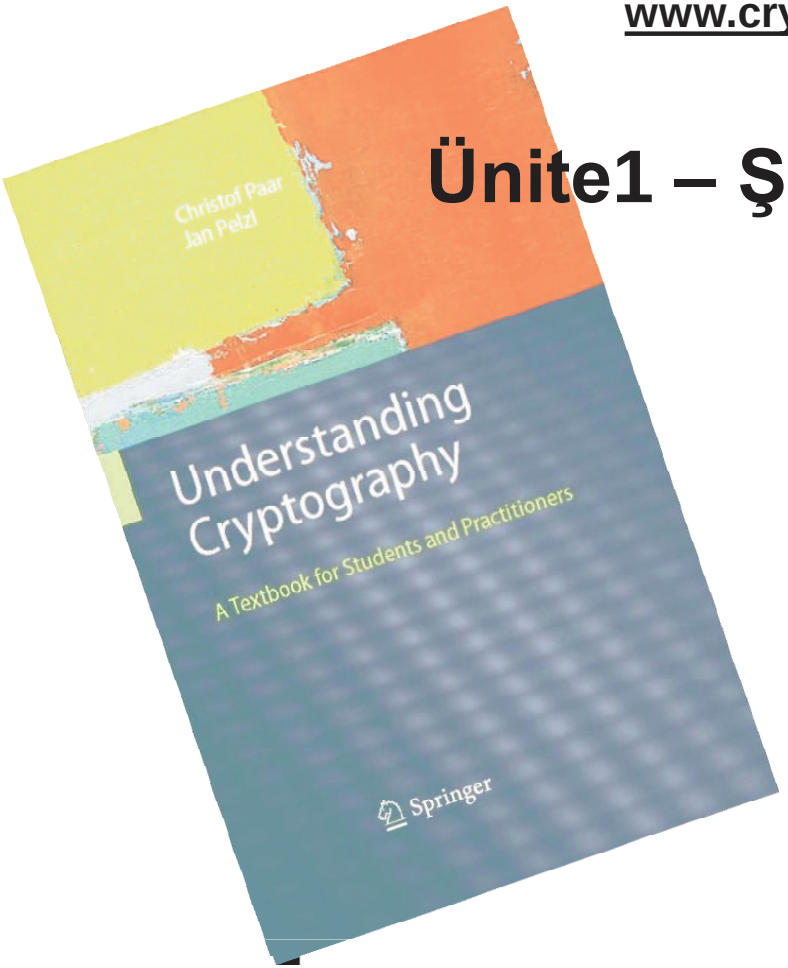
Understanding Cryptography – Öğrenci ve Uygulamacılar İçin Ders kitabı

www.crypto-textbook.com



Ünite1 – Şifrelemeye Giriş

Ünite içeriği

- Şifreleme alanlarına genel bakış
- Simetrik şifrelemenin temelleri
- Kripto analiz
- Yer değiştirmeli şifreleme
- Modüler aritmetik
- Kaymalı (veya sezar) şifreleme ve Affine şifreleme

Ünite içeriği

- **Şifreleme alanlarına genel bakış**
- Simetrik şifrelemenin temelleri
- Kripto analiz
- Yer değiştirmeli şifreleme
- Modüler aritmetik
- Kaymalı (veya sezar) şifreleme ve Affine şifreleme

- Şifreleme hakkında daha çok okuma ve bilgi

Addition to *Understanding Cryptography* .

- A.Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, October 1996.
- H.v.Tilborg (ed.), *Encyclopedia of Cryptography and Security*, Springer, 2005

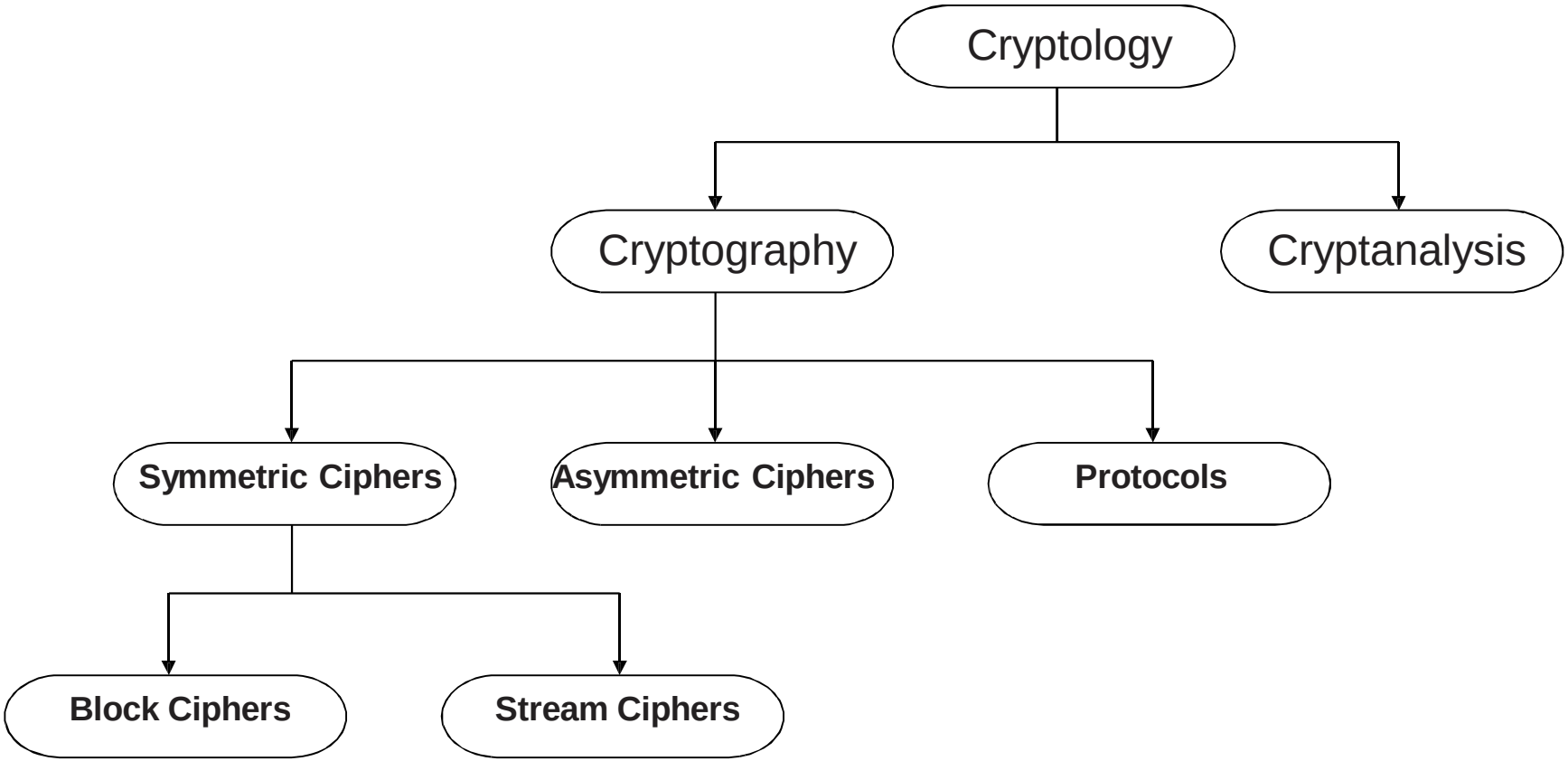
History of Cryptography (great bedtime reading)

- S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography,* Anchor, 2000.
- D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. 2nd edition, Scribner, 1996.

Software (excellent demonstration of many ancient and modern ciphers)

- *Cryptool, http://www.cryptool.de*

- **Şifreleme alanlarının sınıflandırılması**



Bazı temel gerçekler

- **İlk çağ şifreleme:** ilk şifreleme işaretleri M.Ö. 2000 mısırda kahirede görülmüştür. Harf-tabanlı şifreleme yapısı (örneğin sezar şifreleme) ondan sonra popülerleşti.

- **Simetrik şifreleme:** Tarih öncesi zamanlardan 1976 ya kadar olan bütün şifreleme yapıları buna örnektir.

- **Asymmetric ciphers:** 1976'da açık anahtar (veya asimetrik) şifreleme Diffie, Hellman ve Merkle tarafından açık bir şekilde önerildi.

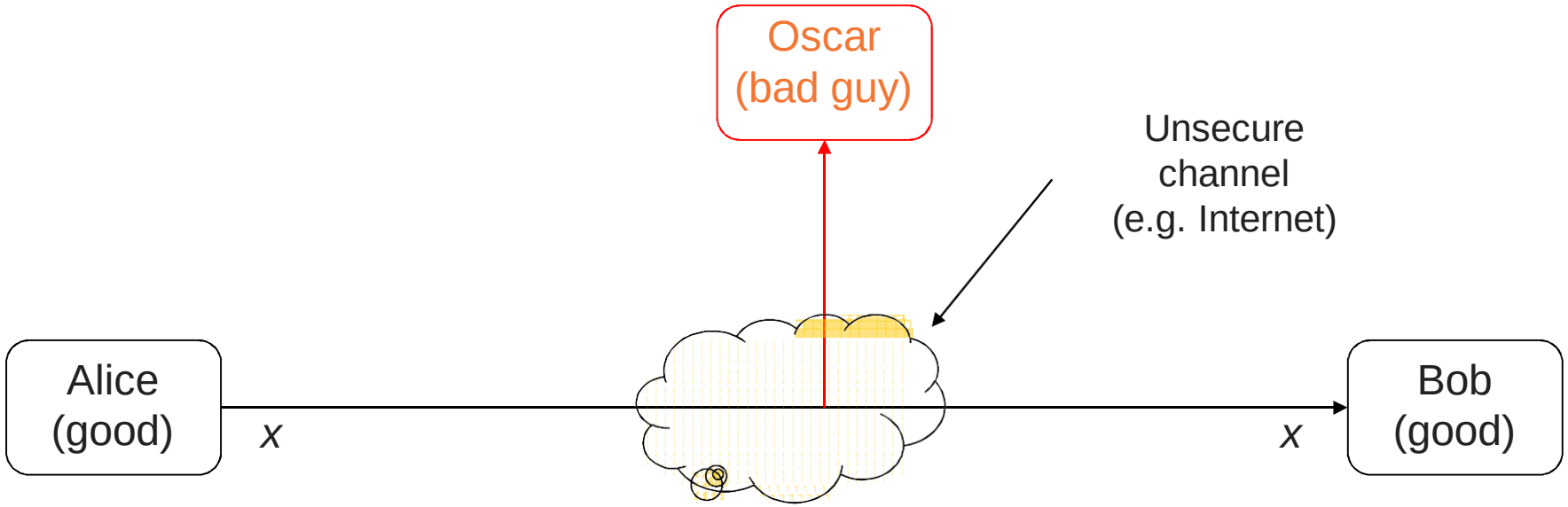
- **Karışık yapılar:** günümüz protokollerinin büyük bir kısmı bu yapıdadır, örneğin ikisini kullanan
  - Simetrik şifreleme (örneğin şifreleme ve mesaj doğrulama için) ve
  - Asimetrik şifreleme (örneğin; mesaj değişimi ve sayısal imza için).

Ünite içeriği

- Şifreleme alanlarına genel bakış
- **Simetrik şifrelemenin temelleri**
- Kripto analiz
- Yer değiştirmeli şifreleme
- Modüler aritmetik
- Kaymalı (veya sezar) şifreleme ve Affine şifreleme

- **Symmetric Cryptography**

Alternatif isimler: **özel anahtarlı**, **tek anahtarlı** veya **gizli anahtarlı** şifreleme.



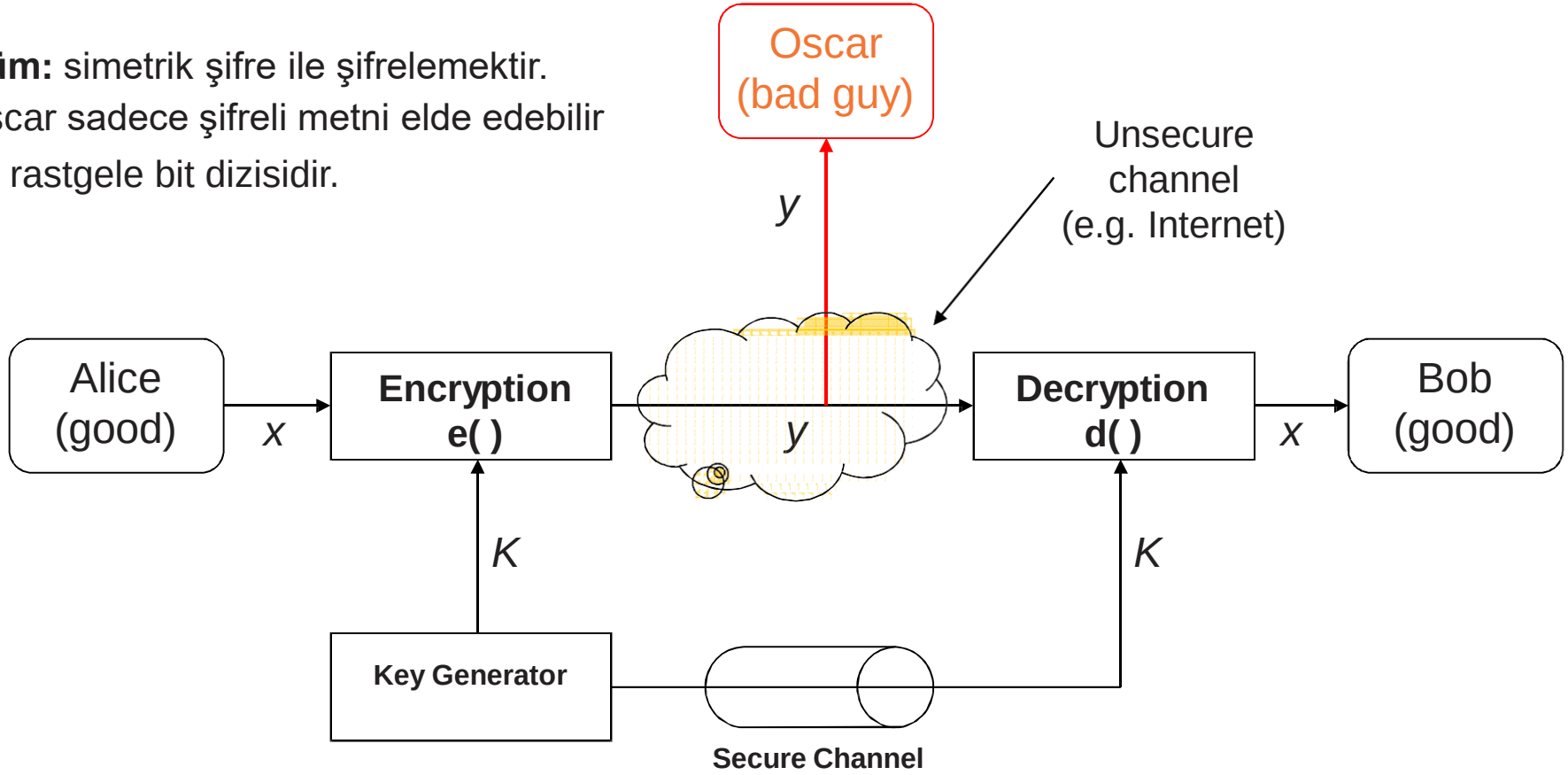
- **Problem Statement:**

1)Alice ve BOB güvenli olmayan kanal üzerinden haberleşmek istiyorlar (örneğin, WLAN veya Internet).

2) kötü niyetli üçüncü kişi olan Oscar kanala ulaşabilir fakat fakat haberleşmeyi anlayamamalı.

- **Symmetric Cryptography**

Çözüm: simetrik şifre ile şifrelemektir.
⇒ Oscar sadece şifreli metni elde edebilir
buda rastgele bit dizisidir.



- x **düz metin**
- y **şifreli metin**
- *K* **anahta**r değeri
- Bütün anahtar değerleri {*K*1, *K*2, ...,*Kn*} **anahtar uzayıdı**r

- **Simetrik şifreleme**

• Şifreleme denklemi	$\mathbf{y = e_K(x)}$
• Şifre çözme denklemi	$\mathbf{x = d_K(y)}$

- İki tarafta da aynı anahtar değeri kullanılıyorsa şifreleme ve şifre çözme işlemleri birbirinin tersidir:

$$d_K(y) = d_K(e_K(x)) = x$$

- önemli: anahtar Bob ve Alice arasında güvenli bir kanaldan iletilmeli.
- Güvenli kanal kurye veya benzeri yöntemlerle oluşturulabilir.
- Bununla birlikte saldırgan K anahtar değerini bilmediği sürece güvenlidir.

⇒ **güvenli haberleşme problemini güvenli iletim ve K anahtar değerinin saklanması azaltmaktadır.**

Ünite içeriği

- Şifreleme alanlarına genel bakış
- Simetrik şifrelemenin temelleri
- Kripto analiz
- **Yer değiştirmeli şifreleme (The Substitution Cipher)**
- Modüler aritmetik
- Kaymalı (veya sezar) şifreleme ve Affine şifreleme

• Yer Değiştirmeli Şifreleme (The Substitution Cipher)

- Tarihsel şifreleme
- Kaba kuvvet vs analitik saldırıları anlamak için harika bir araç
- İkinci dünya savaşına kadar bitlerden ziyade harflere dayanan şifreler kullanıldı.

fikir: düz metindeki her bir harfe şifreli metinde sabit bir harfle yer değiştirsin.

Plaintext		Ciphertext
A	→	k
B	→	d
C	→	w
	....	

örneğin, `ABBA kddk gibi şifrelenebilir`

- örnek (şifreli metin):

```
iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnb hcc
hwwhbsqvqbre hwq vhlq
```

- Yer değiştirmeli şifreleme ne kadar güvenlidir? Saldırılara bakalım…

- **Yer değiştirme şifrelemeye karşı saldırılar**

1. **Saldırı: sonsuz anahtar arama (kaba kuvvet saldırısı)**

- Basitçe mantıklı bir düz metin elde edilene kadar bütün mümkün yer değiştirmelerin yapılması (dikkat edin ki yer değiştirme bir anahtardır)..
- How many substitution tables (= keys) are there?

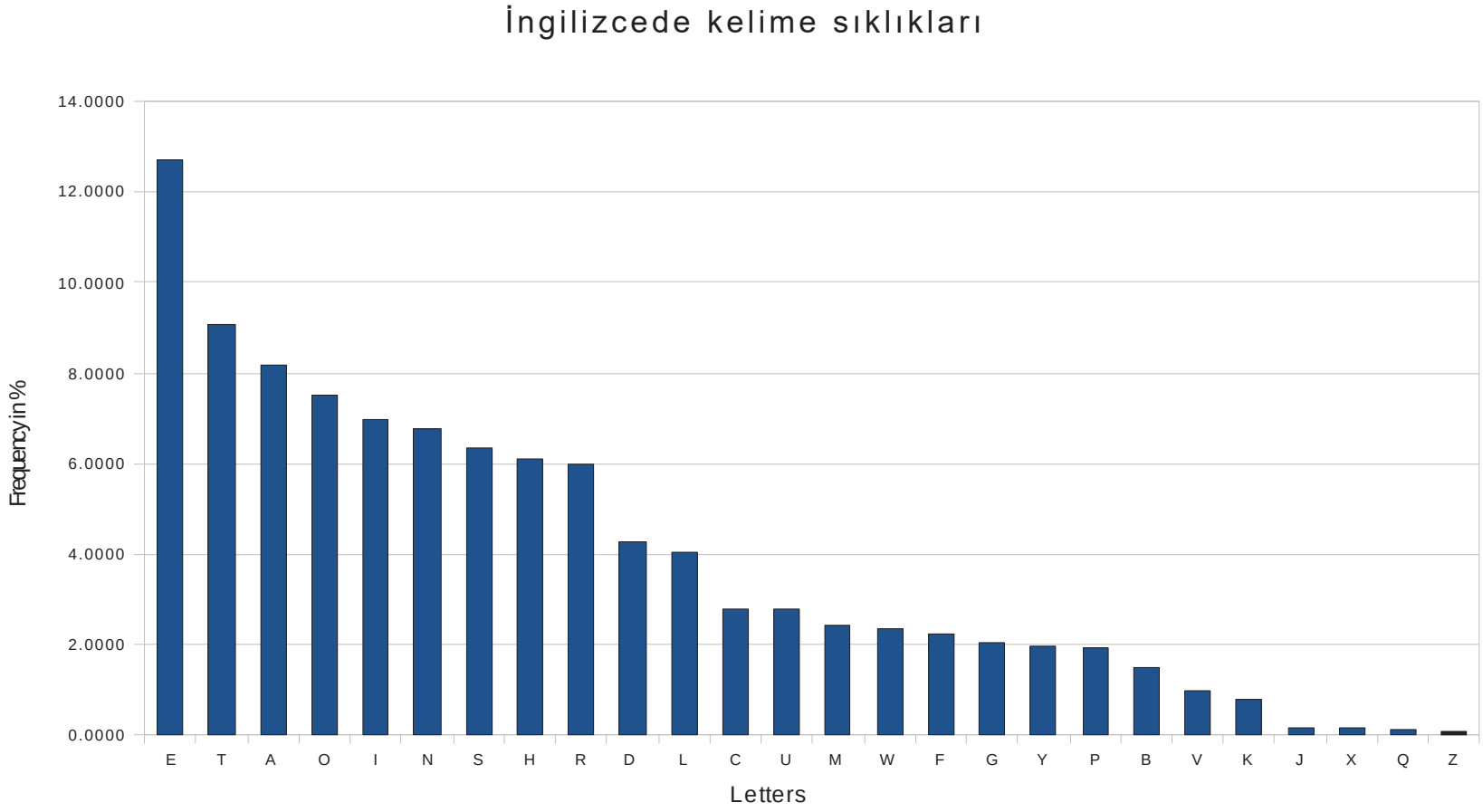
$$26 \times 25 \times \ldots \times 3 \times 2 \times 1 = 26! \approx 2^{88}$$

2^{88} Anahtar arasından değerleri araştırmak günümüz bilgisayarları için mümkün değildir!

- S: kaba kuvvet saldırısı mümkün olmadığı için yer değiştirme şifresinin güvenli olduğunu çıkarabilir miyiz?
- A: hayır! Bütün saldırılara karşı güvenli olmalıdır…

- **2. saldırı: harf frekanslarının analizi (kaba kuvvet saldırısı)**

- İngilizcede harflerin farklı kullanım sıklığı vardır.
- Dahası: düz metindeki sıklık şifreli metinde de korunur.
- Örneğin, „e“ ingilizcede en çok kullanılan harftir; tipik bir ingilizce metindeki harflerin 13% „e“ dir.
- Diğer en çok kullanılan harf yaklaşık 9% la t’ dir.



- **Harf sıklıkları analiziyle yer değiştirme şifrelerinin kırılması**

- Şimdi örneğimize dönüp en çok geçen harfi bulalım:

  `iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnb hcc hwwhbsqvqbre hwq vhlq`

- Şimdi şifreli metinde `q'nun yerine E yazalım`:

  `iE ifcc vEEr fb rdE vfllcE na rdE cfjwhwz hr bnnb hcc hwwhbsEvEbre hwE vhlE`

- Kalan harflerin sıklığına dayanarak daha fazla tahmin yapılır ve düz metin bulunur:

  `WE WILL MEET IN THE MIDDLE OF THE LIBRARY AT NOON ALL ARRANGEMENTS ARE MADE`

Relative letter frequencies of the English language

Letter	Frequency	Letter	Frequency
A	0.0817	N	0.0675
B	0.0150	O	0.0751
C	0.0278	P	0.0193
D	0.0425	Q	0.0010
E	0.1270	R	0.0599
F	0.0223	S	0.0633
G	0.0202	T	0.0906
H	0.0609	U	0.0276
I	0.0697	V	0.0098
J	0.0015	W	0.0236
K	0.0077	X	0.0015
L	0.0403	Y	0.0197
M	0.0241	Z	0.0007

- **Harf sıklıkları analiziyle yer değiştirme şifrelerinin kırılması**

  - Pratikte, sadece harflerin değil ingilizcede sık kullanılan kelime ikilileri ve üçlüleri de şifreli metni çözmek için kullanılır.
  - Problem 1.1 in *Understanding Cryptography* kitabın ilgili metnindeki şifreli metni kırmaya çalışabilirsiniz!

önemli ders: yer değiştirmeli şifre 2^{88} gibi yeterli büyüklükte anahtar uzayına sahip olmasına rağmen, sayısal yöntemlerle kolaylıkla kırılabilir. Bu şifreleme yapılarının bütün saldırılara karşı dayanıklı olması gerektiğini gösteren çok güzel bir örnektir.

FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK
APRKDLYEVLRHHRH

FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK
APRKDLYEVLRHHRH

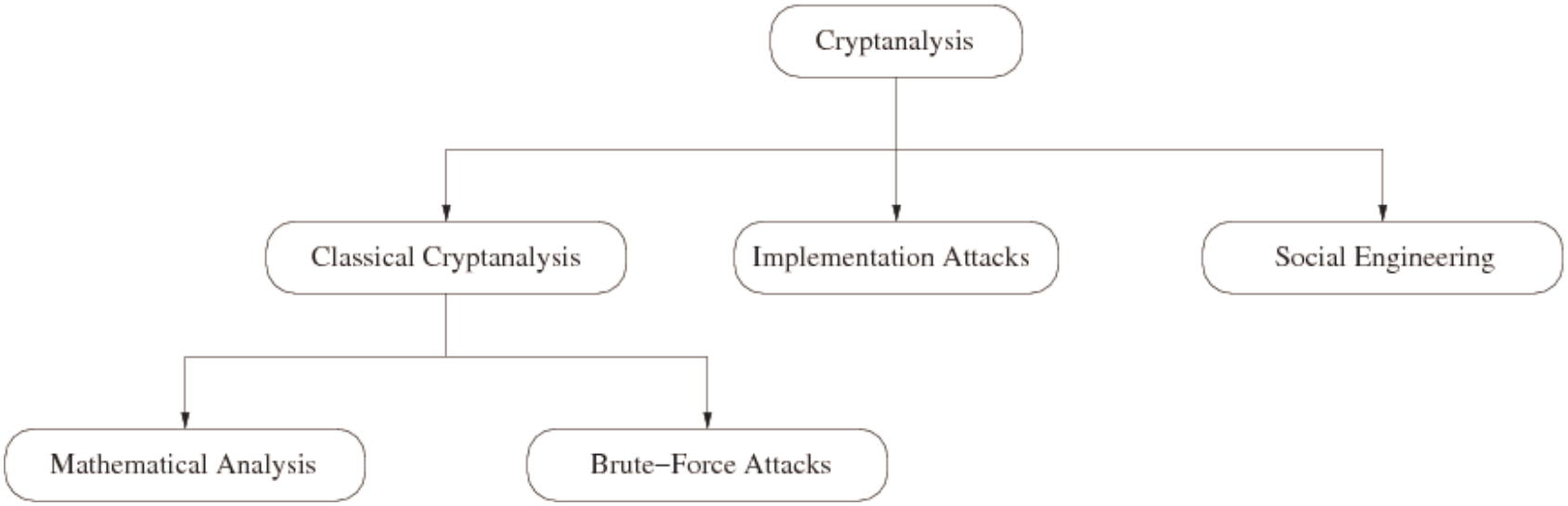
algorithmsarequitegeneraldefinitionsofarit
hmeticprocesses

Ünite içeriği

- Şifreleme alanlarına genel bakış
- Simetrik şifrelemenin temelleri
- **Kripto analiz**
- Yer değiştirmeli şifreleme
- Modüler aritmetik
- Kaymalı (veya sezar) şifreleme ve Affine şifreleme

- **Neden kripto analize ihtiyaç duyarız?**

- Herhangi pratik bir şifre için güvenliğin matematiksel bir kanıtı yoktur.
- Sistemin güvenli olduğunu garanti etmenin tek yolu sistemi kırmaya çalışmaktır!



- **Şifre Analizi: Şifreleme Sistemlerine Saldırı**

- **Klasik saldırılar**
  - Matematiksel analiz
  - Kaba kuvvet saldırısı
- **Uygulama saldırıları**: Ters mühendislikle veya güç ölçümüyle anahtar değerini çıkarmaya çalışırız, örneğin bankalar için kullanılan banking smart card.
- **Sosyal mühendislik**: örneğin kullanıcının şifresini vermesi için kandırmak

Kerckhoff prensibi

Kerckhoff prensibi modern şifrelemede çok iyidir:

Saldırgan gizli anahtar dışında sistemle ilgili her şeyi biliyor olsa bile şifreleme sistemi güvenli olmalıdır .

- Kirşof prensiplerini pratikte uygulayabilmek için:
  Sadece iyi şifreleyiciler tarafından birkaç yıl kriptoanaliz edilmiş geniş bir ölçekte kullanılan şifreler kullanılmalı! (*Understanding Cryptography* only treats such ciphers)
- **dikkat:** şifrelemenin daha güvenli olması için şifreleme yapısının detaylarını gizlemek daha cazip gelebilir. Bununla beraber, fakat zaman gösteriyor ki bu yapılar mühendisler tarafından incelendiğinde her zaman kırılmıştır. (örneğin: DVD içeriğini korumak için kullanılan program Content Scrambling System (CSS).)

- **Simetrik Şifrelemeye Karşı Kaba Kuvvet Saldırısı**

- Şifreye blok kutular gibi davranır.
- En az bir düz metin şifreli metin çifti (x_0, y_0) gerekir.
- Şart gerçekleşene kadar bütün mümkün anahtarları kontrol eder:

$$d_K(y_0) \stackrel{?}{=} x_0$$

- Kaç Anahtar Biti Yeterlidir?

Key length in bit	Key space	Security life time (assuming brute-force as best possible attack)
64	2^{64}	**Short term** (few days or less)
128	2^{128}	**Long-term** (several decades in the absence of quantum computers)
256	2^{256}	**Long-term** (also resistant against quantum computers – note that QC do not exist at the moment and might never exist)

Önemli: karşı taraf başarmak için sadece bir saldırıya ihtiyaç duyar. Böylece, sosyal mühendislik gibi diğer saldırılar yapılabiliyorsa uzun anahtar uzayı pekte faydalı olmayacaktır..

Key	Key	Worst case time at speed:		
length	space	109/sec	1012/sec	1015/sec
32	232	4 sec	4 ms	4 us
56	256	833 days	20 hrs	72 sec
64	264	584 yrs	213 days	5 hrs
80	280	107 yrs	104 yrs	38 yrs
100	2100	1013 yrs	1010 yrs	107 yrs
128	2128	1022 yrs	1019 yrs	1016 yrs
192	2192	1041 yrs	1038 yrs	1035 yrs
256	2256	1060 yrs	1057 yrs	1054 yrs
26!	288	1010 yrs	107 yrs	104 yrs

Ünite içeriği

- Şifreleme alanlarına genel bakış
- Simetrik şifrelemenin temelleri
- Kripto analiz
- Yer değiştirmeli şifreleme
- **Modüler aritmetik**
- Kaymalı (veya sezar) şifreleme ve Affine şifreleme

- **Modüler aritmetiğe kısa bir giriş**

Neden modüler aritmetik çalışmaya ihtiyacımız var?

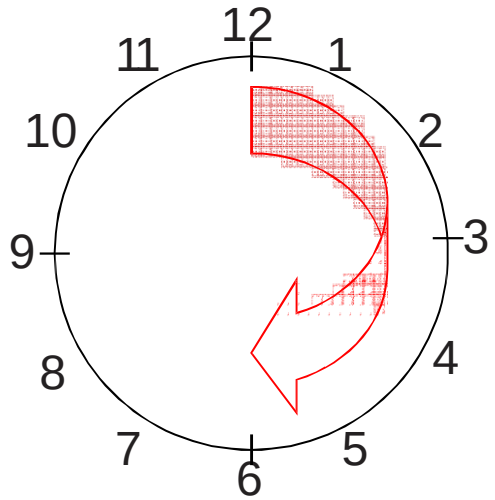
- Asimetrik şifreleme için çok önemlidir (RSA, elliptic curves gibi.)
- Bazı tarihsel şifreler modüler aritmetikle güzel bir şekilde ifade edilebilir(örneğin Caesar and affine cipher later on).

- **Modüler aritmetiğe kısa bir giriş**

Genel konuşursak, birçok şifreleme sistemi sayı kümelerine dayanır şöyle ki

1. **ayrı** (sayılı kümeler oldukça faydalıdır)
2. **sonlu** (ör. sadece sonlu sayılarla hesaplayabilirsek)

çok mu soyut gözüküyor? --- şimdi sonlu kümelere ayrık sayılarla bakalım saate oldukça aşinayızdır.



Enteresan bir şekilde, saat sürekli artmasına rağmen biz belli bir sayı kümenin dışına çıkmayız:

1, 2, 3, … 11, 12, 1, 2, 3, … 11, 12, 1, 2, 3, …:

- **Modüler aritmetiğe kısa bir giriş**

- saate bulunan (1,2,3, … ,12) gibi sayılarla sonlu bir kümeyi hesaplamak için bir aritmetik sistem geliştirelim.
- Çarpma ve toplama gibi işlemlerden sonra elde edilen sayıların yine küme içerisinde kalması çok önemlidir. (örneğin asla 12 den büyük olamaz).

Definition: Modulus Operation

Let *a, r, m* be integers and $m > 0$. We write

$$a \equiv r \bmod m$$

if *(r-a) is divisable by m.*

- "*m*" is called the **modulus (modül)**
- "*r*" is called the **remainder (kalan)**

Modüler azalma için bir örnek.

- Let a= 12 and m= 9 : $12 \equiv 3 \bmod 9$
- Let a= 37 and m= 9: $34 \equiv 7 \bmod 9$
- Let a= -7 and m= 9: $-7 \equiv 2 \bmod 9$

- Modüler aritmetiğin özellikleri

- **Kalan tek değildir**

Şurası ilginçtir ki verilen bir mod m'de kalan a değerine karşılık sonsuz değer denk gelmektedir.

örneğin:

- $12 \equiv 3 \bmod 9$ → 3 geçerli kalandır çünkü 9 böler (3-12)
- $12 \equiv 21 \bmod 9$ → 21 geçerli kalandır çünkü 9 böler(21-12)
- $12 \equiv -6 \bmod 9$ → 6 geçerli kalandır çünkü 9 böler (-6-12)

$$\{\ldots, -24, -15, -6, 3, 12, 15, 24, \ldots\}$$

form what is called an *equivalence class*. There are eight other equivalence classes for the modulus 9:

$$\{\ldots, -27, -18, -9, 0, 9, 18, 27, \ldots\}$$
$$\{\ldots, -26, -17, -8, 1, 10, 19, 28, \ldots\}$$
$$\vdots$$
$$\{\ldots, -19, -10, -1, 8, 17, 26, 35, \ldots\}$$

- Modüler aritmetiğin özellikleri

- **Hangi kalanı seçmeliyiz?**

Genel olarak, ***en küçük pozitif sayı r*** yi alırız. Bu sayı şöyle hesaplanabilir:

quotient remainder

$$a = q \; m + r \qquad \text{where } 0 \le r \le m-1$$

- Example: $a=12$ and $m= 9$

$$12 = 1 \times 9 + 3 \qquad \rightarrow \; r = 3$$

dikkat: This is just a convention. Algoritmik olarak şifreleme fonksiyonumuzu hesaplamak için herhangi bir geçerli kalan kümesini almakta serbestiz .

- Modüler aritmetiğin özellikleri

- **Modüler bölme işlemi nasıl yapılır?**

İlk olarak, şunu belirtelim ki, bölme yapmaktan çok tersini alarak çarpmayı tercih ederiz.
Ex:

$$b / a \equiv b \times a^{-1} \bmod m$$

a^{-1} sayısı a sayısının tersidir *ve şöyle tanımlanır*:

$$a\, a^{-1} \equiv 1 \bmod m$$

Ex: $5 / 7 \bmod 9$ nedir ?

mod 9 da 7 nin tersi *4* çünkü $7 \times 4 \equiv 28 \equiv 1 \bmod 9$, böylece:

$$5 / 7 \equiv 5 \times 4 = 20 \equiv 2 \bmod 9$$

- **Ters hesaplama nasıl yapılır?**

a sayısının *mod m* d tersi vardır eğer sadece ve sadece:

$$\gcd(a, m) = 1$$

(yukarıdaki örneğe dikkat edildiğinde gcd(5, 9) = 1, bundan dolayı modulo 9 da 5 in tersi vardır)

Understanding Cryptography kitabının 6. ünitesinde bu konu daha ayrıntılı anlatılmıştır.

- **Modüler aritmetiğe cebirsel bakış: halka Z_m**

Modüler aritmetiği kümeler ve küme içindeki işlemler açısından görebiliriz. Aritmetik modülü m yaparak, aşağıdaki özelliklere sahip Z_m tamsayı halkasını elde ederiz:

- **Kapatma**: herhangi iki sayıyı toplayıp çarpabiliriz sonuç yine halka içindedir.
- Toplama ve çarpmada birleşme özelliği vardır ör: $a,b,c \in Z_m$

  için $a + (b + c) = (a + b) + c$

  $a \times (b \times c) = (a \times b) \times c$

  Ve toplamada **değişim** özelliği de vardır: $a + b = b + a$
- **dağılma kuralı** : $a\times(b+c) = (a\times b)+(a\times c)$ şeklindedir $a,b,c \in Z_m$

  toplama için etkisiz eleman sıfırdır, i.e., for all $a \in Z_m$ $a + 0 \equiv a \bmod m$
- $\in Z_m$, her zaman **toplamaya göre tersi –*a*** vardır. Şöyle ki

  $a + (-a) \equiv 0 \bmod m$
- **çarpmaya göre etkisiz eleman 1 dir**, örneğin $a \in Z_m$ *için*

  $a \times 1 \equiv a \bmod m$
- **çarpmaya göre ters a^{-1}**

  $a \times a^{-1} \equiv 1 \bmod m$

  Z_m deki bazı değerler için vardır hepsi için olmayabilir.

- **Modüler aritmetiğe cebirsel bakış: halka Z_m**

Kısaca, halka üzerinde toplama çıkarma çarpma işlemlerini yapabildiğimiz bir yapıdır fakat sadece bazı elemanları bölebiliriz (yani çarpmaya göre tersi olanları).

- Eğer sadece : gcd *(a, m) = 1 ise* Z_m deki bir sayının çarpmaya göre tersi vardır.

  o zaman *a* ve *m* nin aralarında asal olduğunu söyleyebiliriz.

$$a \cdot a^{-1} \equiv 1 \bmod m$$

- Ör: şu halkaya dikkat edersek $Z_9 = \{0,1,2,3,4,5,6,7,8\}$
  0, 3 ve 6 nın tersi yoktur çünkü bu sayılar 9 la aralarında asaldır. Diğer elemanların tersi ise şu şekildedir:

$1^{-1} \equiv 1 \bmod 9$	$2^{-1} \equiv 5 \bmod 9$	$4^{-1} \equiv 7 \bmod 9$
$5^{-1} \equiv 2 \bmod 9$	$7^{-1} \equiv 4 \bmod 9$	$8^{-1} \equiv 8 \bmod 9$

Ünite İçeriği

- Şifreleme alanlarına genel bakış
- Simetrik şifrelemenin temelleri
- Kripto analiz
- Yer değiştirmeli şifreleme
- Modüler aritmetik
- **Kaymalı (veya sezar) şifreleme ve Affine şifreleme**

- **kaymalı (veya Sezar) şifreleme**

- İlk şifrelerin Julius Caesar tarafından kullanıldığı iddia edilir.
- Düz metindeki her harfin yerine bir harf yazılır.
- Değişim kuralı oldukça basit: belirlenen bir k anahtar değeriyle her harften k:sonraki harf alınır.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Örnek *k = 7 için*

Düz metin = `ATTACK` = 0, 19, 19, 0, 2, 10

Şifreli metin = `haahr` = 7, 0, 0, 7, 17
Burada işlemler mod 26 da yapılmaktadır yani 26 değerini aşan durumda mod 26 daki değeri alınır.

- **Kaymalı (veya Sezar) Şifreleme**

- Şifrelemenin zekice matematiksel tarifi.

Let k, x, y ε {0,1, …, 25}

- Encryption: $y = e_k(x) \equiv x + k \bmod 26$
- Decryption: $x = d_k(x) \equiv y - k \bmod 26$

- S; kaymalı şifre güvenli midir?
- C: Hayır! Birkaç saldırı mümkün, including:
  - Sonsuz anahtar arama (anahtar uzayı sadece 26!)
  - Harf sıklığı analizi, yer değiştirme şifresinde olduğu gibi

Affine Şifreleme

- Kaymalı şifrenin gelişmiş hali: düz metne sadece anahtar değerini eklemekten ziyade, başka bir anahtar değeriyle de toplarız.
- Burada iki parçadan oluşan bir anahtar değeri kullanırız: k = (a, b)

Let k, x, y ε {0,1, …, 25}

- Encryption: $y = e_k(x) \equiv a\,x + b \bmod 26$
- Decryption: $x = d_k(x) \equiv a^{-1}(\,y - b) \bmod 26$

- Şifreleme işleminde tersini almaya ihtiyaç duyduğumuz için, aşağıdaki ifadeye göre sadece tersi olan sayılar kullanılır:

$$\gcd(a, 26) = 1$$

bu şartı sağlayan 12 değer vardır.

- Bundan dolayı anahtar uzayı sadece 12 x 26 = 312 (cf. Sec 1.4 in *Understanding Cryptography*)
- Yine aşağıdakileri içeren birkaç saldırı vardır:
  - Detaylı anahtar uzayı ve harf sıklığı analizi, yer değiştirme şifresine karşı benzer saldırılar.