یا ذاالامن والامان

مفاهیم رمزنگاری و رمزنگاری کلاسیک

مبانی امنیت اطلاعات و شبکه‌های کامپیوتری

محمدرضا رازیان*

بهار و تابستان ۱۳۹۵

مرکز تخصصی آپا

دانشگاه سمنان

مرکز تخصصی آپا دانشگاه سمنان

http://cert.semnan.ac.ir

آزمایشگاه امنیت داده و شبکه شریف

http://dnsl.ce.sharif.ir

*Homepage: www.mrazian.com

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:** اطلاعی که در رمز مورداستفاده 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

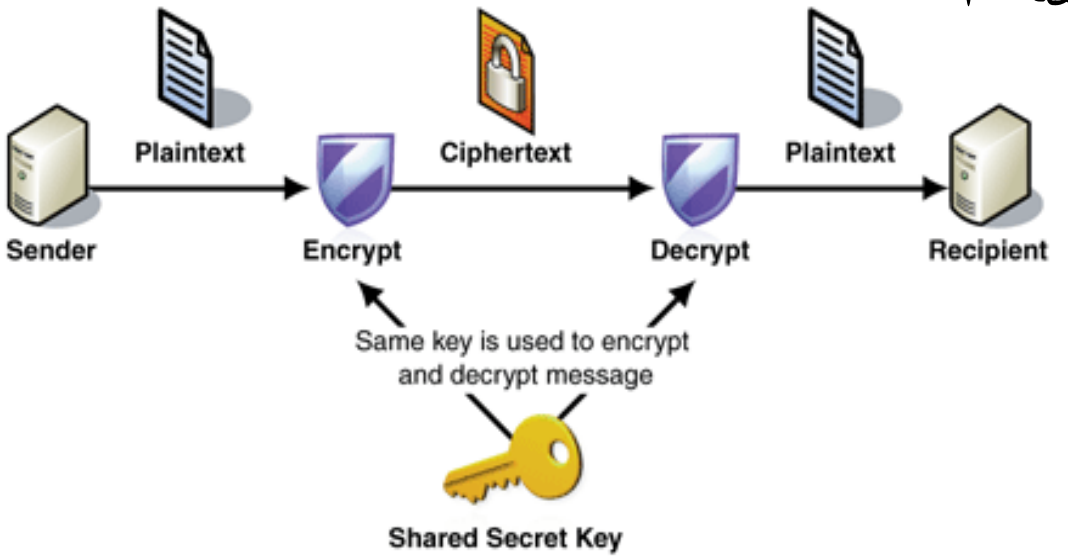
- **Cryptography:** study of encryption principles/methods
  - **رمزنویسی:** علم اصول و روش‌های رمزگذاری
- **Cryptanalysis (codebreaking):** the study of principles/ methods of deciphering ciphertext *without* knowing key
  - **تحلیل رمز:** علم اصول و روش‌های رمزگشایی متن رمز بدون اطلاع از کلید
- **Cryptology:** the field of both cryptography and cryptanalysis
  - **رمزنگاری:** علم حاصل از ترکیب رمزنویسی و تحلیل رمز

رمزنگاری

- رمزنگاری یکی از روش‌های دستیابی به محرمانگی داده‌ها است.
- الگوریتم‌های رمزنگاری متفاوتی وجود دارند که
  - از دیدگاه تعداد کلید به دو دسته تقسیم می شوند
    - رمزنگاری متقارن
    - رمزنگاری نامتقارن (که به رمزنگاری با کلید عمومی نیز شهرت دارد)

رمزنگاری متقارن (Symmetric)

- معادل با رمزنگاری معمولی/ رمزنگاری کلید خصوصی/ رمزنگاری تک‌کلیدی
- فرستنده و گیرنده از یک کلید مشترک استفاده می‌کنند.
- تمام رمزنگاری‌های کلاسیک از نوع متقارن هستند.
- تنها نوع رمزنگاری تا قبل از دهه ۷۰



فهرست مطالب

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.

$$Y = \mathrm{E}_K(X)$$
$$X = \mathrm{D}_K(Y)$$

- فرض بر آن است که الگوریتم برای همه مشخص است.
- بنابراین نیاز به یک کانال امن برای توزیع کلید است.

ابعاد رمزنگاری

- **اَعمال مورد استفاده برای رمزگذاری**
  - جایگزینی (Substitution): جایگزینی هر عنصر با عنصری دیگر
  - جایگشت (Transposition): جابجایی عناصر رمزشده
- **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 می‌شوند.
  - جریانی: عناصر متن به طور پیوسته به ورودی داده شده و در هر لحظه یک عنصر رمز شده خارج می‌شود.

حملات تحلیل رمزنگاری

- **هدف از حمله:**
  - استخراج کلید
  - استخراج متن آشکار از متن رمزشده

- **نحوه حمله:**
  - بررسی خصوصیات الگوریتم رمز
  - بررسی مجموعه‌ای از متن‌های آشکار و رمزشده آنها

انواع حملات تحلیل رمزنگاری

نوع حمله	اطلاعات در اختیار تحلیلگر رمز
ciphertext only	•الگوریتم رمز •متن رمز
known plaintext	•الگوریتم رمز •متن رمز •یک یا چند جفت متن آشکار و رمز شده آن
chosen plaintext	•الگوریتم رمز •متن رمز •متن آشکار انتخاب شده توسط تحلیلگر و متن رمز معادل آن
chosen ciphertext	•الگوریتم رمز •متن رمز •متن رمز انتخاب شده توسط تحلیلگر و متن آشکار حاصل از رمزگشایی آن
chosen text	•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

جستجوی تمام حالات
(Brute Force Search)

- ابتدایی‌ترین حمله
- فرض بر این است که متن آشکار قابل شناسایی است.

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

رمزهای کلاسیک

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

رمزهای کلاسیک

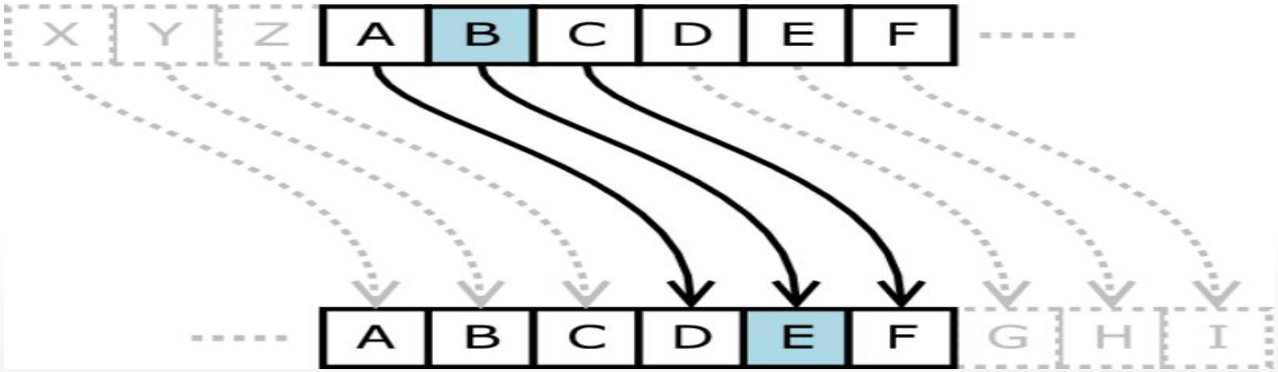
- **جانشینی (substitution)**
  - تک حرفی: جانشینی یک حرف با حرف دیگر
    - تک الفبایی مثل سزار
    - چند الفبایی مثل ویجینیر
  - چند حرفی: مثال Playfair Cipher، Hill Cipher
    - حملات شناخته شده با استفاده از توزیع فرکانس‌ها
- **جایگشت (جابه‌جایی) transposition**
  - جابجایی بین حروف متن اصلی (ترتیب حروف اصلی را به هم می زنیم بدون تغییر حروف اصلی) شکست رمز سخت‌تر.

رمز سزار (Caesar)

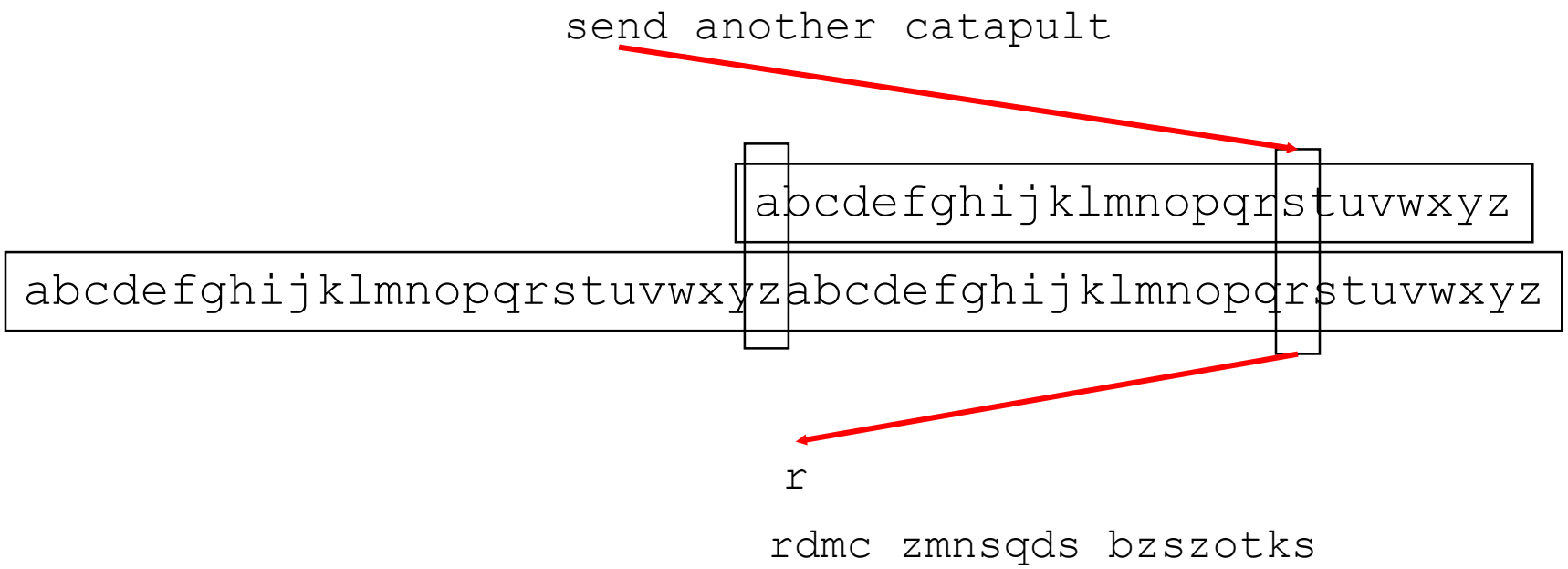
- یکی از اولین سیستم های رمزنگاری سزار است. هر حرف با ۳ حرف بعد خود جانشین

- $C = E(3, p) = (p + 3) \bmod 26$

- plain: meet me after the toga party
- cipher: PHHW PH DIWHU WKH WRJD SDUWB



الگوریتم سزار کلی



خصوصیات

- تنها از یک فرمول جایگزینی مشابه فرمول فوق استفاده می‌شود.
- تنها ۲۵ کلید لازم است کنترل شود.

Let us assign a numerical equivalent to each letter:

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

Then the algorithm can be expressed as follows. For each plaintext letter p, substitute the ciphertext letter C:[2]

$$C = \mathrm{E}(3, p) = (p + 3) \bmod 26$$

A shift may be of any amount, so that the general Caesar algorithm is

$$C = \mathrm{E}(k, p) = (p + k) \bmod 26 \qquad \textbf{(2.1)}$$

where k takes on a value in the range 1 to 25. The decryption algorithm is simply

$$p = \mathrm{D}(k, C) = (C - k) \bmod 26 \qquad \textbf{(2.2)}$$

[1]When letters are involved, the following conventions are used in this book. Plaintext is always in lowercase; ciphertext is in uppercase; key values are in italicized lowercase.

[2]We define a mod n to be the remainder when a is divided by n. For example, 11 mod 7 = 4. See Chapter 4 for a further discussion of modular arithmetic.

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

جستجوی همه حالات (کلیدهای ممکن)

- شکستن الگوریتم سزار کلی

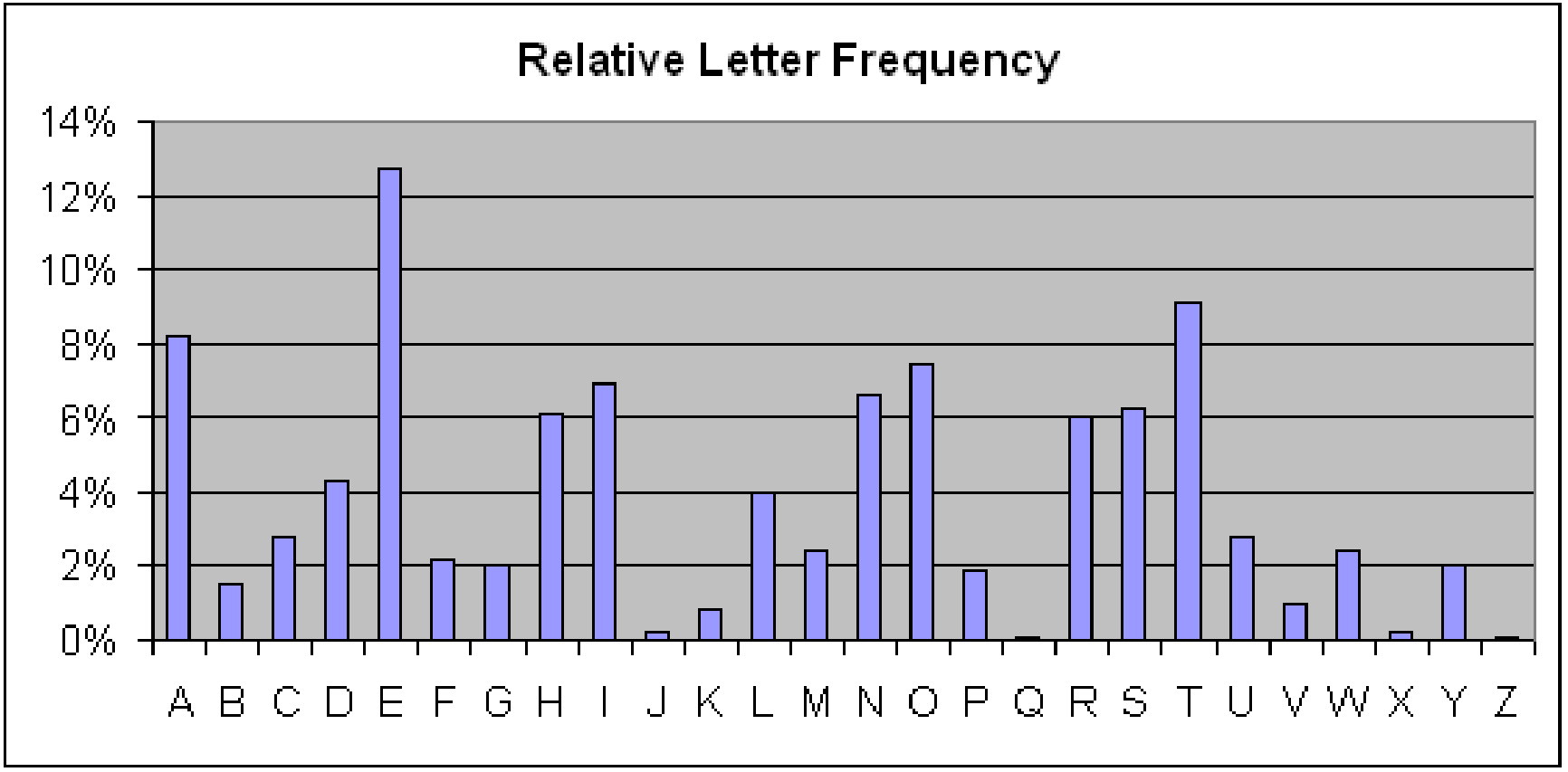
- BPM VMOWBQIBQWVA NWZ I AMBBTMUMVB WN BPM ABZQSMIZM IB IV QUXIAAM ZMKWUUMVL EM QVKZMIAM WCZ WNNMZ

(B,P,M)->(1,15,12)
K = 1 -> (0,14,11) ->(A,O,L)

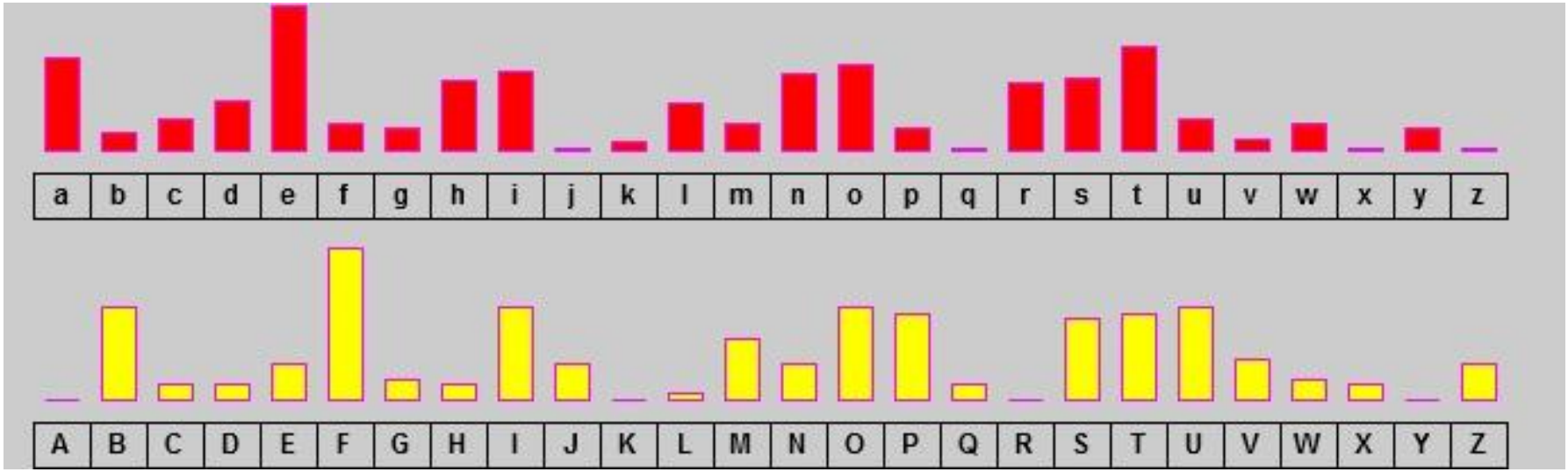
Subtract	Get			Corresponding to letters		
1	1	15	12	A	O	L
2	26	14	11	Z	N	K
3	25	13	10	Y	M	J
4	24	12	9	X	L	I
5	23	11	8	W	K	H
6	22	10	7	V	J	G
7	21	9	6	U	I	F
8	20	8	5	T	H	E

تحلیل فرکانسی

فراوانی حروف انگلیسی در متون



جدول فرکانسی و شیفت‌یافته آن



رمز جانشینی تک الفبایی کلی

- 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

امنیت رمز تک الفبایی

- در حال حاضر تعداد کل کلیدها به صورت زیر است
- $26! = 4 \times 10^{26}$
- با این تعداد زیاد کلید به نظر امن می‌آید.
- اما این نظر اشتباه است
- مسئله ویژگی‌های زبان است.

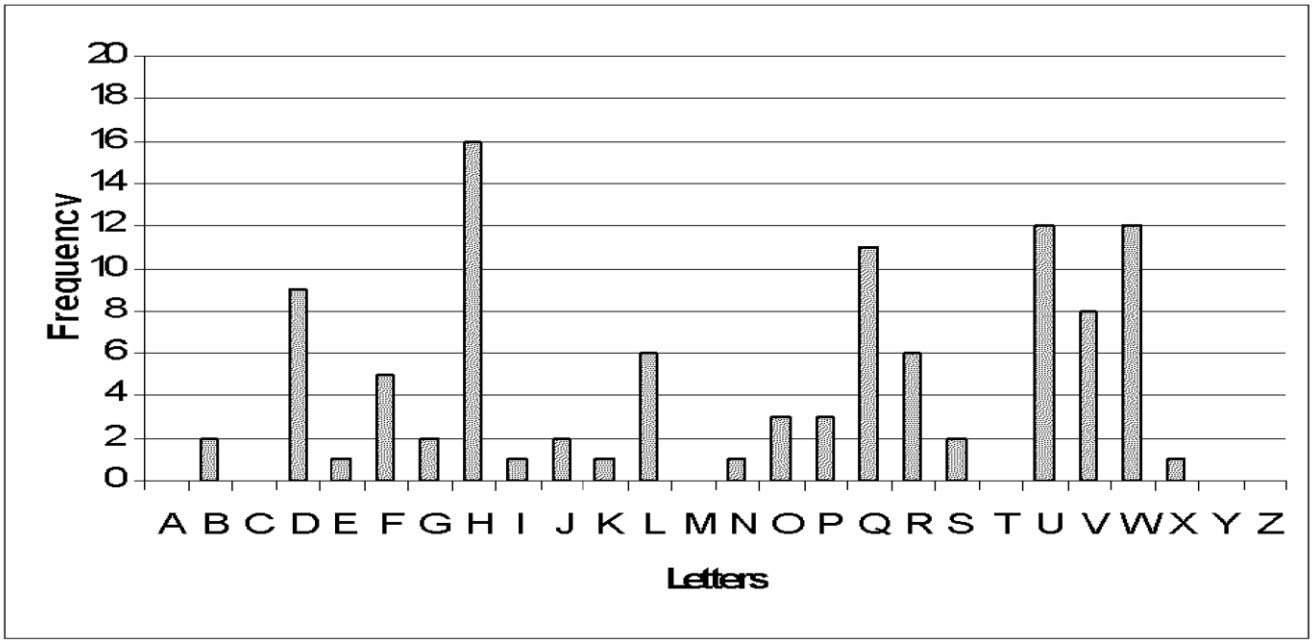
تحلیل رمز جانشینی تک الفبایی کلی

- **حمله Brute-Force**
  - تعداد کلیدهای ممکن ۴×۱۰^{۲۶} = !۲۶ ⇐ غیرممکن

- **امکان حمله فرکانسی**
  - با مقایسه نمودار فراوانی حروف در متن رمز شده با نمودار استاندارد فراوانی حروف، می‌توان تناظر احتمالی حروف را پیدا کرد.
  - مثال در اسلاید بعد

تحلیل تحلیل رمز جانشینی تک الفبایی کلی (مثال)

DHULDOUHFRQQLVVDQFHUHSRUWVHQHPBUH . . .



فراوانی حروف متن رمزشده (جانشینی تک الفبایی)

رمز Playfair

- تعداد زیاد کلید در رمز تک الفبایی کمکی به فراهم کردن امنیت نکرد
- یک رویکرد برای بهبود امنیت، رمز کردن چند حرف بود
- رمز Playfair یک مثال از این نوع رمز است

رمز Playfair

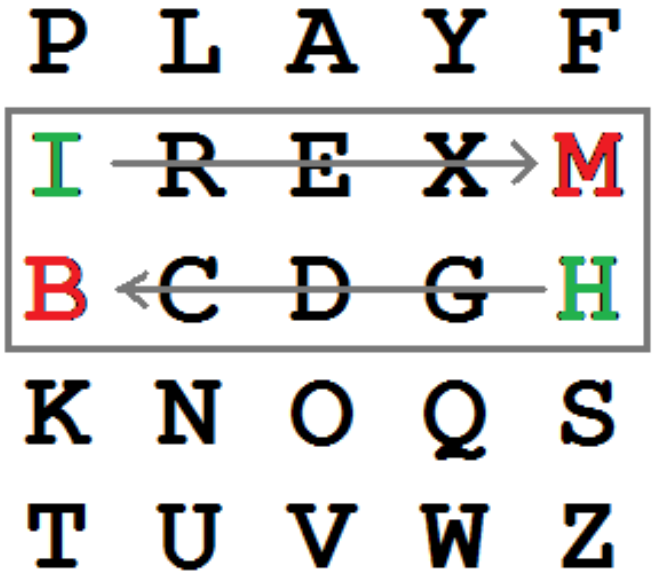
- در این روش ۲۵ حرف از حروف زبان انگلیسی (به استثنا j) در یک جدول ۵*۵ به طور تصادفی درج می‌گردد.

- a 5*5 matrix of letters based on a keyword
- fill in letters of keyword (sans duplicates)
- fill rest of matrix with other letters
- eg. using the keyword MONARCHY

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

رمز Playfair

- **Plaintext is encrypted two letters at a time**
  - if a pair is a repeated letter, insert filler like 'X’
  - if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
  - if both letters fall in the same column, replace each with the letter below it (wrapping to top from bottom)
  - otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair
- **Security much improved over monoalphabetic since have 26 x 26 = 676 diagrams. would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic)**



HI

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

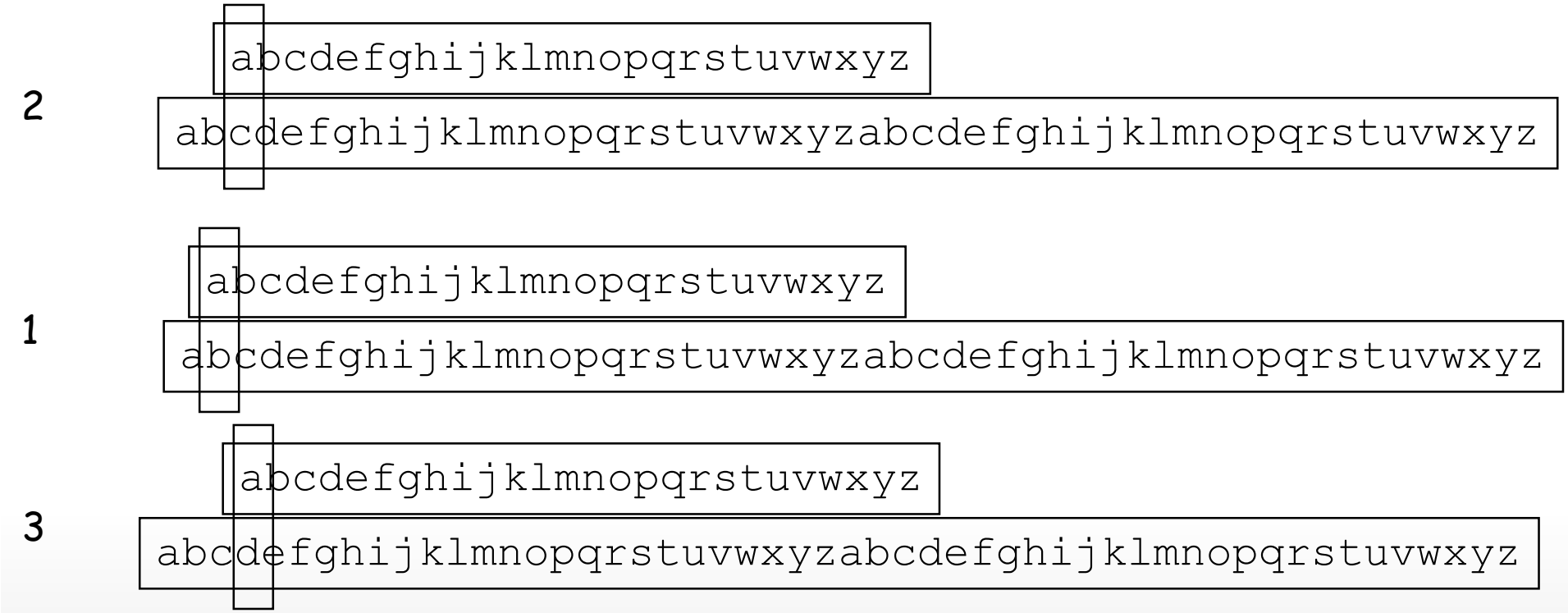
BM

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 توزیع حروف برای شکست رمز استفاده کرد.
- نمونه‌ها:
  - جانشینی Vigenere

مثال رمز چندالفبایی: جانشینی ۲۱۳

Plain: **send another catapult**



Cipher: **ufqf bqqukgs fcudrvov**

رمز Vigenère

- نوعی رمز جانشینی تک حرفی چند الفبایی محسوب می‌شود.
- از یک ماتریس ۲۶ در ۲۶ و یک کلید برای رمزگذاری متن استفاده می‌شود.
- حروف متوالی کلید، سطر ماتریس و حروف متوالی متن، ستون ماتریس را مشخص می‌کنند.
- کلید معمولا یک کلمه چندحرفی است که تکرار می‌شود.
- برای رمزگذاری و رمزگشایی از تابلوی رمز Vigenere می‌توان استفاده نمود.

جدول ویژنر Vigenere

Key \ Plaintext	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
a	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
b	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	A
c	C	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
d	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
e	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	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

جدول ویژنر Vigenere

رمز Vigenère

- **رمزگذاری:**

ستون = حرف موردنظر

سطر = حرف کلید

محل تقاطع = رمزشده حرف موردنظر

- **رمزگشایی:**

سطر= حرف کلید

محل تقاطع = حرف رمز شده

ستون = حرف رمزگشایی شده

P= SEND ANOTHER CATAPULT
K= hail caeserh ailcaese
C= ZEVO CNSLLVY CIECPYDX

تحلیل رمز Vigenère

- برای هر حرف، جانشینی‌های مختلفی را به کار می‌برد.
- با جانشینی‌های مختلف، تحلیل فرکانسی را مشکل می‌کند، ولی کاملا غیرممکن نمی‌کند.
- ابتدا باید مشخص کرد که جانشینی تک الفبایی است یا نه.
  - با تحلیل فرکانس حروف به سادگی این مساله مشخص می‌شود.
- در صورت استفاده از Vigenere می‌توان از روش Kasiski طول کلید را به دست آورد.
- گسترش کلید به اندازه متن آشکار (با ترکیب کلید با متن) هم مشکل را حل نمی‌کند.
  - خصوصیات توزیع حروف در کلید حاصله مشکل آفرین است.

ایده‌های تحلیل رمز کلاسیک

- **روش Kasiski:** این روش بر مبنای یافتن الگوهای تکراری (عموماً سه حرفی) در متن رمزشده و پیدا کردن طول کلید مورداستفاده استوار است.

- ایده : فاصله بین دو تکرار از الگوهای تکراری، باید حتما بر طول کلید مورد استفاده بخش‌پذیر باشد.

- **K:** VIGVIGVIGVIGVIG
- **P:** THEBOYHASTHEBAG
- **C:** OPKWWECIYOPKWIM

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 مورداستفاده در رمزنگاری متقارن مدرن

رمز جایگشت ستونی

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

SAETENR*NO**DTS**HE*

- کلید: ترتیب نوشتن ستون‌ها (در اینجا 43125)

NO**DTS*ENR*SAET*HE*

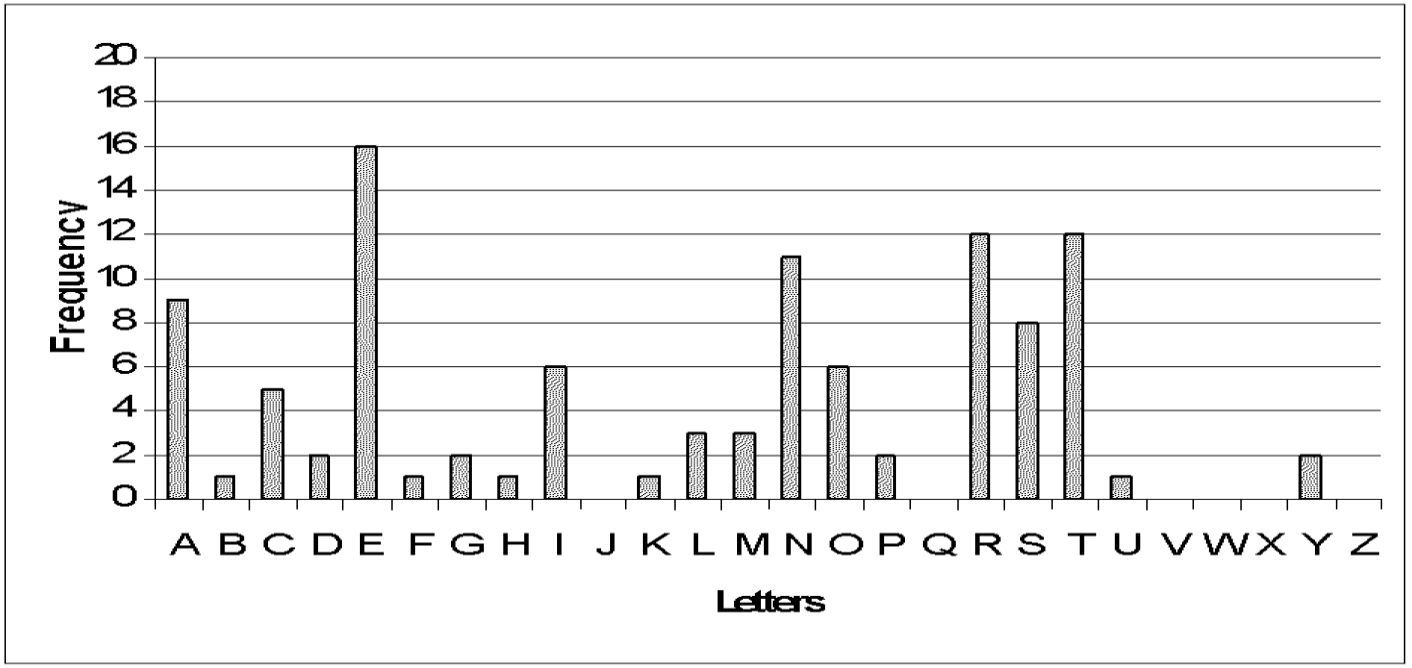
43125

SEND*
ANOTH
ER*SE
T****

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

تحلیل رمز جایگشتی

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

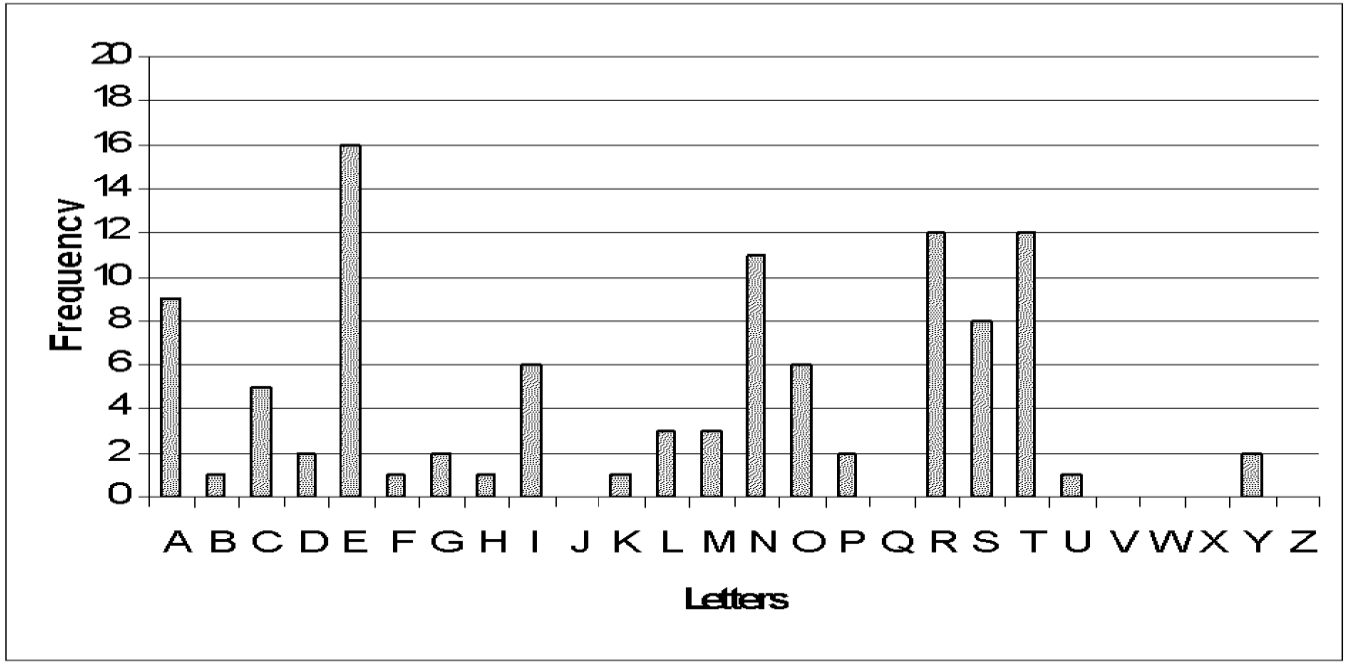


تحلیل رمز جایگشتی (مثال)

aerialreco	ANRMEMTNNO
nnaissance	ENEYMAAGGR
reportsene	RAPRETLTYP
myreinforc	IIOENEIHOD
ementsesti	ASRITDOEUC
matedatbat	LSTNSANNRL
talionstre	RASFETSTSS
ngthenteri	ENEOSBTEER
ngyoursect	CCNRTARRCK
orPDClarke	OEECITEITE

تحلیل رمز جایگشتی (مثال)

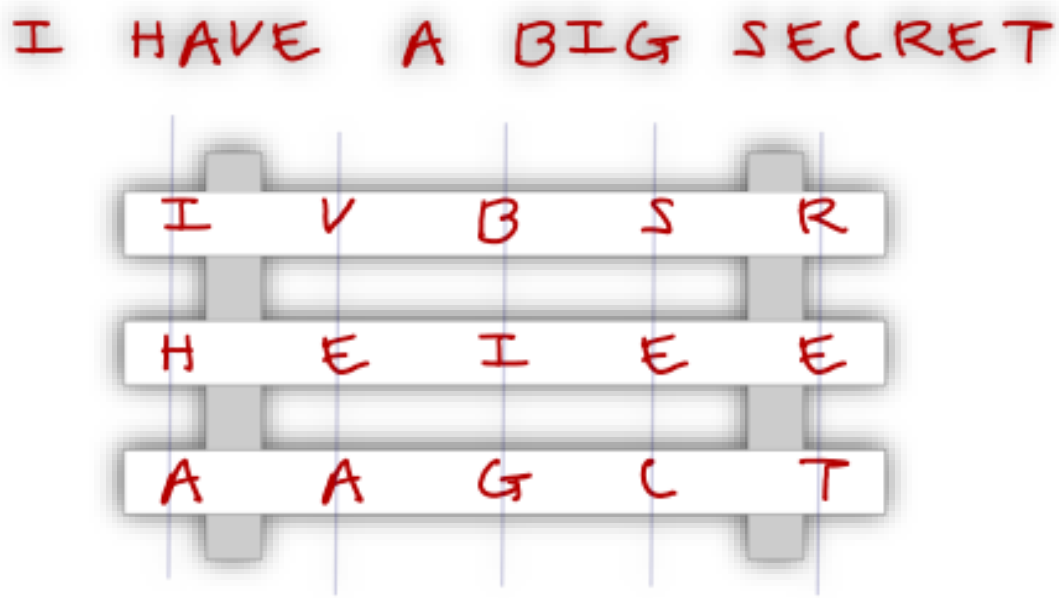
ANRMEMTNNOENEYMAAGGRRAPRETLTYPIIOENE
IHODASRITDOEUCLSTNSANNRLRASFETSTSSEN
EOSBTEERCCNRTARRCKOEECITEITE



تحلیل رمز جایگشتی

- از مقایسه نمودارهای قبلی می‌توان فهمید در رمز جایگشتی:
- فراوانی حروف در متن رمزشده تفاوتی با فراوانی متن اصلی ندارد.
- تحلیلگر نمی‌تواند از نمودارهای فراوانی استفاده کند.

روش Rail Fence



IVBSR HEIEE AAGCT

Vernam Cipher

- ultimate defense is to use a key as long as the plaintext
- with no statistical relationship to it
- invented by AT&T engineer Gilbert Vernam in 1918
- originally proposed using a very long but eventually repeating key

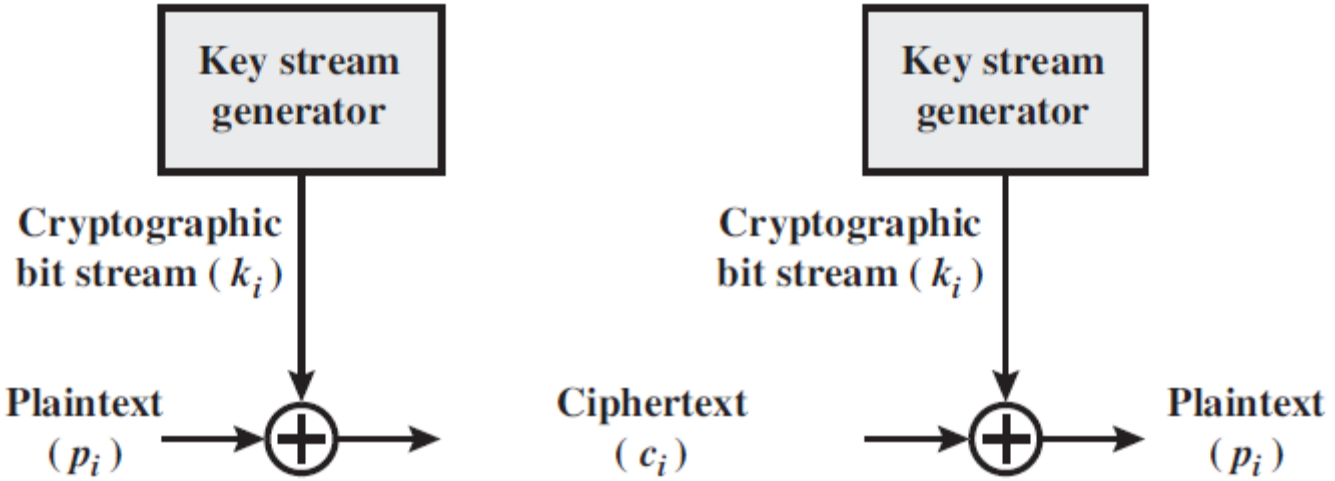


Figure 2.7 Vernam Cipher

رمز One-Time Pad

- اگر از کلید کاملا 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: $P_i = C_i \oplus K_i$

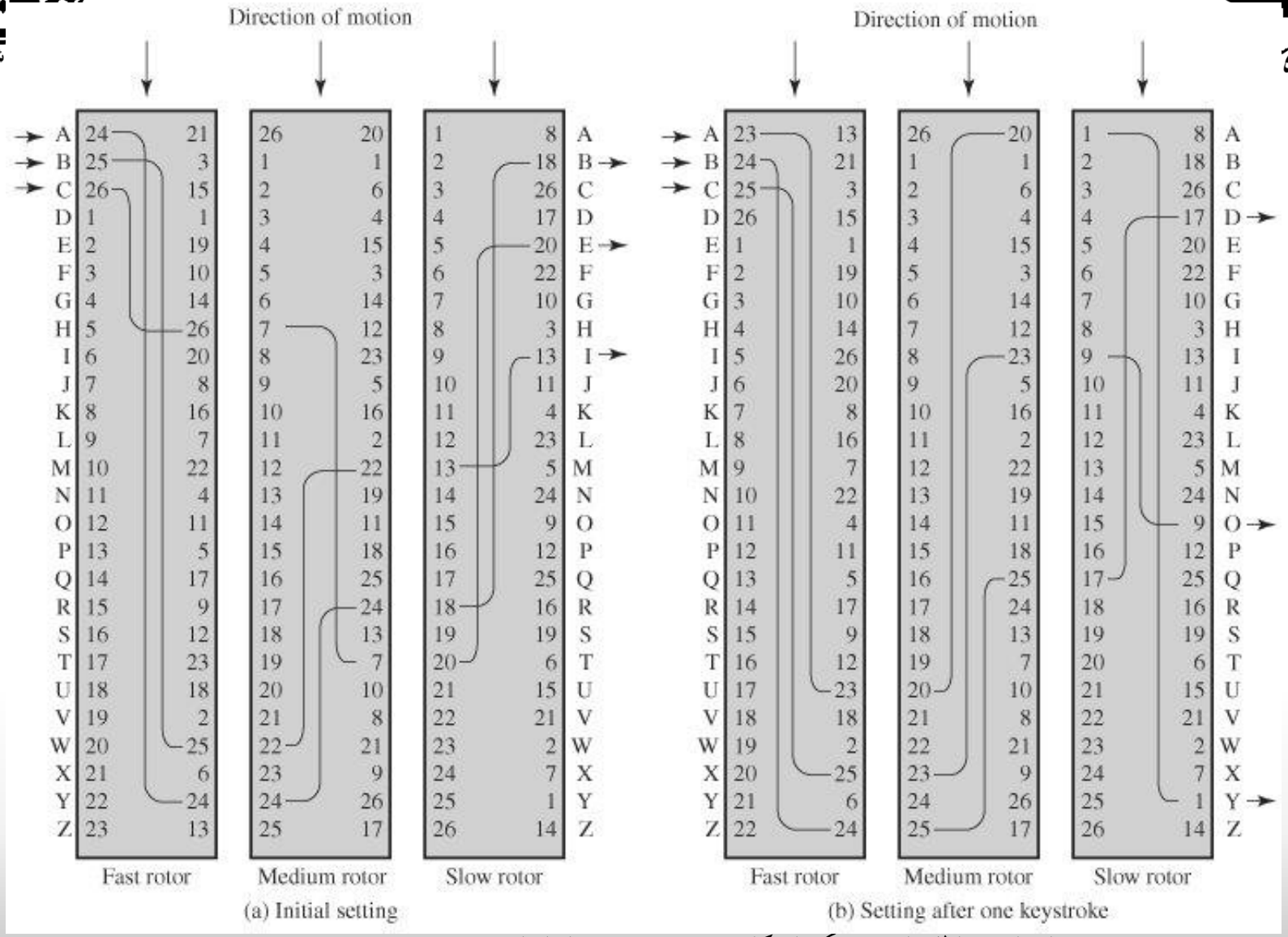
تحلیل رمز One-Time Pad

- 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)

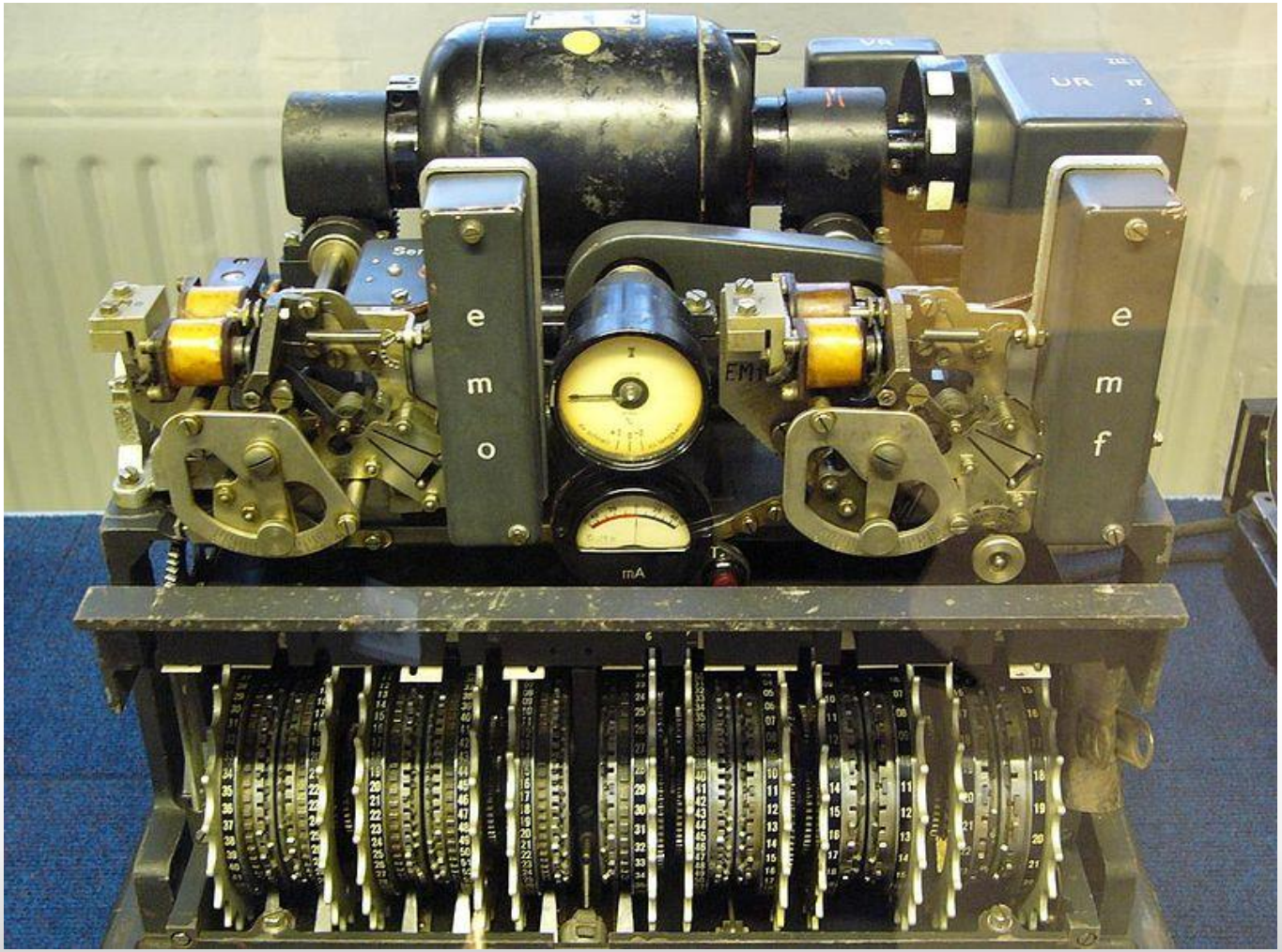
ماشینهای روتور
(Rotor Machines)

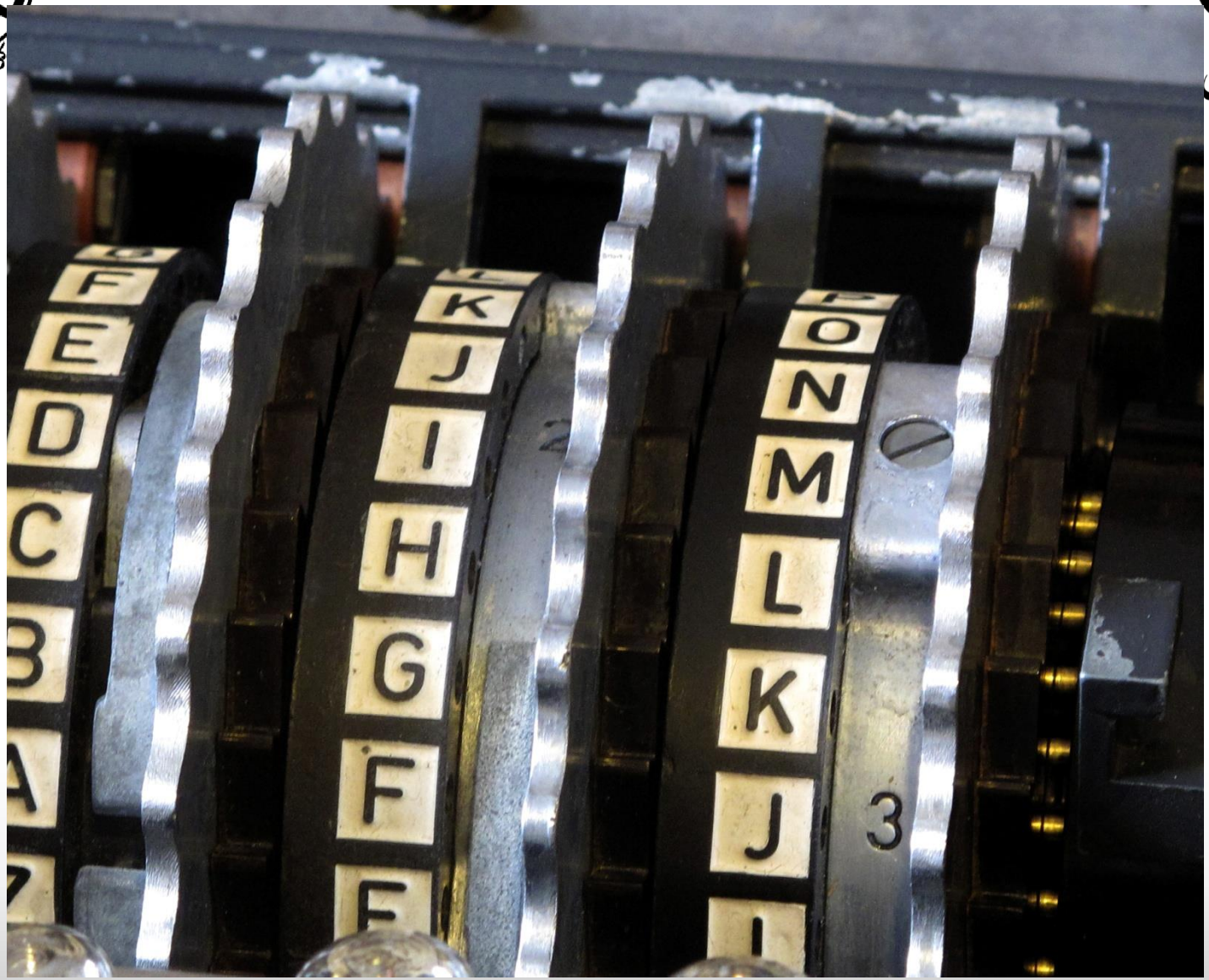
- ماشین روتور یک پیاده‌سازی الکترونیکی-مکانیکی از رمزچندالفبایی محسوب می‌شود.
- در این روش، داده‌ها از داخل تعدادی سیلندر که در مقابل هم قرار گرفته‌اند، عبور می‌کنند. هر سیلندر یک رمز تک الفبایی را انجام می‌دهد.
- به ازای هر حرف از ورودی، سیلندر اول به اندازه یک حرف می‌چرخد با یک دور گردش کامل هر روتور، روتور بعدی به اندازه یک حرف جابجا می‌شود.
- دوره تناوب ماشین روتور با افزایش تعداد روترها افزایش می یابد (26^n).
- آلمان ها 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.

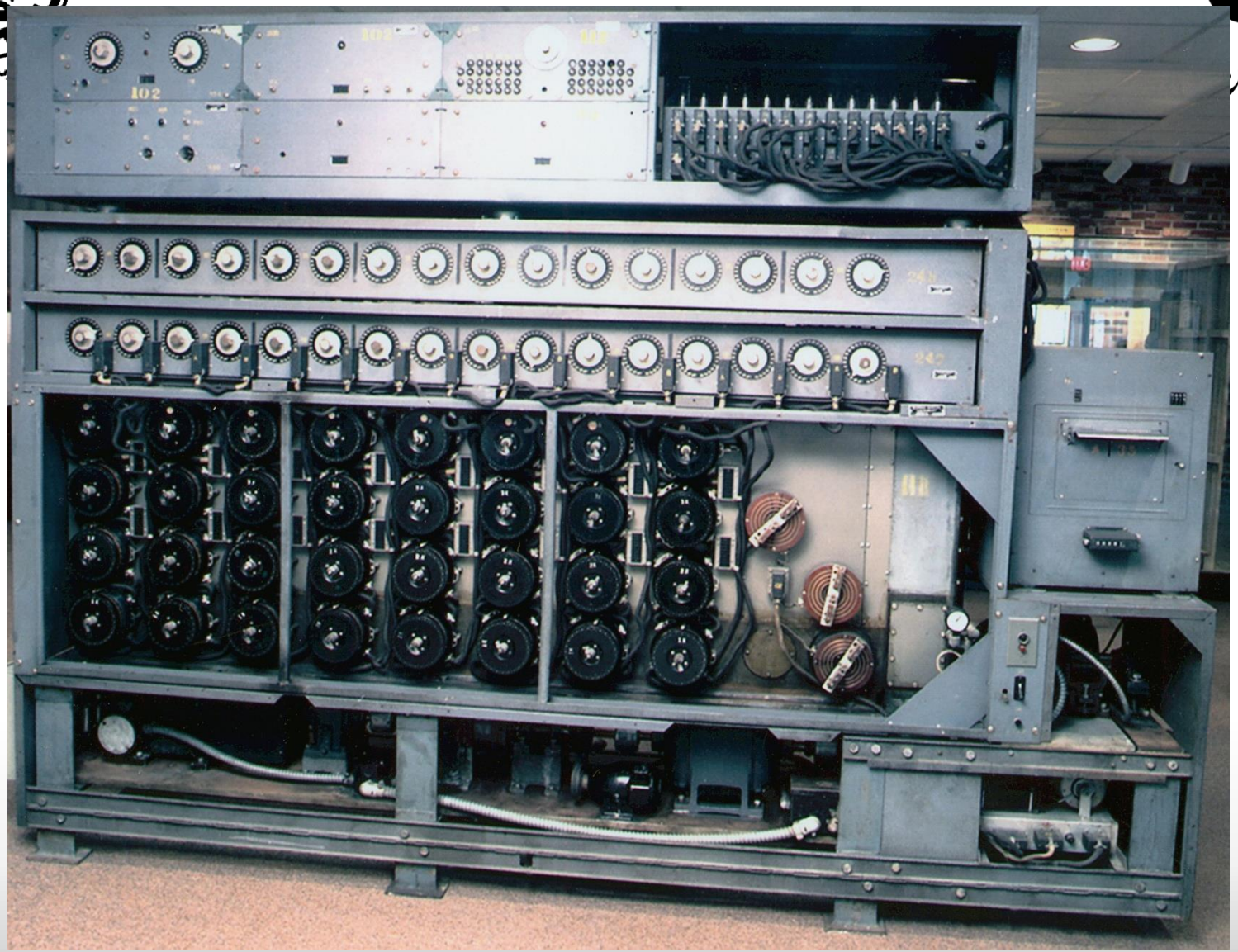
ماشینهای روتور

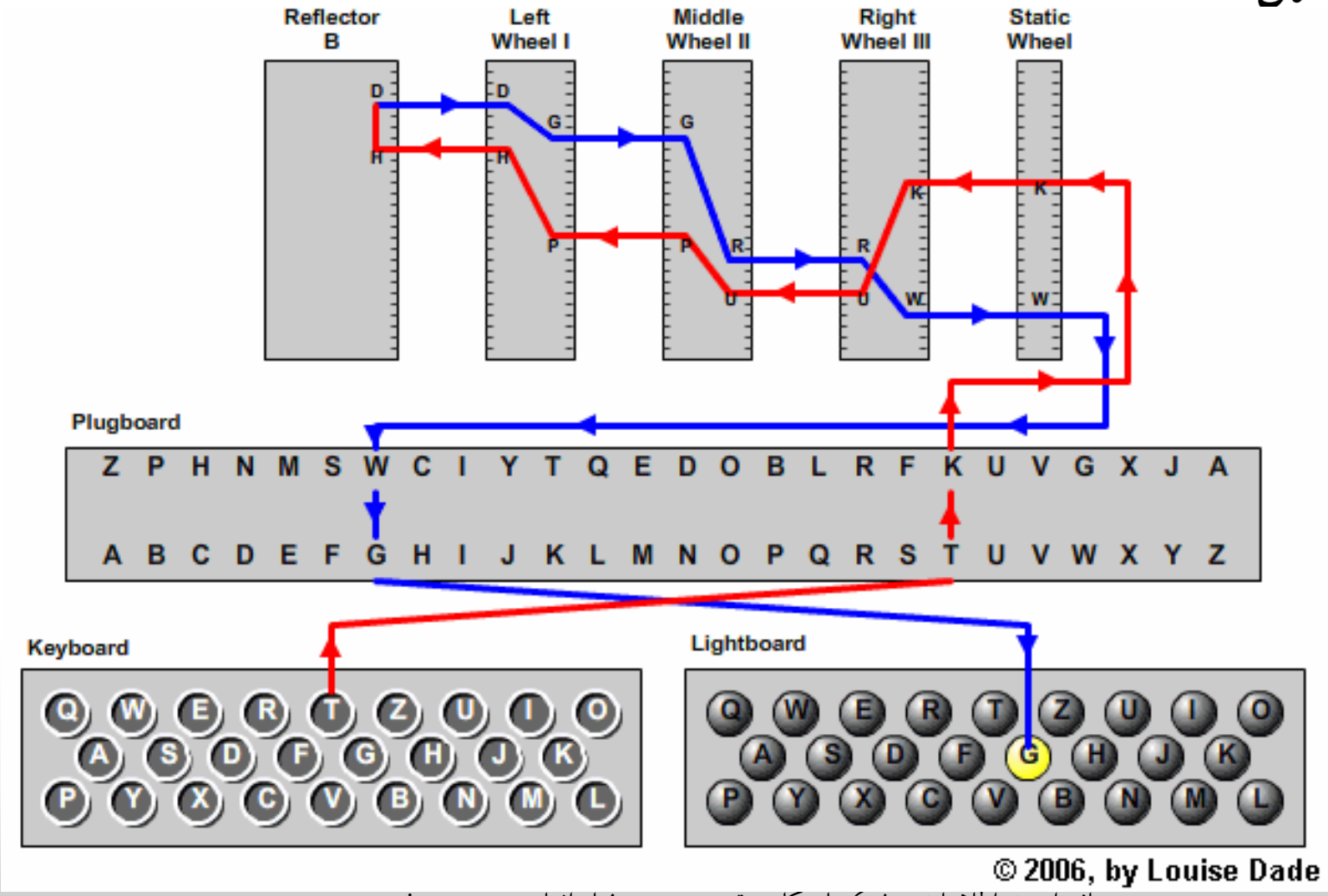


ماشینهای روتور




F
E
D
C
B
A
K
J
I
H
G
F
E
N
M
L
K
J
I
2
3




Reflector B
Left Wheel I
Middle Wheel II
Right Wheel III
Static Wheel
Plugboard
Z P H N M S W C I Y T Q E D O B L R F K U V G X J A
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
Keyboard
Lightboard
© 2006, by Louise Dade

Steganography

- An alternative to encryption
- Hides existence of message
  - Using only a subset of letters/words in a longer message marked in some way
  - Using invisible ink
  - Hiding in LSB in graphic image or sound file
- Has drawbacks
  - High overhead to hide relatively few info bits
- Advantage is can obscure encryption use

منابع

- اسلایدهای دکتر مرتضی امینی (منبع اصلی) – درس امنیت داده و شبکه
- جزوه درس اصول رمزنگاری دکتر عارف
- Cryptography and Network Security Principles and Practices, By William Stallings 5th Edition
- Elementary Cryptanalysis A mathematical approach, by Abraham Sinkov