



یادداشت‌های امن و ایمنی

امنیت داده و شبکه

مفاهیم رمزنگاری و رمزنگاری کلاسیک

مرتضی امینی - نیمسال دوم ۱۴۰۰-۱۳۹۹



فهرست مطالب

□ تعاریف

□ نیازمندی‌های رمزنگاری

□ رمز کلاسیک - جانشینی

□ رمز کلاسیک - جایگشت



تعاریف اولیه

□ **Plaintext:** the original message

□ متن آشکار: پیام اصلی رمز نشده

□ **Ciphertext:** the coded message

□ متن رمز: پیام رمز شده

□ **Cipher:** algorithm for transforming plaintext to ciphertext

□ رمز: الگوریتم تبدیل متن آشکار به متن رمز

□ **Key:** info used in cipher known only to sender/receiver

□ **کلید:** اطلاعاتی که در رمز مورد استفاده قرار می‌گیرد و فقط فرستنده و/یا گیرنده پیام آن را می‌دانند.



تعاریف اولیه

□ **Encipher (encrypt):** converting plaintext to ciphertext

□ رمزگذاری: تبدیل متن آشکار به متن رمز

□ **Decipher (decrypt):** recovering plaintext from ciphertext

□ رمزگشایی: استخراج متن آشکار از متن رمز



تعاریف اولیه

- **Cryptography:** study of encryption principles/methods

□ رمز نویسی: علم اصول و روش های رمز گذاری

- **Cryptanalysis (codebreaking):** the study of principles/ methods of deciphering ciphertext *without* knowing key

□ تحلیل رمز: علم اصول و روش های رمز گشایی متن رمز بدون اطلاع از کلید

- **Cryptology:** the field of both cryptography and cryptanalysis

□ رمز نگاری: علم حاصل از ترکیب رمز نویسی و تحلیل رمز

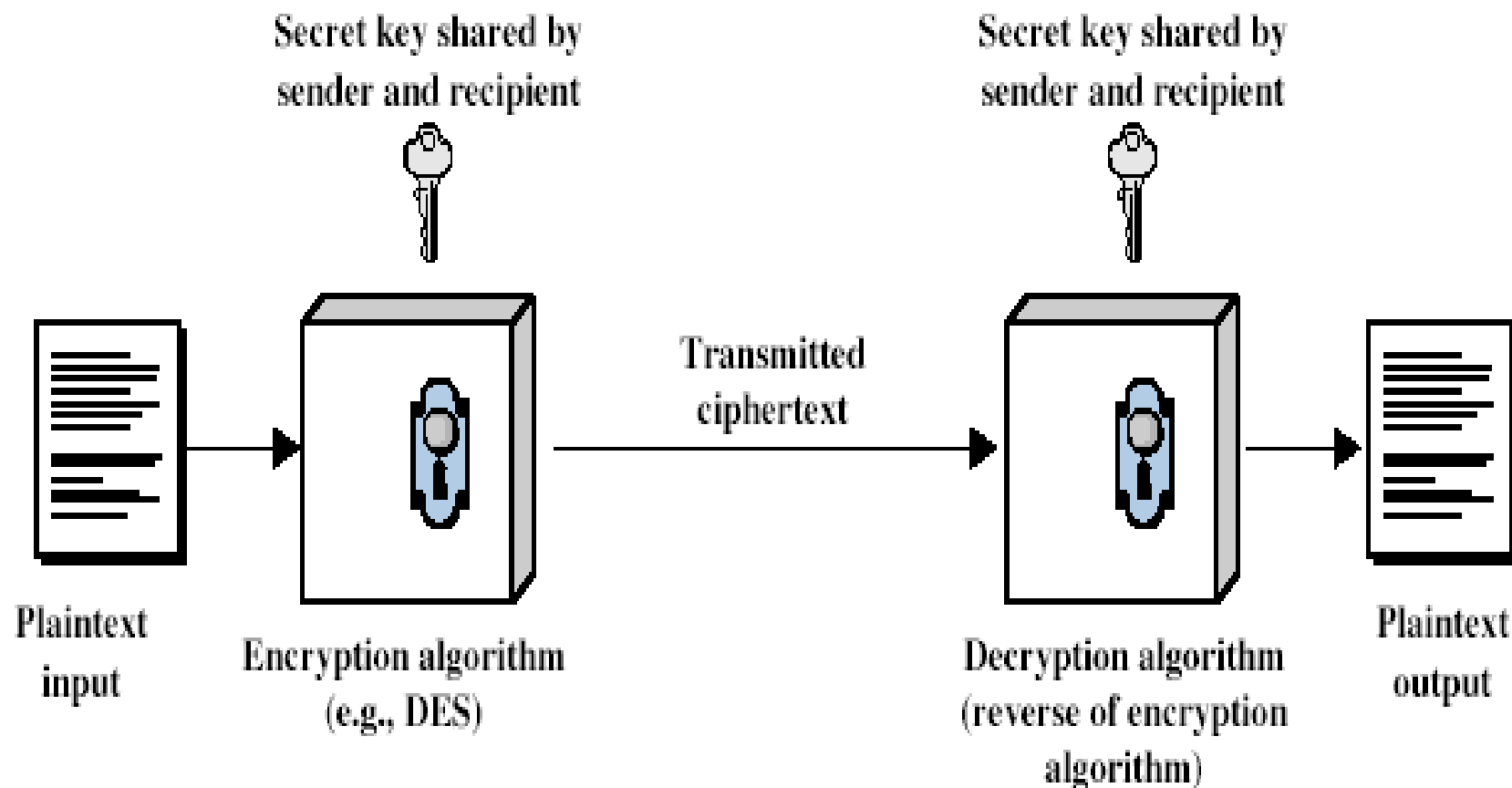


رمزنگاری متقارن (Symmetric)

- معادل با رمزنگاری معمولی / رمزنگاری کلید خصوصی / رمزنگاری تک کلیدی
- فرستنده و گیرنده از یک کلید مشترک استفاده می کنند.
- تمام رمزنگاری های کلاسیک از نوع متقارن هستند.
- تنها نوع رمزنگاری تا قبل از دهه ۷۰



مدل رمزنگاری متقارن





فهرست مطالب

□ تعاریف

□ نیازمندی‌های رمزنگاری

□ رمز کلاسیک - جانشینی

□ رمز کلاسیک - جایگشت



نیازمندی‌ها

□ دو نیازمندی برای استفاده امن از رمزنگاری متقارن:

■ یک الگوریتم رمزنگاری قوی

■ یک کلید سری که تنها فرستنده و گیرنده از آن آگاه هستند.

$$Y = E_K(X)$$

$$X = D_K(Y)$$

□ فرض بر آن است که الگوریتم برای همه مشخص است.

□ بنابراین نیاز به یک کانال امن برای توزیع کلید است.



ابعاد رمزنگاری

□ اعمال مورد استفاده برای رمزگذاری

- جانشینی (Substitution): جایگزینی هر عنصر با عنصری دیگر
- جایگشت (Transposition): جابجایی عناصر رمز شده

□ تعداد کلیدهای مورد استفاده

- یک کلید خصوصی مشترک
- یک جفت کلید برای هر طرف ارتباط (کلید عمومی + کلید خصوصی)

□ روش پردازش متن آشکار

- بلوکی: بلوکی از عناصر متن پردازش و رمز می شوند.
- جریان: عناصر متن به طور پیوسته به ورودی داده شده و در هر لحظه یک عنصر رمز شده خارج می شود.



حملات تحلیل رمزنگاری

□ هدف از حمله:

- استخراج کلید
- استخراج متن آشکار از متن رمز شده

□ نحوه حمله:

- بررسی خصوصیات الگوریتم رمز
- بررسی مجموعه‌ای از متن‌های آشکار و رمز شده آنها



انواع حملات تحلیل رمزنگاری

اطلاعات در اختیار تحلیلگر رمز	نوع حمله
<ul style="list-style-type: none">• الگوریتم رمز• متن رمز	ciphertext only
<ul style="list-style-type: none">• الگوریتم رمز• متن رمز• یک یا چند جفت متن آشکار و رمز شده آن	known plaintext
<ul style="list-style-type: none">• الگوریتم رمز• متن رمز• متن آشکار انتخاب شده توسط تحلیلگر و متن رمز معادل آن	chosen plaintext
<ul style="list-style-type: none">• الگوریتم رمز• متن رمز• متن رمز انتخاب شده توسط تحلیلگر و متن آشکار حاصل از رمزگشایی آن	chosen ciphertext
<ul style="list-style-type: none">• الگوریتم رمز• متن رمز• متن آشکار انتخاب شده توسط تحلیلگر و متن رمز معادل آن• متن رمز انتخاب شده توسط تحلیلگر و متن آشکار حاصل از رمزگشایی آن	chosen text

جستجوی تمام حالات (Brute Force Search)



□ ابتدایی ترین حمله

□ فرض بر این است که متن آشکار قابل شناسایی است.

	Key size (bits)	Number of alternative keys	Time required at 1 decryption/ μ s	Time required at 10^6 decryption/ μ s
DES →	32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu$ s = 35.8 minutes	2.15 milliseconds
AES →	56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu$ s = 1142 years	10.01 hours
3DES →	128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu$ s = 5.4×10^{24} years	5.4×10^{18} years
Substitution code →	168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu$ s = 5.9×10^{36} years	5.9×10^{30} years
	26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu$ s = 6.4×10^{12} years	6.4×10^6 years



دیگر تعاریف

□ امنیت مطلق

- مستقل از قدرت محاسباتی در دسترس، متن رمز شده اطلاع کافی برای تعیین قطعی متن آشکار ارائه نکند (و بنابراین الگوریتم رمز مستقل از مدت زمانی که مهاجم در اختیار دارد قابل شکستن نباشد).

□ امنیت محاسباتی

- با داشتن منابع محاسباتی محدود (مانند زمان)، رمز قابل شکستن نباشد.



فهرست مطالب

□ تعاریف

□ نیازمندی‌های رمزنگاری

□ رمز کلاسیک - جانشینی

□ رمز کلاسیک - جایگشت



رمزهای کلاسیک

- از زمان جنگ جهانی دوم مورد استفاده قرار می گرفتند.
- قبل از به وجود آمدن سیستم‌های کامپیوتری امروزی بصورت دستی انجام می شدند.
- مبتنی بر دو روش اصلی جانشینی و جایگشت هستند.



رمزهای کلاسیک

□ جایگشت

- جابجایی بین حروف متن اصلی
- شکست رمز سخت تر.

□ جانشینی

- جانشینی یک حرف با حرف دیگر
- تک الفبایی
- چند الفبایی
- حملات شناخته شده با استفاده از توزیع فرکانسها



ایده‌های تحلیل رمز کلاسیک

حملات Brute Force

■ جستجوی همه حالات (کلیدهای ممکن)

حملات تحلیل فرکانسی

■ فراوانی حروف (etanos...)

■ فراوانی ترکیبات حروف (th, nt)

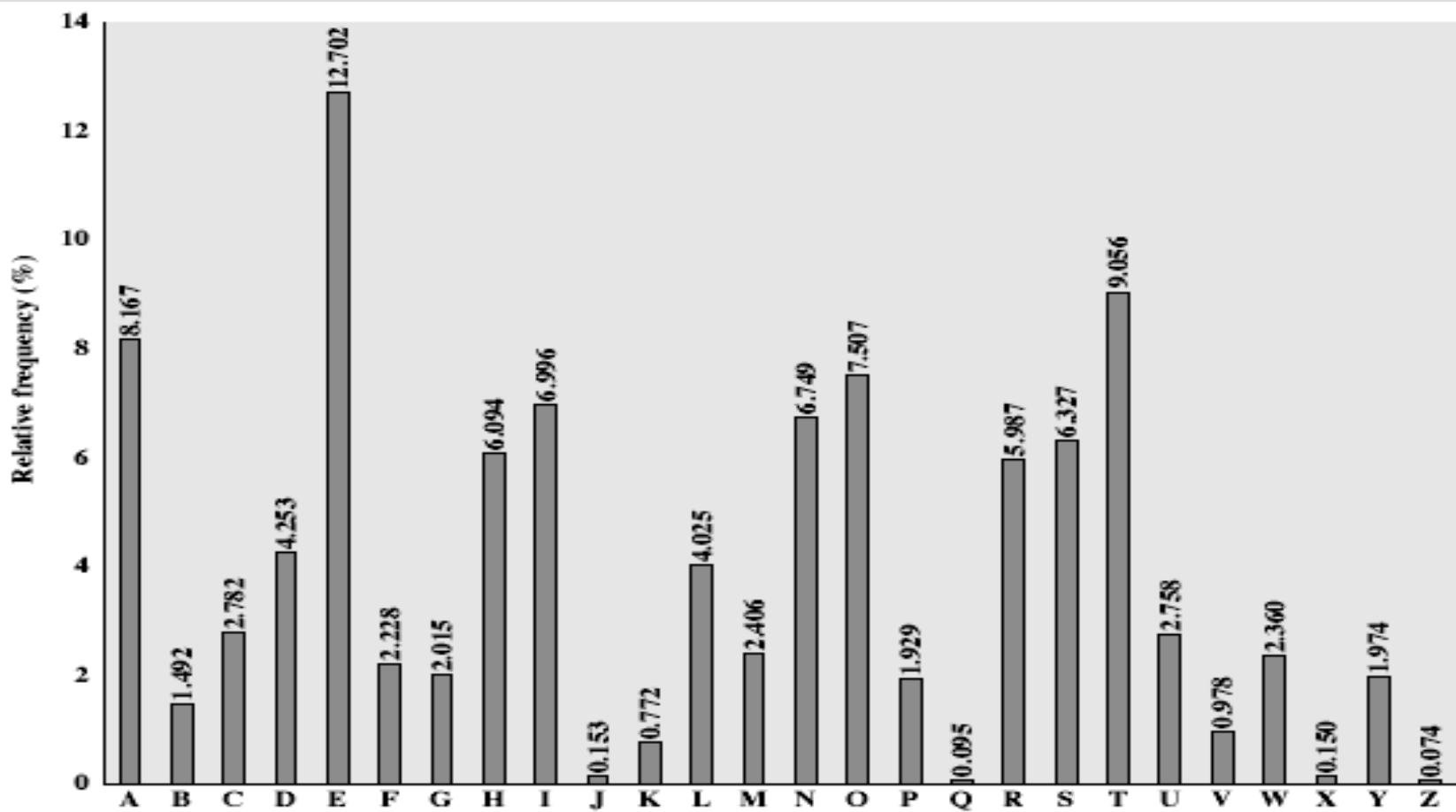
■ حروف ابتدا و انتهای کلمه (th___, ___nt, ___gh)

■ نظم موجود در گرامر زبان



تحلیل فرکانسی

فراوانی حروف انگلیسی در متون





ایده‌های تحلیل رمز کلاسیک

□ **متد Kasiski:** این روش بر مبنای یافتن الگوهای تکراری (عموماً سه حرفی) در متن رمز شده و پیدا کردن طول کلید مورد استفاده استوار است.

■ ایده: فاصله بین دو تکرار از الگوهای تکراری، باید حتماً بر طول کلید مورد استفاده بخش پذیر باشد.

■ **K:** VIGVIGVIGVIGVIG

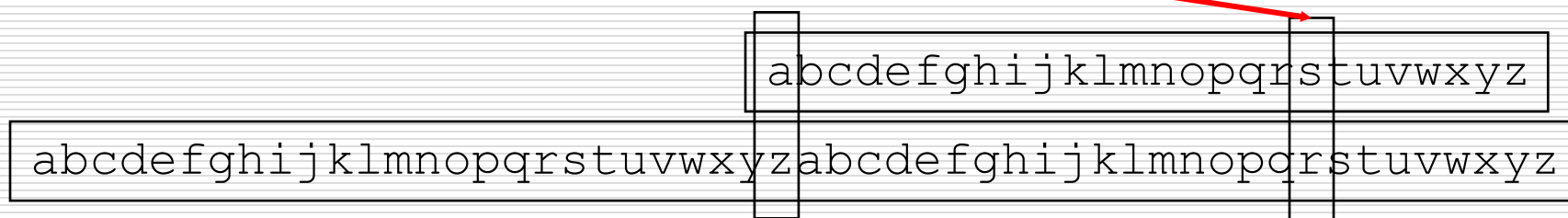
■ **P:** THEBOYHASTHEBAG

■ **C:** OPKWWECIYOPKWIM



رمز جانشینی سزار

send another catapult



$$K = 25$$

$$C = P + K \pmod{26}$$

r

rdmc zmnsqds bzsotks

• تنها از یک فرمول جایگزینی مشابه فرمول فوق استفاده می شود.

خصوصیات

• تنها ۲۵ کلید لازم است کنترل شود.



رمز جانشینی تک الفبایی

• هر حرف با حرف دیگری در الفبا جایگزین می شود.

Plain: a b c d e f g h i j k l m n o p q r s t u v w x y z

Cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

نمونه ها:

- Playfair Cipher
- Hill Cipher



تحلیل رمز جانشینی تک الفبایی

□ حمله Brute-Force

■ تعداد کلیدهای ممکن $26! = 4 \times 10^{26} \Leftarrow$ غیرممکن

□ امکان حمله فرکانسی

■ با مقایسه نمودار فراوانی حروف در متن رمز شده با نمودار استاندارد

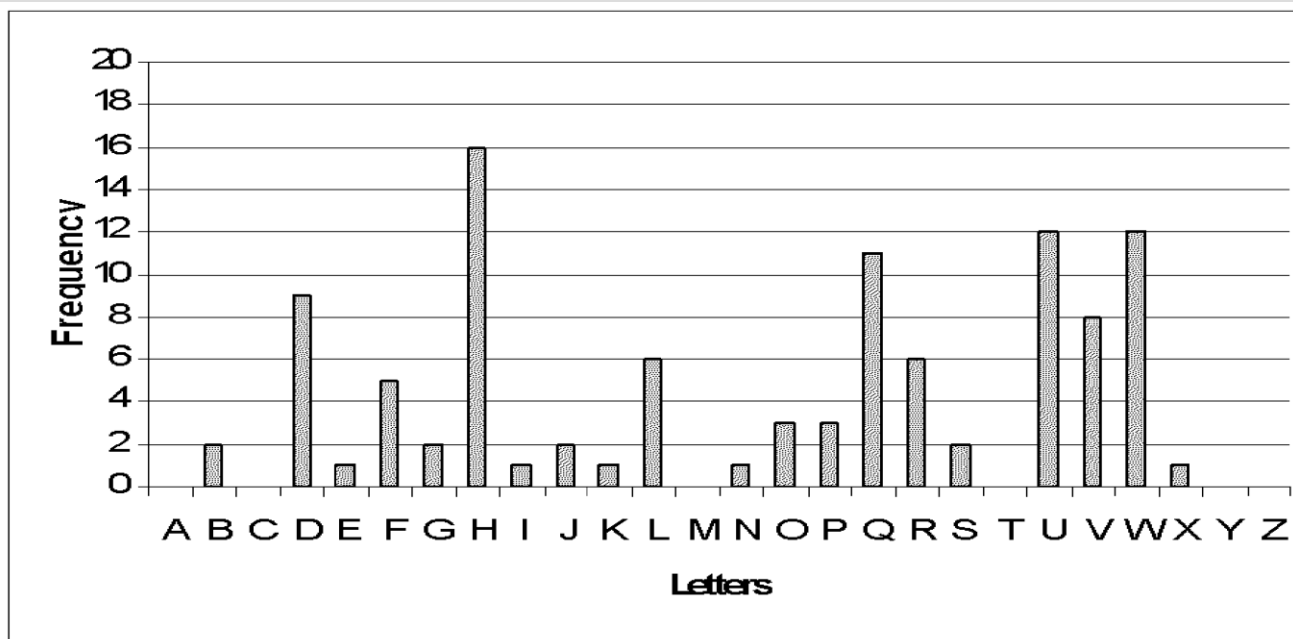
فراوانی حروف، می توان تناظر احتمالی حروف را پیدا کرد.

■ مثال در اسلاید بعد



تحليل رمز جانشینی تک الفبایی (مثال)

DHULDOUHFRQQLVVDQFHUHSRUWVHQHPBUH . . .



فراوانی حروف متن رمز شده (جانشینی تک الفبایی)



رمز جانشینی چندالفبایی

□ خصوصیات

- استفاده از مجموعه‌ای از جانشینی‌های تک الفبایی مختلف بصورت متوالی.
- کلید نمایانگر این است که چه ترتیبی از قواعد جانشینی باید به کار برده شود.
- همچنان می‌توان از فرکانس یا توزیع حروف برای شکست رمز استفاده کرد.

□ نمونه‌ها:

■ جانشینی Vigenere



مثال رمز چندالفبایی: جانشینی ۲۱۳

حروف به ترتیب به
رمزکننده‌های تک الفبایی برای
رمز شدن داده می‌شوند.

Plain: send another catapult

abcdefghijklmnopqrstuvwxyz

abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz

abcdefghijklmnopqrstuvwxyz

abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz

abcdefghijklmnopqrstuvwxyz

abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz

Cipher: ufqf bqqukgs fcudrvov

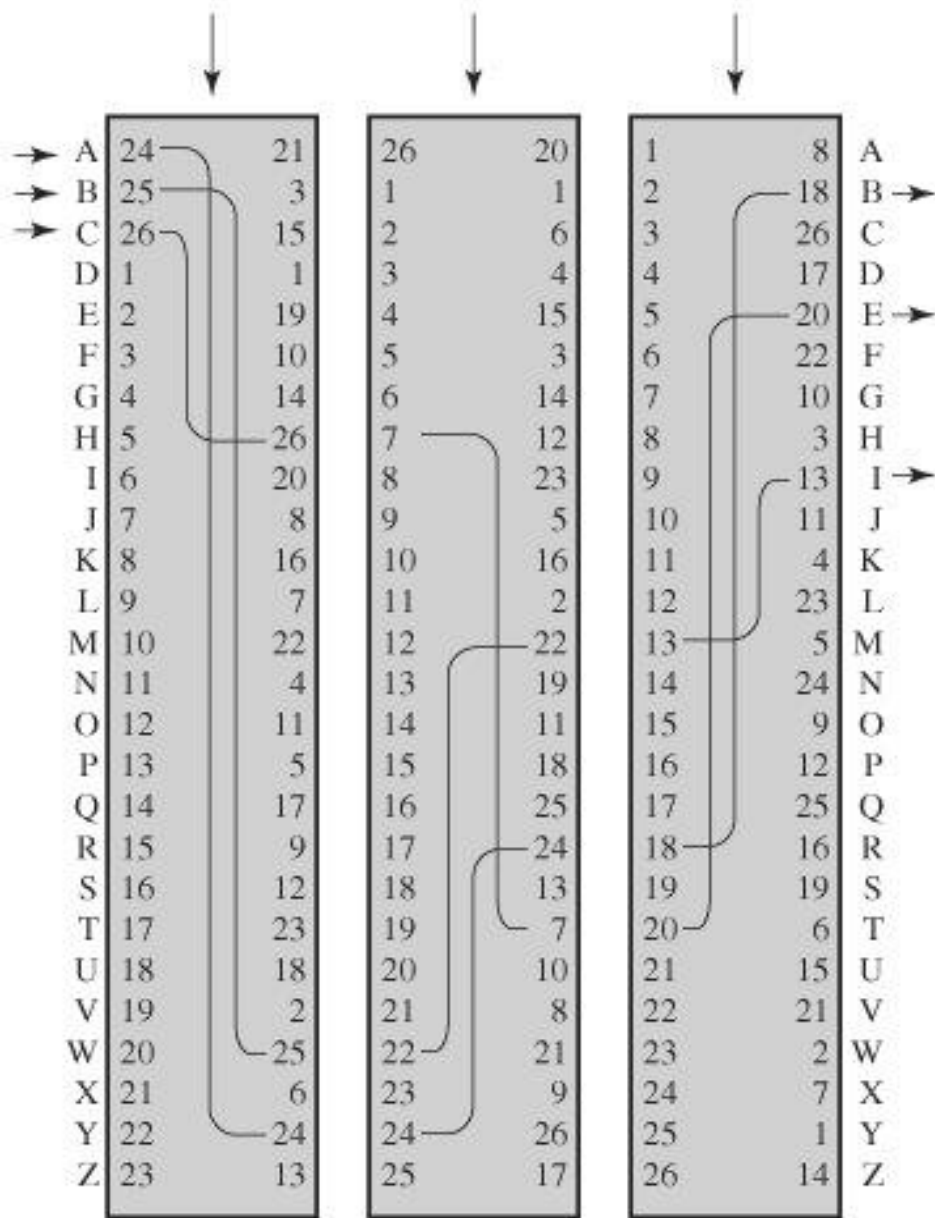
ماشینهای روتور (Rotor Machines)



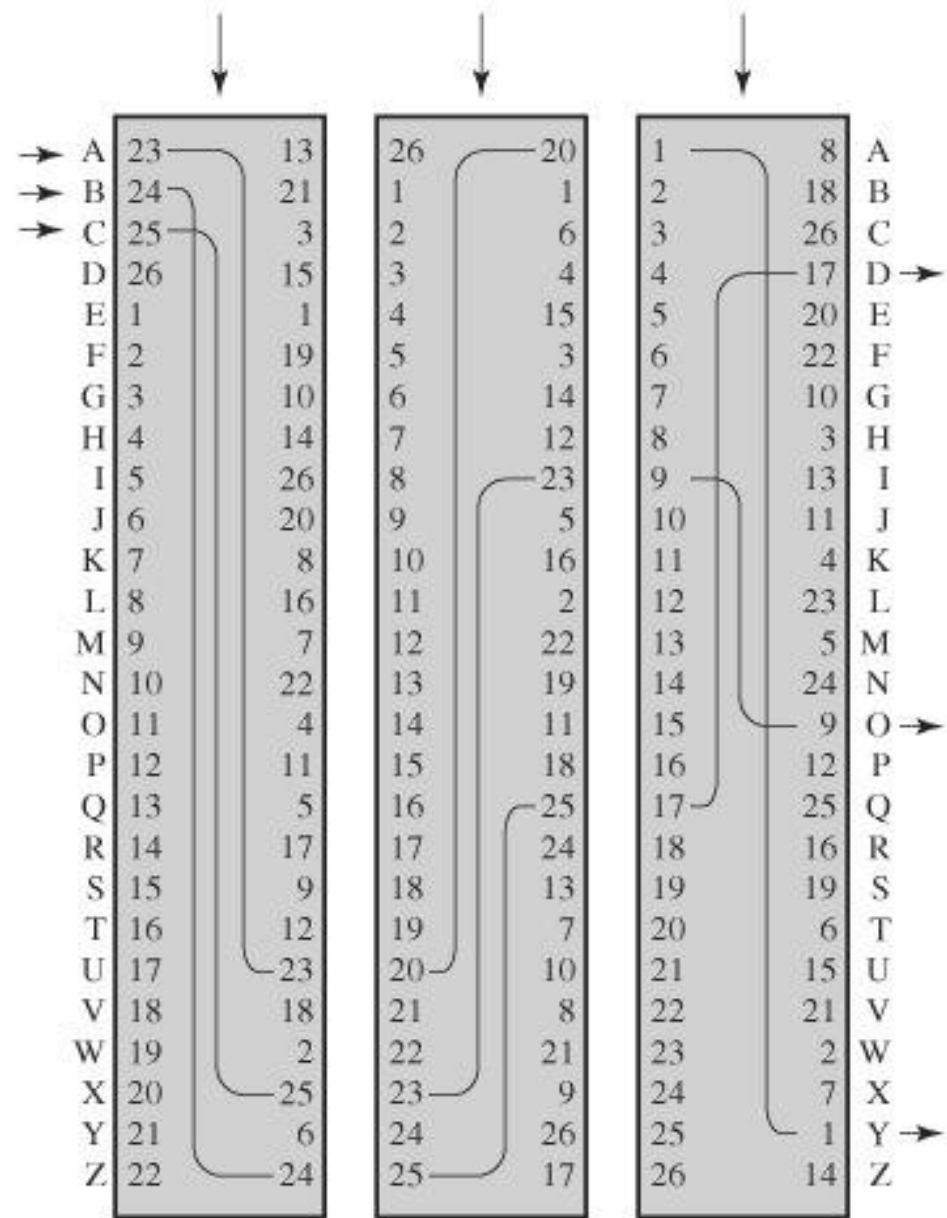
- ماشین روتور یک پیاده‌سازی الکترونیکی-مکانیکی از رمزچندالفبایی محسوب می‌شود.
- در این روش، داده‌ها از داخل تعدادی سیلندر که در مقابل هم قرار گرفته‌اند، عبور می‌کنند. هر سیلندر یک رمز تک الفبایی را انجام می‌دهد.
- به ازای هر حرف از ورودی، سیلندر اول به اندازه یک حرف می‌چرخد با یک دور گردش کامل هر روتور، روتور بعدی به اندازه یک حرف جابجا می‌شود.
- دوره تناوب ماشین روتور با افزایش تعداد روتورها افزایش می‌یابد (26^n).
- آلمان‌ها اعتقاد داشتند که ماشین روتور طراحی شده توسط آنها (با نام Enigma) غیرقابل شکست است، ولی متفقین توانستند رمز آن را کشف کنند و بسیاری از اطلاعات سری آنها را فاش کنند.

Direction of motion

Direction of motion

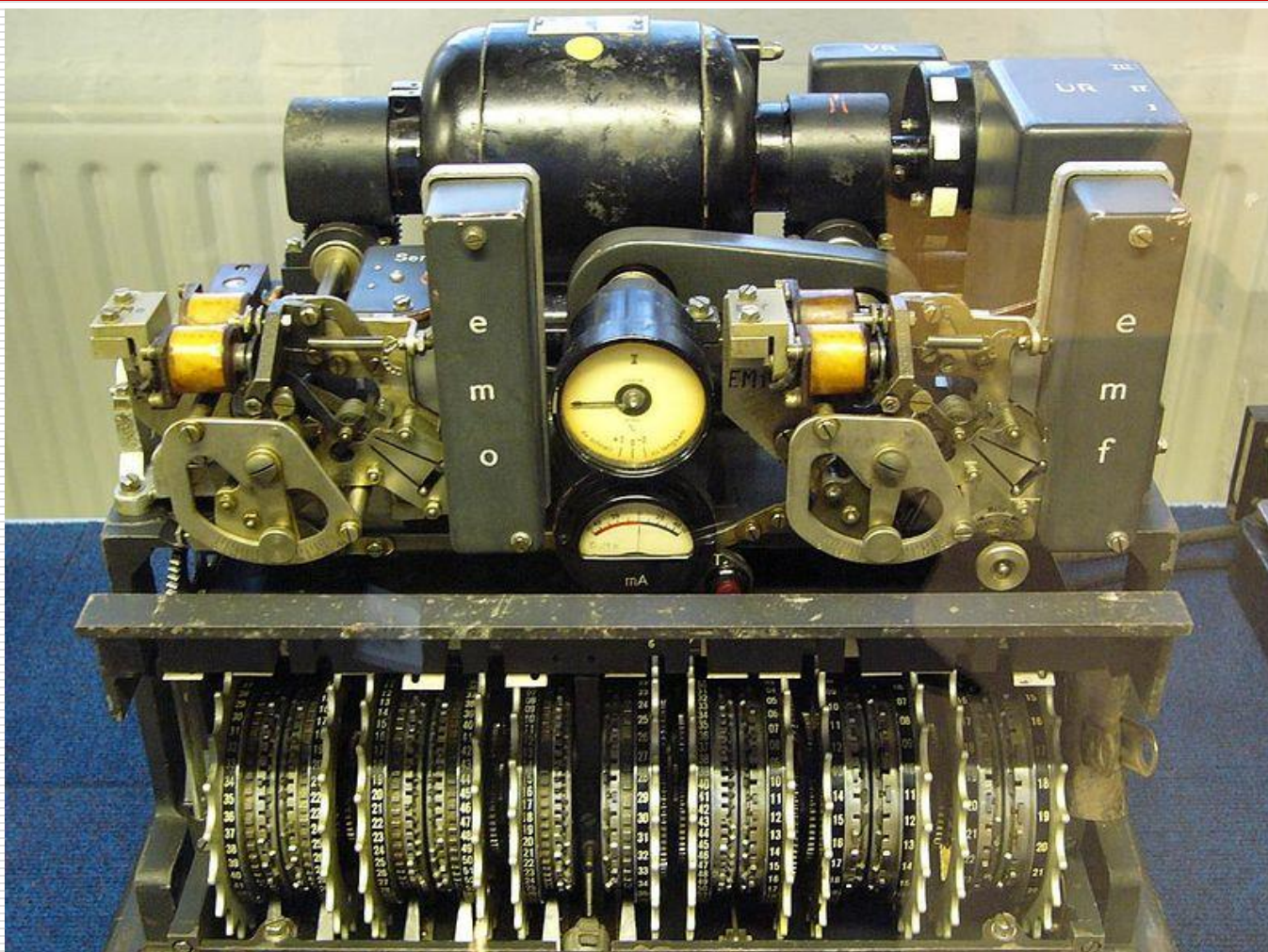


(a) Initial setting



(b) Setting after one keystroke

ماشینهای روتور





رمز One-Time Pad

□ اگر از کلید **کاملاً تصادفی** به اندازه متن آشکار استفاده شود، رمز حاصله امن خواهد بود.

□ این نوع کلید Pad نام دارد.

□ در One-Time Pad از هر کلید فقط یک بار می‌شود استفاده کرد.

□ رمزگذاری: $C_i = P_i \oplus K_i$

\oplus means XOR

□ رمزگشایی: $P_i = C_i \oplus K_i$



تحلیل رمز One-Time Pad

- این رمز، از **امنیت مطلق** برخوردار است، چرا که هیچ رابطه‌ای بین متن آشکار و متن رمز شده وجود ندارد.
- یعنی می‌توان بین هر متن آشکار و هر متن رمز شده، یک کلید رمز متناظر پیدا کرد.
- **مشکل این روش:**
 - تولید کلید تصادفی به تعداد زیاد
 - توزیع کلید (نیاز به ارسال کلید برای هر متن به اندازه خود آن)



فهرست مطالب

□ تعاریف

□ نیازمندی‌های رمزنگاری

□ رمز کلاسیک - جانشینی

□ رمز کلاسیک - جایگشت



رمز جایگشتی

□ جابجایی حروف در متن اصلی بدون تغییر حروف الفبا

□ امکان استفاده ترکیبی از آن با رمز جانشینی

■ ایده اصلی مورد استفاده در رمزنگاری متقارن مدرن



رمز جایگشت ستونی

- متن را بصورت سطری بنویسیم و بصورت ستونی بخوانیم.
- کلید: تعداد ستون‌ها (در اینجا 5)

43125

SEND*

ANOTH

ER*SE

T****

SAETENR*NO**DTS**HE*

- کلید: ترتیب نوشتن ستون‌ها (در اینجا 43125)

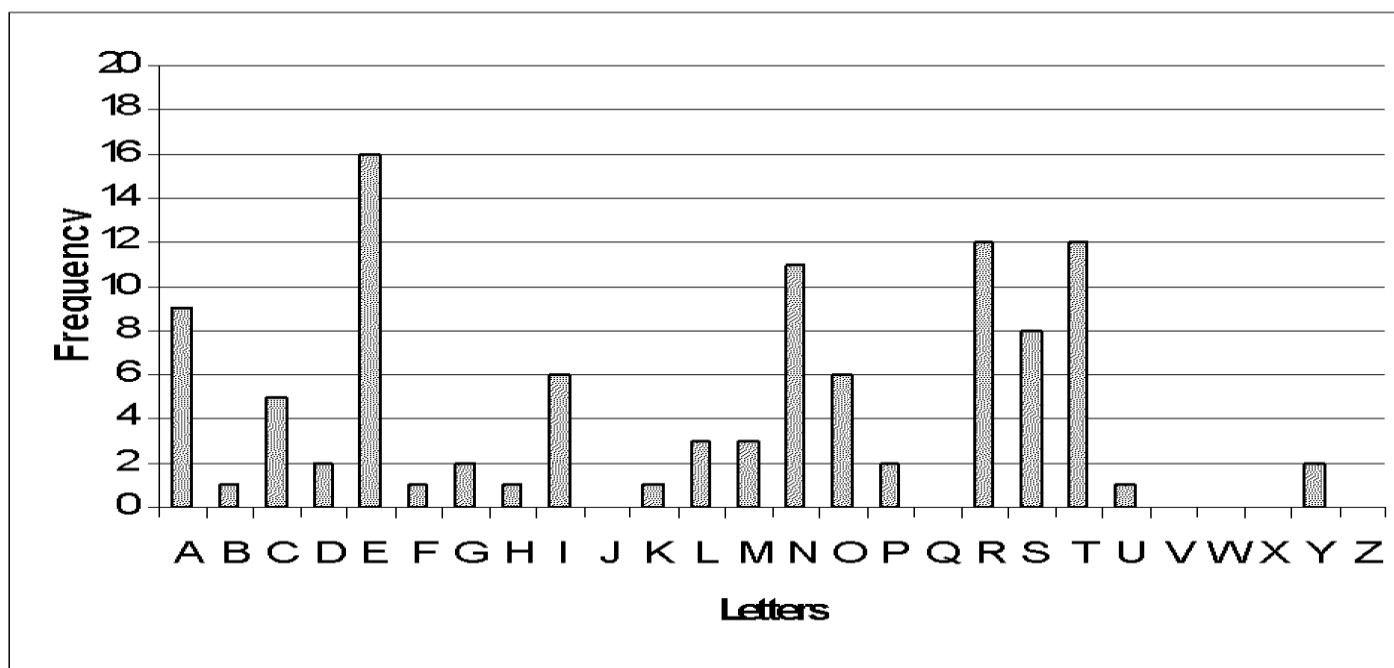
NO**DTS*ENR*SAET*HE*

- می‌توان برای امنیت بیشتر چند بار جایگشت را انجام داد.



تحليل رمز جايجشتى

Aerial reconnaissance reports enemy reinforcements estimated at battalion strength entering your sector PD Clarke



فراوانی حروف متن اصلی



تحلیل رمز جایگشتی (مثال)

aerialreco
nnaissance
reportsene
myreinforc
ementsesti
matedatbat
talionstre
ngthenteri
ngyoursect
orPDClarke

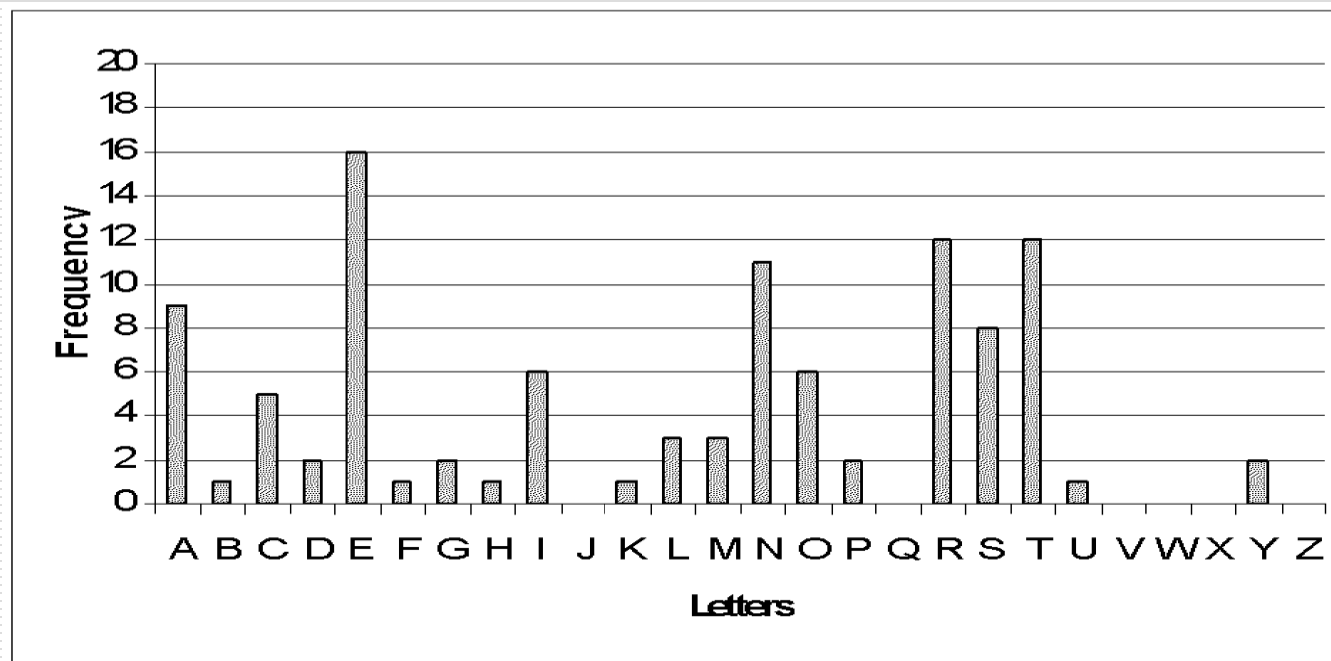


ANRMEMTNNO
ENEYMAAGGR
RAPRETLTYP
IIOENEIHOD
ASRITDOEUC
LSTNSANNRL
RASFETSTSS
ENEOSBTEER
CCNRTARRCK
OEECITEITE



تحليل رمز جايجشتي (مثال)

ANRMEMTNNOENEYMAAGGRRAPRETLTYPIIOENE
IHODASRITDOEUCLSTNSANNRLRASFETSTSSSEN
EOSBTEERC CNRTARRCKOEECITEITE



فراوانی حروف متن رمز شده



تحلیل رمز جایگشتی

□ از مقایسه نمودارهای قبلی می توان فهمید در رمز جایگشتی:

■ فراوانی حروف در متن رمز شده تفاوتی با فراوانی متن اصلی ندارد.

■ تحلیلگر نمی تواند از نمودارهای فراوانی استفاده کند.



پایان

مرکز امنیت داده و شبکه شریف

<http://dnsl.ce.sharif.edu>

پست الکترونیکی

amini@sharif.edu