Ayrık Matematik
(Ayrık İşlemsel Yapılar)

Fırat İsmailoğlu, PhD

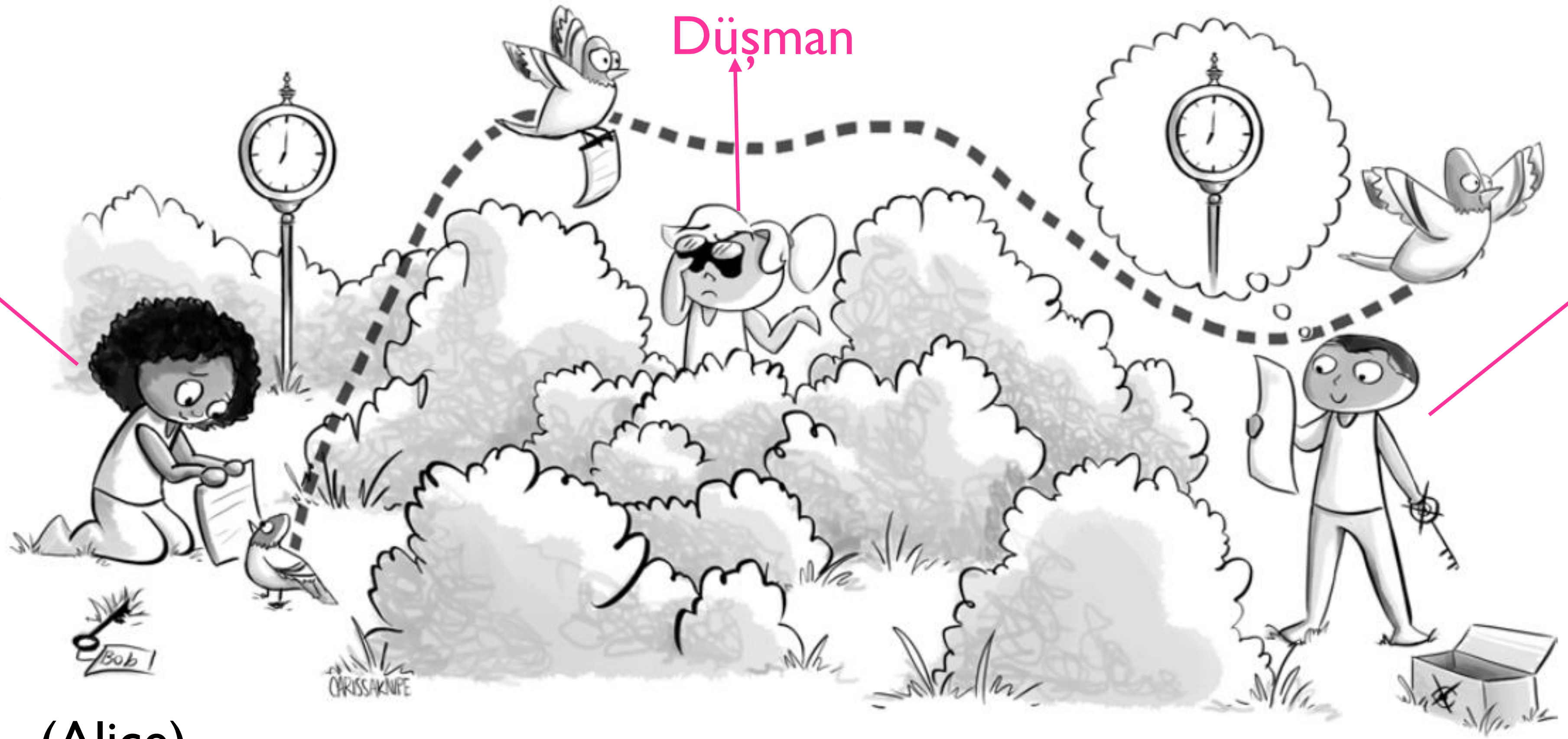
Hafta 7:
Şifreleme
(Kriptoloji)

Hafta 7
Plan

1. Şifreleme Nedir
2. Şifreleme Türleri
3. Gizli Şifreleme
4. Açık Şifreleme
5. Moduler Aritmetiğin Bazı Özellikleri
6. RSA Şifreleme Sistemi

Şifreleme Nedir?

Sifereleme gizli mesajlar gönderme ve alma metodlarının bir calismasidir. Sifrelemede amac hassas bilgiyi yalnizca bilmesi gereken insalarin bilmesidir.



Gecmiste şifreleme daha cok askeri ve diplomatik amaclarla kullaniliyordu. Bugun ise internet ve elektronik ticaret sayesinde herkes icin gunluk hayatin bir parcasi oldu.

Whatsapp mesajlari, kredi karti islemleri, VPN, email gonderimi..

Bir sifre, bu sifreyi kirmak icin gereken hesaplama gucu kadar guvenlidir.

Genel olarak sifreleme metodlarini ikiye ayırabiliriz: Gizli Şifreleme – Açık Şifreleme

Şifreleme

Gizli şifreleme
(Private-Key Cryptography)

Açık şifreleme
(Public-Key Cryptography)

Gizli Şifreleme (Private Key Cryptogragy)

Gizli şifreleme geleneksel şifreleme yöntemidir.

Burada göndericinin ve alıcının daha önce üzerinde anlaştığı bir şifreleme yöntemi vardır (şifreyi her ikisi de bilir).

Gönderici bu yönteme göre mesajı şifreler; alıcı bu yönteme göre kendine gelen mesajı deşifre eder.

En önemli gizli şifreleme yöntemlerinden biri Sezar Şifresi'dir.

Sezar Şifresi (Caeser Cipher)

Sezar Şifresi'nde her bir harf, kendisinden belirli bir sayı sonra gelen harfle yer değistirir.

Her harfin kendinden kaç sonra gelen harfle yer değiştirecegi alıcının ve göndericinin daha önceden bildigi şifredir (anahtardır).

x yer değiştirme (atlama) miktarı olmak üzere

i. harf, $i + x \ (mod\ 29)$. harf ile yer değiştirir.

Sezar Şifresi (Caeser Cipher)

Örnek olarak x'i 3 alalım, böylece her bir harf kendinden sonra gelen 3. harfle yer değiştirir.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E

Bu şifreleme ile A, Ç olur; B, D olur; C, E olur....

Orjinal metin: SALDIRI SABAH SAAT BEŞTE

Şifrelenmiş metin: UÇOGKTK UÇDÇJ UÇÇV DĞÜVĞ

Sezar Şifresi (Caeser Cipher)

Burada x yer değiştirme miktarı için yalnızca 29 seçenek vardır. Bu 29 seçeneğin tamamını deneyebilir metni deşifre edebiliriz. Bu şifreyi kırmak için gereken hesaplama gücü azdır. Bu şifre kolay bir şifredir.

Alternatif olarak x her bir harf için farklı bir değer alabilir. Yani her bir harf farklı bir sayıda kaydırılabilir.

Örneğin A kendinden 2 harf sonra gelen B olur; B kendinden 5 harf sonra gelen F olur.

Bu şekilde alfabedeki 29 harfi 29! şekilde sıralayabiliriz (permütasyon); yani 29! tane farklı şifreleme elde edebiliriz. Fakat bu bile günümüz bilgisayarları ile kolayca kırılabilcek bir şifreleme olur.

Gizli Şifreleme 2. Örnek:

Diyelimki gönderici ve alıcı $k = 10111000$ şifresini biliyor olsun.

Gönderici $m = 01101110$ mesajını m ve k'nın XOR'u ile göndersin. Şu halde alıcaya gidecek şifreli mesaj:

m	0 1 1 0 1 1 1 0	$\longrightarrow$ mesaj
k	1 0 1 1 1 0 0 0	$\longrightarrow$ şifre
$c = m \oplus k$	1 1 0 1 0 1 1 0	$\longrightarrow$ şifreli mesaj

Alıcı yine k şifresini kullanarak şıfreli mesajı deşifre edebilir:

c	1 1 0 1 0 1 1 0	$\longrightarrow$ şifreli mesaj
k	1 0 1 1 1 0 0 0	$\longrightarrow$ şifre
$m = c \oplus k$	0 1 1 0 1 1 1 0	$\longrightarrow$ mesaj

Not: a ve b ayni uzunlukta herhangi iki bit olmak uzere: $(a \oplus b) \oplus b = a$

Gizli şifrelemedeki iki önemli sorun:

1. şifreyi bilen kişi kolayca mesajı deşifre edebilir,

2. şifreleme yöntemi çok kez tekrar ederse, şifreyi kırmak isteyen kişi yeterince zamanı parası ve hesaplama gücü varsa şifreyi kırar.

Örnek olarak ikinci dünya savaşında Almanlar tarafından kullanılan Enigma şifrelemesi verilebilir. Bu, gizli bir şifrelemeye örnektir, yani gönderici ve alıcının ikisinin de bildigi bir sifre vardır. Fakat şifreleme sistemi ne kadar karmaşık ve gelişmiş olmasına rağmen müttefikler tarafından kırılmıştır.

Açık Şifreleme (Public Key Cryptogragy)

Açık şifrelemede göndericinin ve alıcının (her kullanıcının) bir açık ve bir gizli anahtarı olur.

Açık anahtar (public key): mesajın şifrelenmesinde kullanılır.

Gizli anahtar (private key) mesajın deşifre edilmesinde kullanılır.

Açık anahtarlar herkes tarafından bilinir.

Gizli anahtar yalnızca sahibi tarafından bilinir.

Ana fikir: gönderici, alıcının açık anahtarını kullanarak mesajı şifreler. Alıcı kendi gizli anahtarını kullanarak gelen mesajı deşifre eder.

Açık şifrelemede düşman şifreli mesajı görse; hatta alıcının açık anahtarını bilse (yani mesajın şifreleme yöntemini bilse) dahi mesajı deşifre edemez!

Açık Şifreleme (Public Key Cryptogragy)

Alıcının açık anahtarı
(Alice)

Alıcının gizli anahtarı
(Bob)

Açık Şifreleme (Public Key Cryptogragy)

Açık şifrelemede için ihtiyacımız olan şey hesaplaması kolay fakat tersini almanın zor olduğu bir fonksiyon bulmaktir.

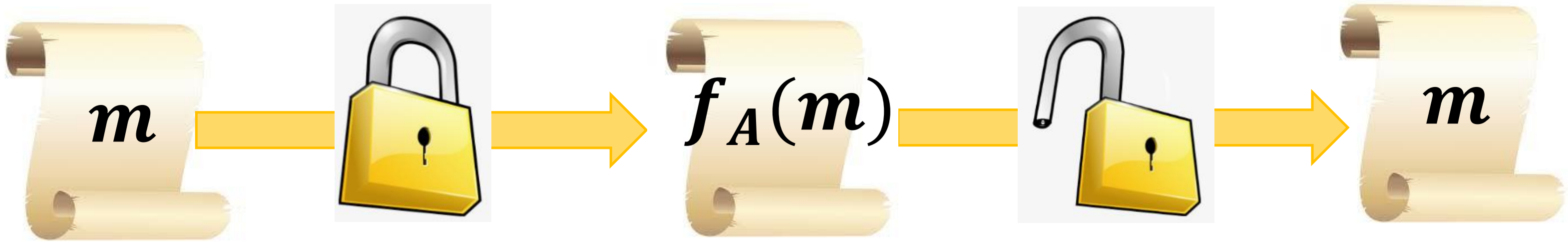
f_A fonksiyonu alıcı için şifreleme fonksiyonu olsun. Yani alıcıya gönderilen mesajlar bu fonksiyon ile şifrelensin. Burada f_A'yı hesaplamak için gereken bilgi herkes tarafından bilinebilir.

Alıcıya gönderilecek bir m mesajı $f_A(m)$ olur; böylece şifrelenir.

Fakat yalnızca alıcı bu fonksiyonun tersini alabilmelidir, yani deşifre edebilir $m = f_A^{-1}(f_A(m))$.

f_A açık anahtarı ile şifreleme

f_A^{-1} gizli anahtarı ile deşifre etme



Orjinal mesaj

Şifrelenmiş mesaj

Deşifre edilmiş mesaj

Gönderici

Alıcı

RSA en çok kullanlıan açık şifreleme methodur. Bu method moduler aritmetiğe dayanır.

Bu yüzden bu methoda geçmeden önce öncelikle moduler aritmetigi hatirlayalim.

Modüler Aritmetik

Öklid'in Bölme Teoremi: $k \geq 1$ ve n bir tamsayı olsun. Bu durumda her zaman d ve r tamsayıları bulunur öyleki:

i. $0 \leq r < k$

ii. $n = kd + r$

($n =$ bölünen, $k =$ bölen, $r =$ kalan, $d =$ bölüm)

ör. $k = 8$ ve $n = 19$ olsun. Bu durumda $d = 2$ ve $r = 3$ olur:

i. $0 \leq 3 < 8$

ii. $19 = 8 \cdot 2 + 3$

Mod

$k \geq 1$ ve n bir tamsayı olsun. n'*nin* k ile bölümünden kalan r ise $(r \leq k)$; n mod k'da r'ye denktir denir. Bu ifade şöyle gösterilir:

$$n \equiv r \ (mod\ k)$$

Aynı şekilde eğer $n \equiv r \ (mod\ k)$ ise vardır bir d tamsayısı öyleki $n = kd + r$.

Modüler Aritmetiğin Bazı Özellikleri

a , b ve k bir tamsayı ve $k > 0$ olsun. Bu durumda

$a + b \ (mod\ k) = [a \ (mod\ k) + b \ (mod\ k)](mod\ k)$
$a \cdot b \ (mod\ k) = [a \ (mod\ k) \cdot b \ (mod\ k)](mod\ k)$
$a^b \ (mod\ k) = \left[\left(a \ (mod\ k)\right)^b\right](mod\ k)$

ör. $18 + 49\ (mod\ 5) = [18\ (mod\ 5) + 49\ (mod\ 5)]\ (mod\ 5) = 3 + 4\ (mod\ 5) = 2.$

ör. $18 \cdot 49\ (mod\ 5) = [18\ (mod\ 5) \cdot 49\ (mod\ 5)]\ (mod\ 5) = 3 \cdot 4\ (mod\ 5) = 2.$

ör. $18^{49}\ (mod\ 5) = [(18\ (mod\ 5)\ )^{49}]\ (mod\ 5) = 3^{49}\ (mod\ 5) = (3^4)^{12} \cdot 3\ (mod\ 5)$

$$
\begin{aligned}
&= [(3^4)^{12}\ (mod\ 5)\ \cdot 3\ (mod\ 5)](mod\ 5) \\
&= [(3^4\ (mod\ 5))^{12}\ \cdot 3\ (mod\ 5)](mod\ 5) \\
&= [1^{12} \cdot 3\ (mod\ 5)](mod\ 5) \\
&= 3
\end{aligned}
$$

İki Sayının En Büyük Ortak Bölenini Hesaplama

Ortak bölen: n, m ve $d \neq 0$ tamsayı olsun. Eğer d sayısı n sayısını bölerse $(d|n)$ ve d sayısı b sayısını bölerse $(d|m)$ ise d, n ve m'nin bir ortak bölenidir denir.

Verilen iki sayının ortak bölenlerinin en büyüğünü (obeb) hesaplamak için öklid algoritmasını kullanacağız.

İki Sayının En Büyük Ortak Bölenini Hesaplama

```
öklid(n,m)
Giriş: pozitif tamsayılar n ve m≥n
Çıkış: obeb(n,m)
if m (mod n) == 0 {
    return n;
else
    return öklid(m (mod n), n)
```

ör. öklid (20,70) = öklid (10, 20)=10

ör. öklid(36, 93)=öklid(21,36)=öklid(15,21)=öklid(6,15)=öklid(3,6)=3

Aralarında Asal Sayılar

Eğer iki sayının ortak bölenlerinin en büyüğü 1 ise bu iki sayı aralarında asaldır denir.

Modüler Aritmetikte Bir Sayının Çarpmaya Göre Tersi

n, m ve $k \geq 1$ tamsayı olsun. Eğer

$$n \cdot m \equiv 1\ (mod\ k)$$

oluyorsa m sayisina n sayisinin $mod\ k$'da çarpmaya göre tersi denir.

ör. $mod\ 11$'de 4'un tersi 3'tür. $(4 \cdot 3 = 12\ \equiv 1\ (mod\ 11))$

Teorem: $\mathbb{Z}_n = \{0,1, \dots, n-1\}$ kümesinde bir m sayının çarpmaya göre tersinin olabilmesi için m ile n aralarında asal olmalidirlar. (yani obebleri 1 olmalı)

ör. $\mathbb{Z}_{12}$'de 5,7 ve 11'in çarpmaya göre tersleri vardır.

Fermat'ın Küçük Teoremi

p bir asal sayı olsun. a bir tamsayı ve p'nin bir katı olmamak üzere:

$$a^{p-1} \equiv 1 \; (mode \; p)$$

ör. $p = 7$ olsun. Bu durumda 7'nin katı olmayan her sayının 6. kuvveti mode 7'de 1'e denk olur.

$\mathbb{Z}_7$'deki her sayının 6. kuvveti 1'e denk olur.

Ayrıca $a^{p-1} \equiv 1 \; (mode \; p)$ denkliğinde her iki tarafı a ile çarparak $a^p \equiv a \; (mode \; p)$ denkligide kolayca elde edilir.

RSA Şifrelemesi (Rivest – Shamir – Adleman)

Alıcının Yapması Gerekenler:

1. İki tane büyük asal sayı seçilir: p ve q
2. $n = p \cdot q$
3. $(p-1) \cdot (q-1)$ çarpımıyla aralalarında asal olan bir $e \neq 1$ seçilir.
4. e'nin $mod(p-1) \cdot (q-1)$ de çarpmaya göre tersi bulunur:
$$d = e^{-1} mod(p-1) \cdot (q-1)$$
5. e ve n göndericiye gönderilir (e ve n, alıcının açık anahtarını (public key) oluşturur)
6. d gizlenir (d alıcının gizli anahtarıdır (private key))

Göndericinin Yapması Gerekenler:

1. Alıcının açık anahtarını (e ve n) alınır.
2. Gönderilecek m mesajı $f_A(m) = m^e \ (mod\ n)$ sekilde sifrelenerek alıcıya gönderilir.

RSA Şifrelemesi (Rivest – Shamir – Adleman)

<u>Alıcının Şifrelenmiş Mesajı Aldığında</u>:

Gizli anahtarı olan d'yi kullanarak şifrelenmiş mesajın $mod\ n$'de d. kuvvetini alarak gelen mesaji deşifre eder:

$$\left(m^{e}\ (mod\ n)\right)^{d} = m^{ed}(mod\ n) = m\ (mode\ n)$$

Not: Şifrelenmiş mesaj $m^{e}\ (mod\ n)$ dir. Düşman şifrelemede kullanilan açık anahtar olan e ve n'yi bilse dahi m mesajına ulaşamaz; çunku m^{e} nin $mode\ n$'de e. dereceden kökünü almak çok zor hatta imkansızdır.

Bu yüzden m mesajına ulaşmak için tek yapılmasi gereken gizli anahtar olan d'ye ulaşmaktır.

ör. Kolay bir örnek olmasi bakimindann $p = 13$ ve $q = 17$ asal sayılarını alalım. Bu durumda $n = 13 \cdot 17 = 221$ olur.

Açık anahtarı oluşturmak için $(13-1)\cdot(17-1) = 192$ ile aralarında asal olan $e = 5$ seçelim.

e'nin $mode$ 192'daki tersi $e^{-1} = d = 77$ olur. $(5^{77} \equiv 1\ (mode\ 192))$

Açık anahtar : $(5{,}221)$

Gizli anahtar: $(77{,}221)$

Örnegin gönderilecek mesaj $m = 45$ olsun.

Şiferlenmiş mesaj: $45^5\ (mode\ 221) = 197\ (mode\ 221)$

Deşifre edilen mesaj: $197^{77}\ (mode\ 221) = 45.$