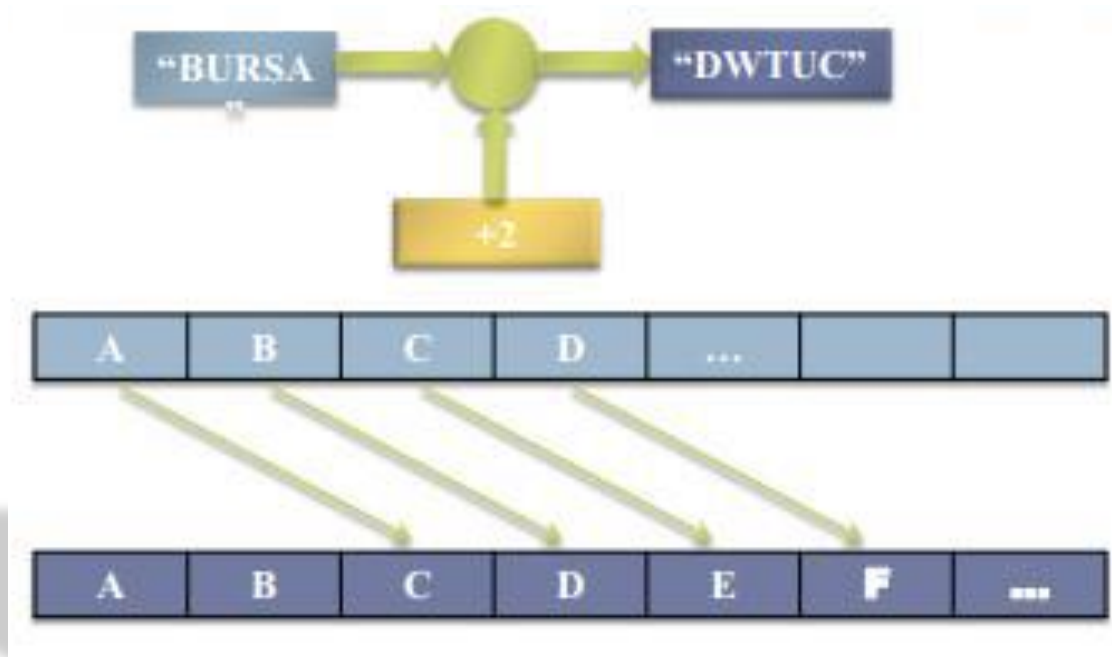
❑ **Adım4:** Ayşe çantayı aldığı anda çantanın üzerinde sadece kendi takmış olduğu kilit vardır. Elindeki anahtarı kullanan Ayşe, çantayı açar ve Barış'ın göndermiş olduğu belgeleri sadece kendisinin almış olduğundan emin olur.

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.
- ❑ Genel anahtarlı bir şifreleme tekniği
- ❑ Çok büyük tamsayıları oluşturma ve bu sayıları işlemenin zorluğu üzerine düşünülmüştür.
- ❑ Anahtar oluşturma işlemi için asal sayılar kullanılarak daha güvenli bir yapı oluşturulmuştur.

RSA Algoritması

❑ Anahtar oluşturma algoritması:

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

RSA Algoritması

- ❑ 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

RSA Algoritması

- ❑ 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 değeri küçük ya da hesaplanması kolay bir değer seçilebilir. Bu durumda da yukarıda bahsettiğimiz gibi değerlerin küçüklüğü ve tekrarlı kullanılması sonucu güvenliği azaltmaktadır.

RSA Algoritması

❑ Örnek:

❑ İki farklı asal sayı seçelim

❑ $p = 61$ ve $q = 53$

❑ İki asal sayının çarpımını hesapla

❑ $n = p \times q = 61 \times 53 = 3233$

❑ Totient değerini hesapla

❑ $\varphi(3233) = (61 - 1) \cdot (53 - 1) = 3120$

❑ 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.

❑ d 'yi e 'nin $\varphi(n)$ 'deki çarpmaya göre tersi olarak hesaplayalım.


❑ $d=2753$

❑ $(e \cdot d) \bmod \varphi(n) = 1$ yani $e \cdot d = 1 + X \cdot \varphi(n)$

❑ $17 \cdot d = 46801 = 1 + X \cdot 3120$

RSA Algoritması

Örnek...:

 $17 * d = 46801 = 1 + X * 3120$

X	(X * 3120) Mod 17
1	9
2	1
3	10
4	2
5	11
6	3
7	12
8	4

X	(X * 3120) Mod 17
9	13
10	5
11	14
12	6
13	15
14	7
15	16
D=2753	

RSA Algoritması

❑ Örnek...:

❑ Ortak Anahtar:

❑ $n = 3233, e = 17$

❑ Herhangi bir m mesajı için şifreleme fonksiyonu:
 $m^{17} \pmod{3233}$

❑ Özel Anahtar:

❑ $n = 3233, d = 2753$

❑ Herhangi bir c şifreli mesajı için şifre çözme fonksiyonu:
 $c^{2753} \pmod{3233}$

❑ $m = 65$ için şifre

❑ $c = 65^{17} \pmod{3233} = 2790$

❑ $c = 2790$ için şifre çözme

❑ $m = 2790^{2753} \pmod{3233} = 65$

RSA Algoritması

❑ Örnek:

- ❑ Ayşe Barış'a FEDA sözcüğünü şifreli olarak göndermek istiyor.
- ❑ Barış gizli anahtarlar olan p ve q asallarını 2 ve 11 seçsin.
- ❑ Burada N sayısı $p \cdot q = 2 \cdot 11 = 22$ ve $\phi(N)$ sayısı ise $(p-1) \cdot (q-1) = 1 \cdot 10 = 10$ 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 harfleri 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

RSA Algoritması

Örnek...:

- Ayşe bu sayıların 7. dereceden kuvvetlerini alarak mod22'de hesaplasın.
 - $6^7 = 8 \pmod{22}$
 - $5^7 = 3 \pmod{22}$
 - $4^7 = 16 \pmod{22}$
 - $1^7 = 1 \pmod{22}$
- Ayşe çıkan sonuçları (8-3-16-1) harflere çevirir ve 'HCPA' şifre metnini Barış'a gönderir.
- Şifre metnini alan Barış, şifre çözme algoritmasını uygulamak için d sayısını hesaplar.
 - $e.d = 1 \pmod{\varphi(N)} \Rightarrow 7.d = 1 \pmod{10} \Rightarrow d = 3$

RSA Algoritması

❑ Örnek...:

❑ $d = 3$ sayısı bulunduktan sonra artık deşifre işlemi, şifreli metni sayılara dönüştürüp her sayının 3. kuvvetini alarak $\text{mod } 22$ 'de hesaplamaktır.

❑ $8^3 = 6 \pmod{22}$

❑ $3^3 = 5 \pmod{22}$

❑ $16^3 = 4 \pmod{22}$

❑ $1^3 = 1 \pmod{22}$

❑ Barış 6-5-4-1 sayılarını bularak 'FEDA' sözcüğünü elde etmiş oldu.

RSA Algoritması

- ❑ RSA algoritmasının en büyük dezavantajı;
 - ❑ Asimetrik bir şifreleme algoritması olması
 - ❑ büyük sayılarla işlem yapması nedeniyle yavaş olmasıdır.
- ❑ Özellikle kablosuz ağ sistemlerinde bu algoritmanın kullanılması bazı sorunlara yol açabilir. Çünkü bant 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 .