



یادداشت‌های امن و آلمان

امنیت داده و شبکه

مفاهیم رمزنگاری و رمزنگاری کلاسیک

شرکت و آموزشگاه فنی و حرفه‌ای سورا

www.sooraac.ir

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
رمزنویسی: علم اصول و روش‌های رمزگذاری □

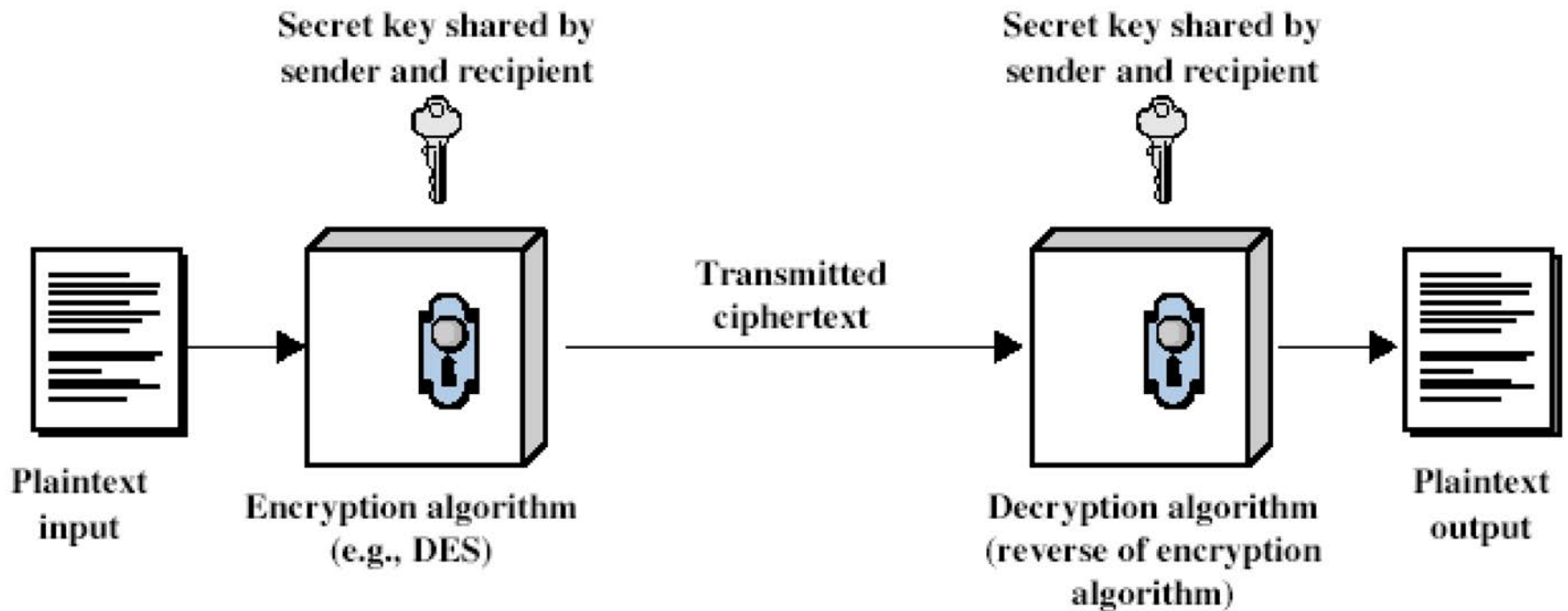
- **Cryptanalysis (codebreaking):** the study of principles/ methods of deciphering ciphertext *without* knowing key
تحلیل رمز: علم اصول و روش‌های رمزگشایی متن رمز بدون اطلاع از کلید □

- **Cryptology:** the field of both cryptography and cryptanalysis
رمزنگاری: علم حاصل از ترکیب رمزنویسی و تحلیل رمز □

رمزنگاری 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

- جایگزینی (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 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 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 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

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 جایگزینی و جایگشت هستند.

رمزهای کلاسیک

جانشینی

■ جانشینی یک حرف با حرف دیگر

□ تک الفبایی

□ چند الفبایی

■ حملات شناخته شده با استفاده از توزیع فرکانسها

جابجشت

■ جابجایی بین حروف متن اصلی

■ شکست رمز سخت تر.

ایده‌های تحلیل رمز کلاسیک

حملات Brute Force

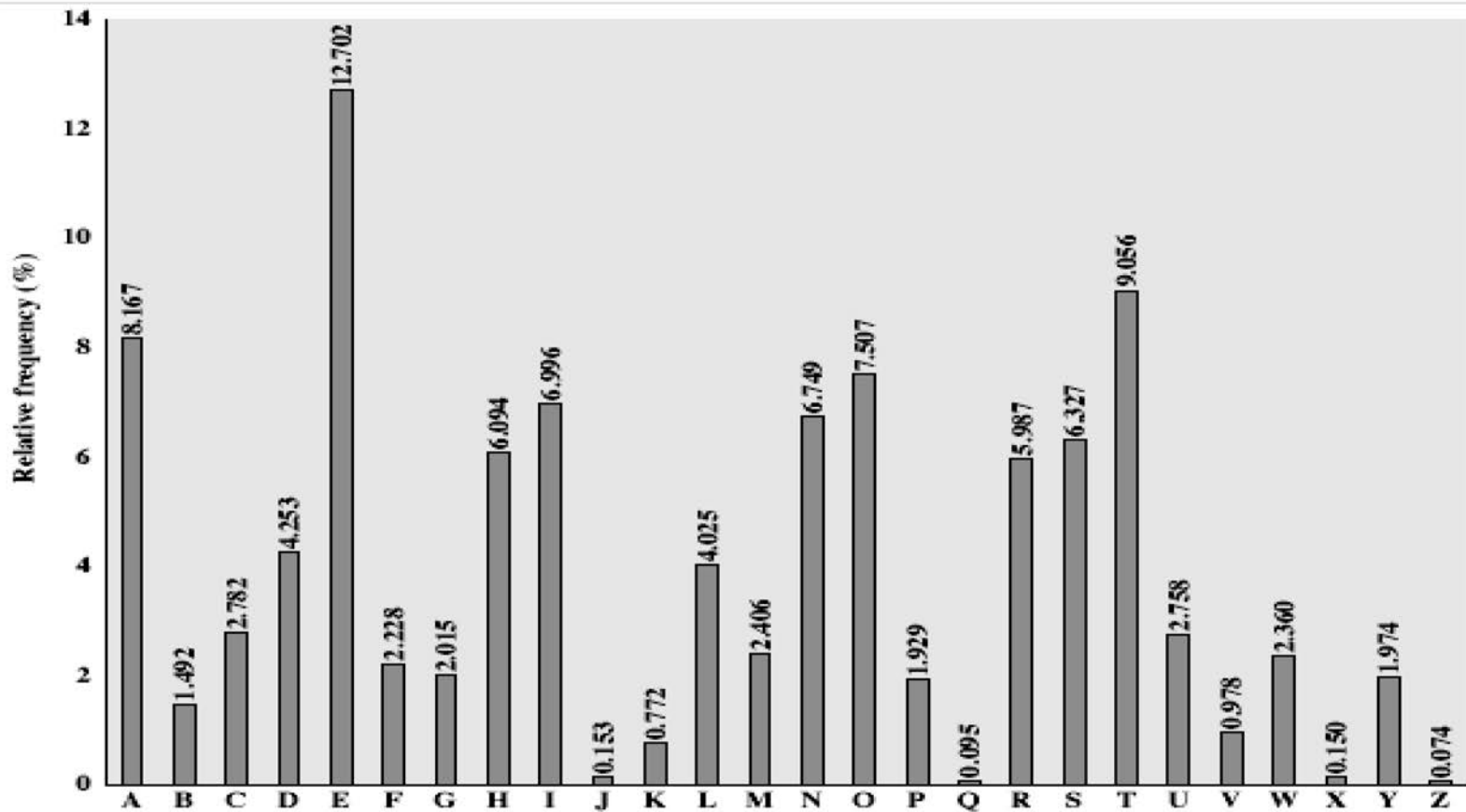
- جستجوی همه حالات (کلیدهای ممکن)

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 رمزشده و پیدا کردن طول کلید مورد استفاده استوار است.

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

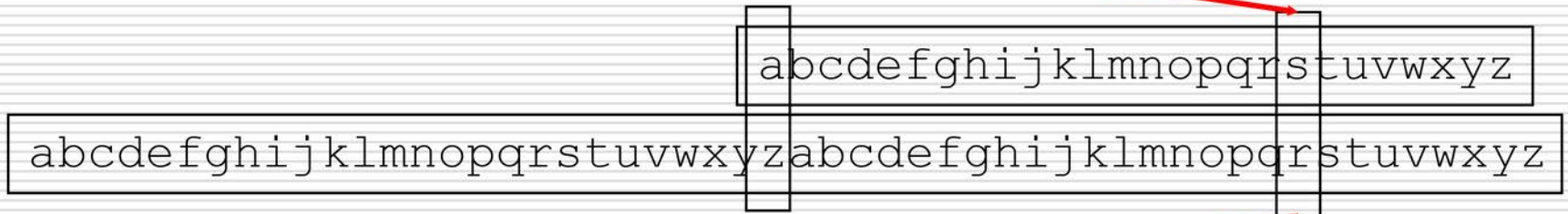
■ **K:** VIGVIGVIGVIGVIG

■ **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 $26! = 4 \times 10^{26} \ll$ غیرممکن

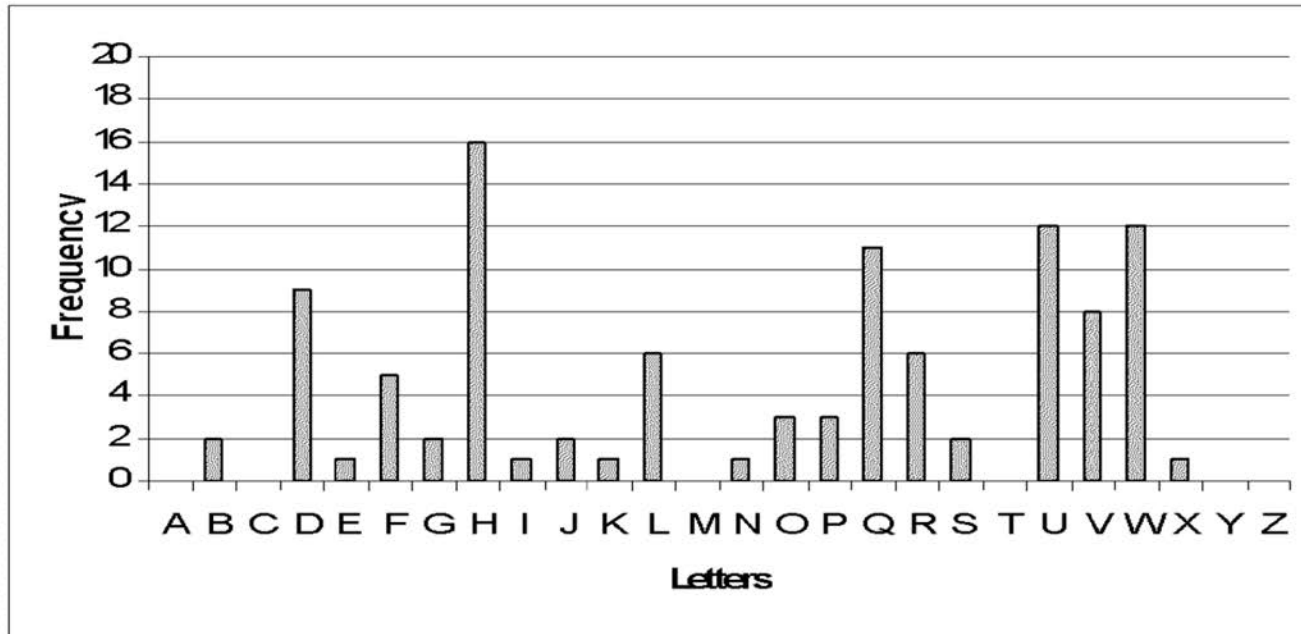
□ امکان حمله فرکانسی

■ 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 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 توزیع حروف برای شکست رمز استفاده کرد.

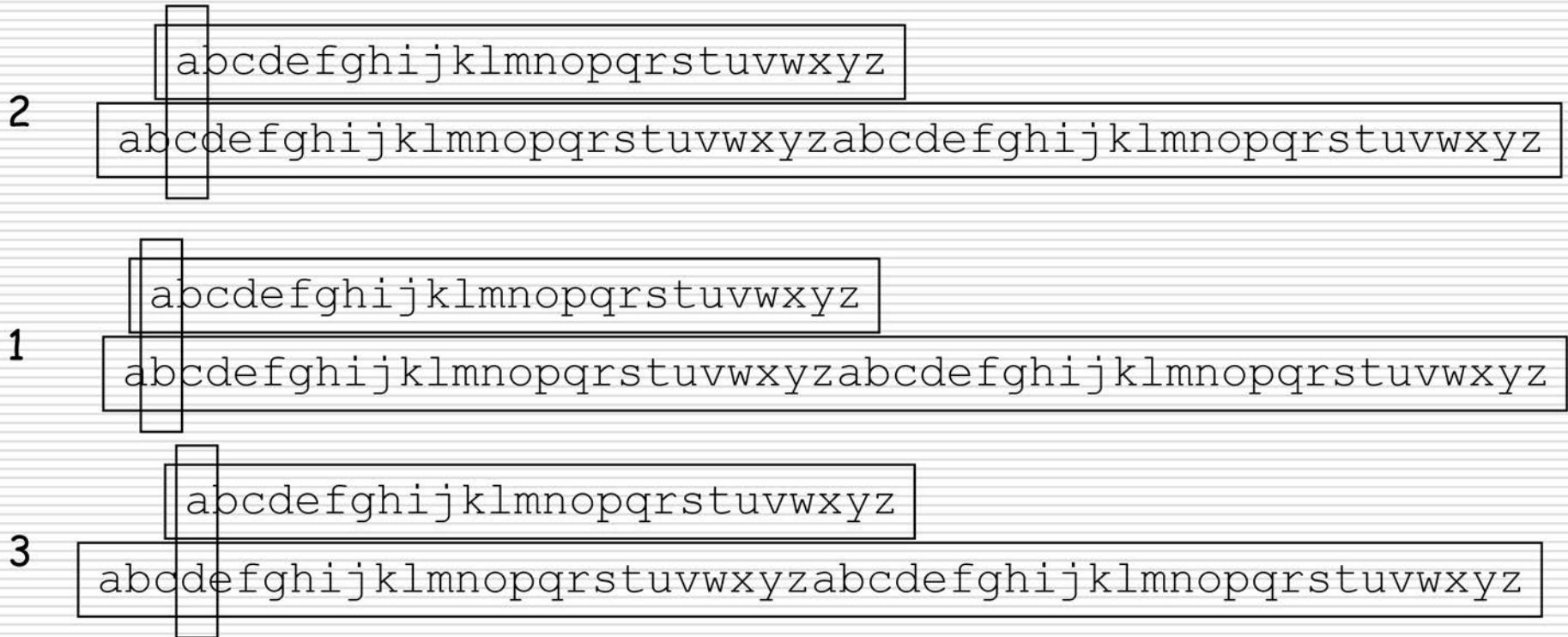
□ نمونه‌ها:

■ جانشینی Vigenere

مثال رمز چندالفبایی: جانشینی

۲۱۳

Plain: send another catapult



Cipher: ufqf bqqukgs fcudrvov

رمز Vigenère

- نوعی رمز جانشینی 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 معمولاً یک کلمه چندحرفی است که تکرار می‌شود.
- برای رمزگذاری و رمزگشایی از تابلوی رمز Vigenere می‌توان استفاده نمود.

تابلوی رمز Vigenere

		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
Key	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

رمز Vigenère

رمز گذاری: □

ستون = حرف مورد نظر

سطر = حرف کلید

محل تقاطع = رمز شده حرف مورد نظر

P= SEND ANOTHER CATAPULT

K= hail caeserh ailcaese

C= ZEVO CNSLLVY CIECPYDX

رمز گشایی: □

سطر = حرف کلید

محل تقاطع = حرف رمز شده

ستون = حرف رمز گشایی شده

تحلیل رمز Vigenère

- برای هر حرف، جانشینی‌های مختلفی را به کار می‌برد.
- با جانشینی‌های مختلف، تحلیل فرکانسی را مشکل می‌کند، ولی کاملاً 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.

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.

$$C_i = P_i \oplus K_i \quad \square \text{ رمز گذاری:}$$

\oplus means XOR

$$P_i = C_i \oplus K_i \quad \square \text{ رمز گشایی:}$$

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

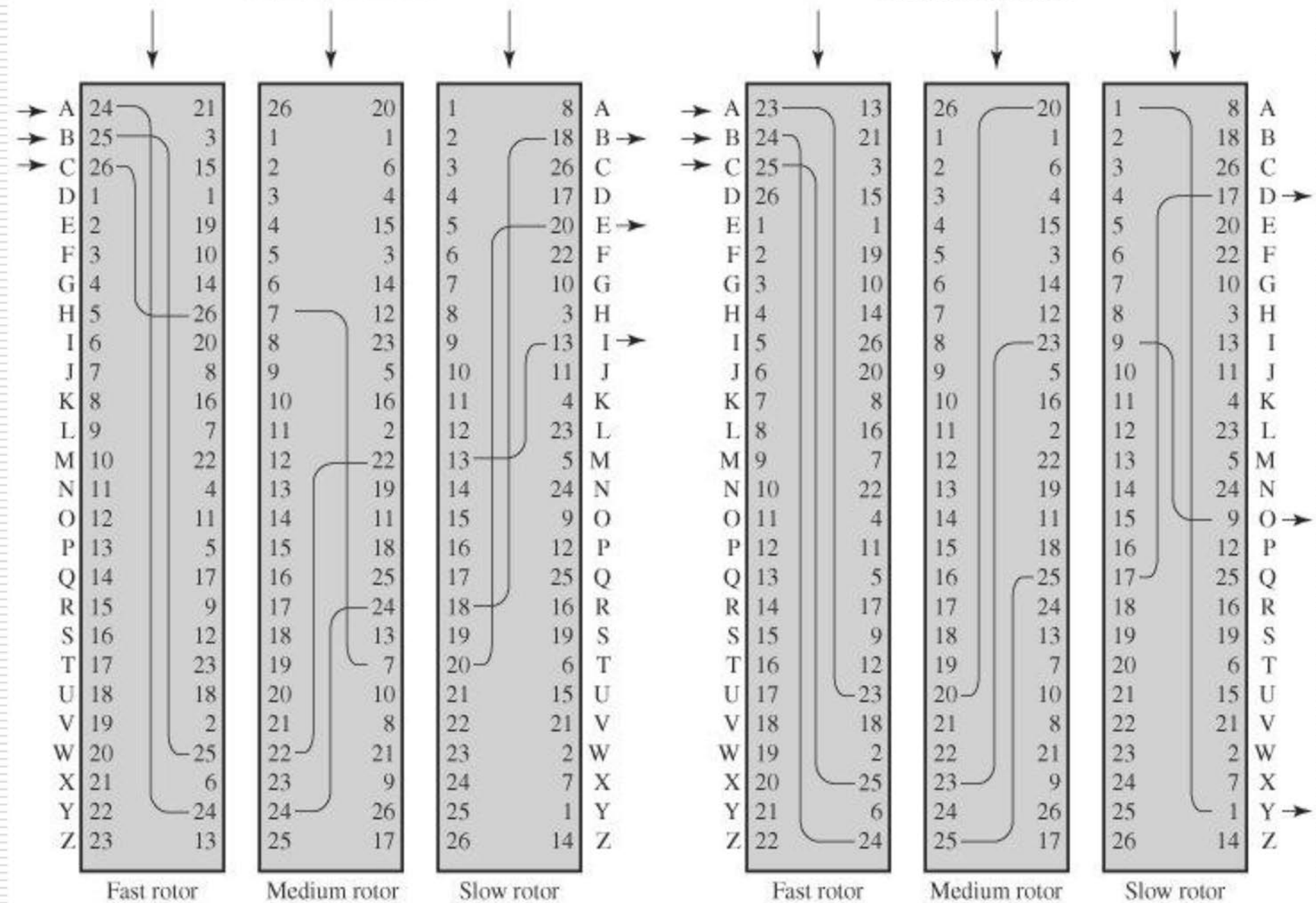
■ توزیع کلید (نیاز به ارسال کلید برای هر متن به اندازه خود آن)

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 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

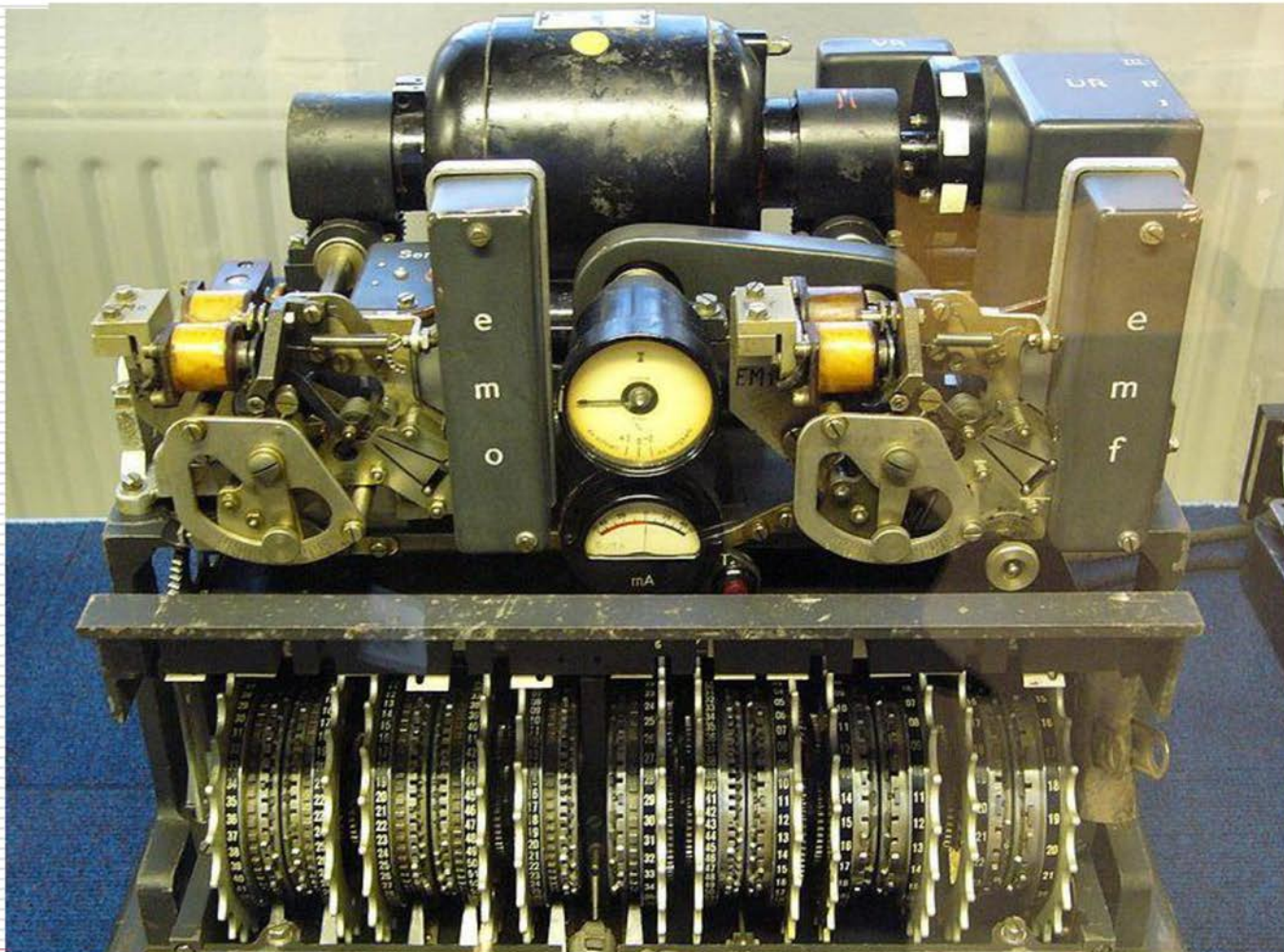
Direction of motion



(a) Initial setting

(b) Setting after one keystroke

ماشینهای روتور



ماشین‌های انیگما (Enigma Machines)

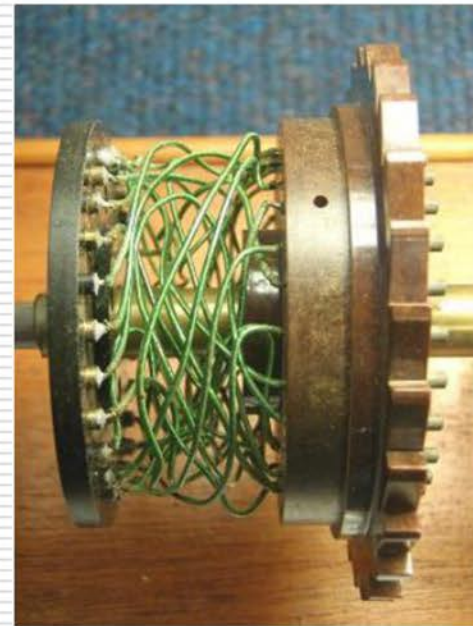
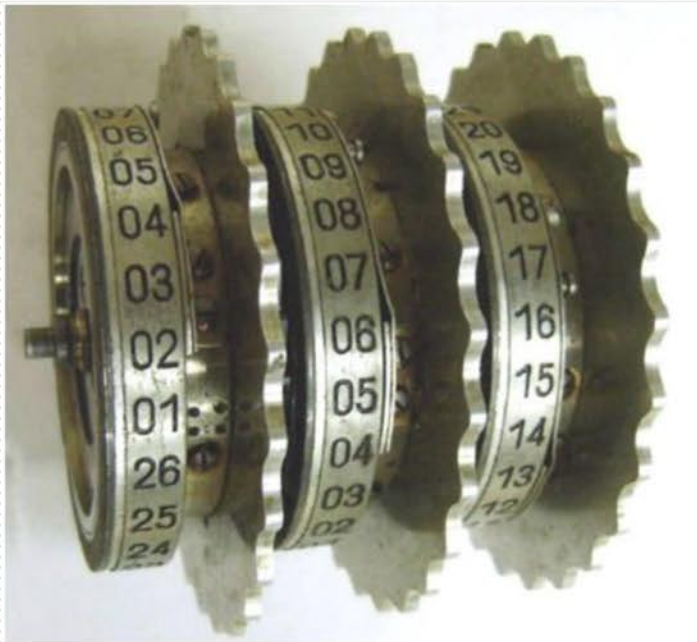


تایپ متن آشکار و روشن شدن لامپ متناظر در متن رمز



چرخنده‌ها – اهداف

- جایگزینی حروف با هم
- تغییر جایگزینی پس از تایپ هر حرف به وسیله چرخش



عملکرد چرخنده‌ها

- با تایپ هر حرف، چرخنده سمت راست (معروف به سریع) یک واحد می‌چرخد.
- با ۲۶ چرخش از چرخنده سریع، چرخنده وسط (معروف به میانی) یک واحد می‌چرخد.
- با ۲۶ چرخش از چرخنده میانی، چرخنده سمت چپ (معروف به کند) یک واحد می‌چرخد.
- چرخش چرخنده سبب می‌شود که سیم‌بندی تغییر کرده و جریان الکتریکی هر بار به نحو جدیدی هدایت شود.
- آلمانها هر روز صبح انیگما را با کلید جدیدی تنظیم می‌کردند.
- پیکربندی‌های هر روز از قبل روی دفترچه کد نوشته شده بود.
- با جوهر حل پذیر در آب برای نیروی زیر دریایی!

ماشین‌های انیگما: تاریخچه ۱-

- Enigma: معما، سخن پیچیده، چیستان
- ماشین‌های انیگما
 - مبدع: آرتور شربیوس، مهندس برق آلمانی (۱۸۷۸ تا ۱۹۲۹)
 - ابداع: اواخر جنگ جهانی اول
 - کاربرد اولیه: تجاری
 - استفاده بعدی: رمزنگاری توسط ارتش آلمان‌ها (افزودن صفحه دوشاخه)
 - در اواخر ۱۹۳۲ توسط لهستانی‌ها شکسته شد.

ماشین‌های انیگما: تاریخچه – ۲

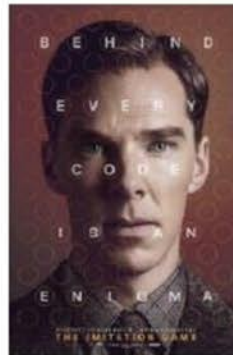
- درست قبل از جنگ جهانی دوم (۱۹۳۸)، آلمان‌ها تغییراتی در انیگما دادند که آن را بسیار پیچیده‌تر کرد.
- نسخه‌های مختلفی از انیگما توسط آلمان‌ها ابداع شد، که پیچیده‌ترین آن‌ها در نیروی دریایی مورد استفاده قرار گرفت.
- با شروع جنگ جهانی دوم و تسخیر لهستان، رمزنگاران لهستانی به فرانسه و از آنجا به انگلیس گریختند.
- تیمی از محقق و اپراتورها (بالغ بر ده هزار نفر) در پارک بلچلی انگلیس اقدام به شکستن رمز انیگما کردند.

ماشین‌های انیگما: تاریخچه – ۳

- ایده‌های آلن تورینگ در ساخت ماشینی برای شکستن انیگما
- حمله واژه محتمل: انیگما هرگز یک حرف را به خودش نمی‌نگاشت
- ماشین برنامه‌پذیر عام: شکستن انیگما ظرف ۲۰ دقیقه



Codebreaker
(2011)



The Imitation
Game (2014)



آلن تورینگ
(۱۹۱۲ تا ۱۹۵۴)

ماشین‌های انیگما: تاریخچه – ۴

- آلمان‌ها به حدی به کد خود مطمئن بودند که شواهد دال بر لو رفتن کدهای خود را نادیده گرفتند.
- انگلیس در حد امکان از متون لو رفته استفاده نمی‌کرد، تا بتواند آلمان‌ها را در غفلت نگه دارد.
- ولو به قیمت کشته شدن بسیاری در جنگ
- شکستن انیگما باعث شد انگلیس از قحطی نجات یابد و عامل مهم پیروزی متفقین محسوب می‌شود.
- پس از جنگ، به دستور چرچیل تمامی تجهیزات و مستندات پارک بلچلی نابود شد: از ترس دست یافتن جاسوسان شوروی بر آن!

فهرست مطالب

تعاریف

نیازمندی‌های رمزنگاری

رمز کلاسیک - جانشینی

رمز کلاسیک - جایگشت (جابجایی)

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 پرچین نرده‌ای (Rail Fence Cipher)

- ساده‌ترین مثال رمز جابه‌جایی
- متن آشکار از بالا به پایین و به صورت قطری روی نرده‌ای یک پرچین فرضی نوشته می‌شود.
- با رسیدن به نرده پایینی، جهت از پایین به بالا تغییر می‌کند.
- با رسیدن به نرده بالایی، جهت از بالا به پایین تغییر می‌کند.
- متن رمز از روی نرده‌ها به طور افقی خوانده می‌شود.



مثال از رمز پرچین نرده‌ای

متن آشکار: we are discovered; flee at once

تعداد نرده (کلید): ۳

W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .

متن رمز:

WECRLTEERDSOEFEAOCAIVDEN

رمز جایگشت ستونی (Columnar)

- 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*

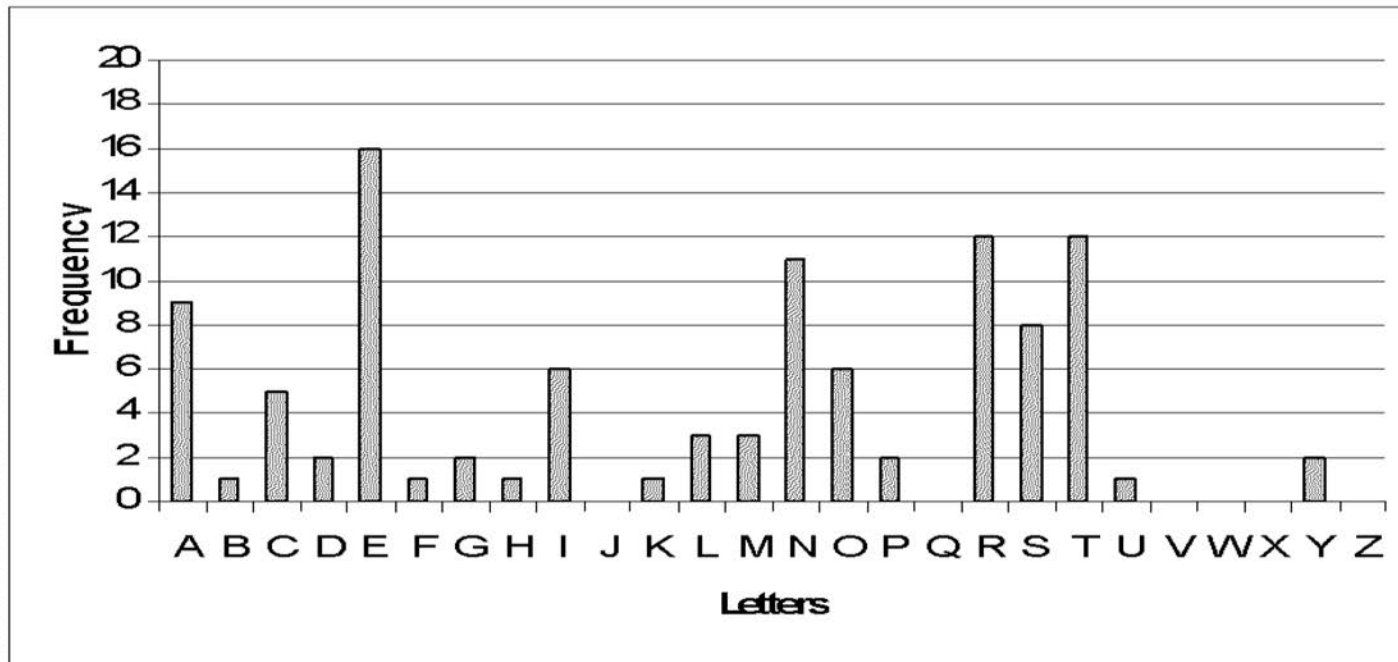
- کلید: ترتیب نوشتن ستون‌ها (در اینجا 43125)

NO**DTS*ENR*SAET*HE*

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

تحلیل رمز جایگشتی

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



فراوانی حروف متن اصلی

تحلیل رمز جایگشتی (مثال)

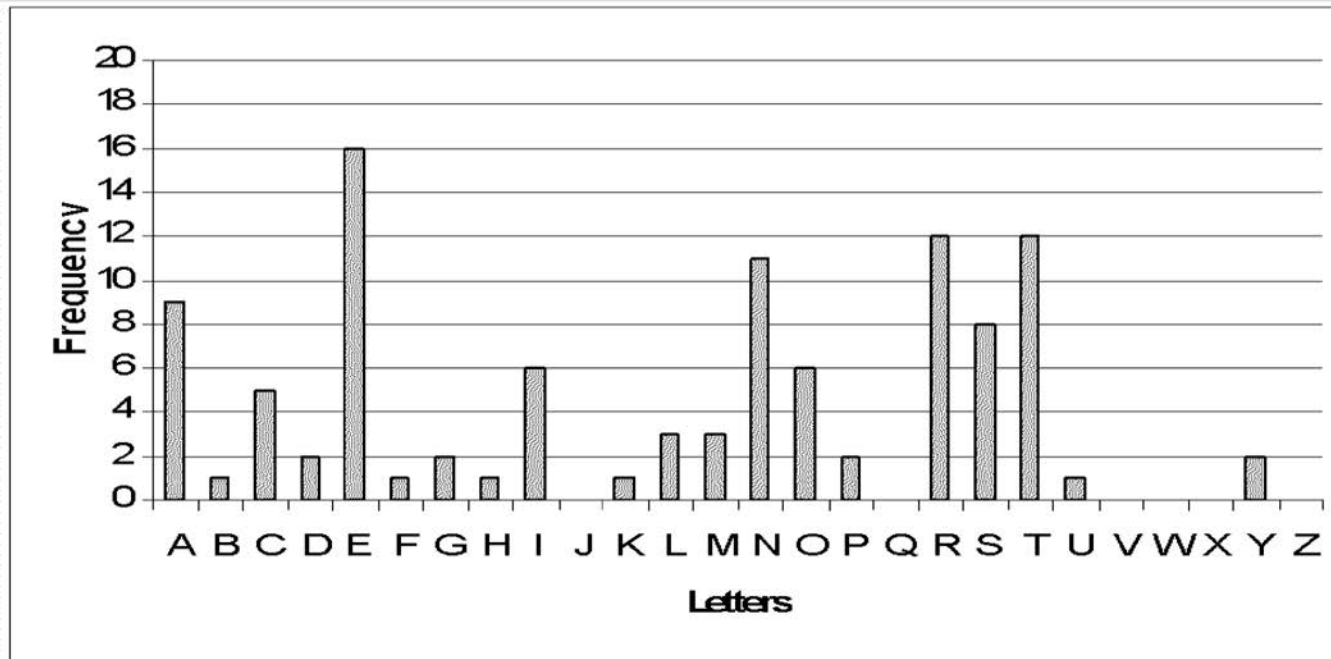
aerialreco
nnaissance
reportsene
myreinforc
ementsesti
matedatbat
talionstre
ngthenteri
ngyoursect
orPDClarke



ANRMEMTNNO
ENEYMAAGGR
RAPRETLTYP
IIOENEIHOD
ASRITDOEUC
LSTNSANNRL
RASFETSTSS
ENEOSBTEER
CCNRTARRCK
OEECITEITE

تحلیل رمز جایگشتی (مثال)

ANRMEMTNNOENEYMAAGGRRAPRETLTYPIIOENE
 IHODASRITDOEUCLSTNSANNRLRASFETSTSSSEN
 EOSBTEERC CNRTARRCKOE ECITEITE



فراوانی حروف متن رمز شده

تحلیل رمز جایگشتی

□ از مقایسه نمودارهای قبلی می‌توان فهمید در رمز جایگشتی:

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

■ تحلیلگر نمی‌تواند از نمودارهای فراوانی استفاده کند.



پایان