



آزمایشگاه امنیت داده و شبکه
<http://dns1.ce.sharif.edu>



دانشگاه صنعتی شریف
دانشکده مهندسی کامپیوتر

درس ۳: مفاهیم رمزنگاری و رمزنگاری کلاسیک

محمد صادق دوستی

• تعاریف

- حملات علیه رمزنگاری
- رمز کلاسیک - جانشینی
- رمز کلاسیک - جابه جایی

- متن آشکار (Plaintext): پیام اصلی (رمز نشده)
- متن رمز (Ciphertext): پیام رمز شده
- رمز (Cipher): الگوریتم تبدیل متن آشکار به متن رمز
- کلید (Key): اطلاعاتی که در رمز مورد استفاده قرار می‌گیرد و فقط گیرنده (و احتمالاً فرستنده) پیام آن را می‌دانند.
- رمزگذاری (Encipher, Encrypt): متن آشکار ← متن رمز
- رمزگشایی (Decipher, Decrypt): متن رمز ← متن آشکار

□ رمزنگاری (Cryptography): مطالعه اصول و روش‌های رمزگذاری

□ تحلیل رمز (Cryptanalysis, Codebreaking): مطالعه اصول و روش‌های رمزگشایی متن رمز بدون اطلاع از کلید

□ رمزشناسی (Cryptology): علم حاصل از ترکیب رمزنگاری و تحلیل رمز

رمزنگاری متقارن (Symmetric)

□ معادل با: رمزنگاری معمولی؛ رمزنگاری کلید خصوصی؛ رمزنگاری

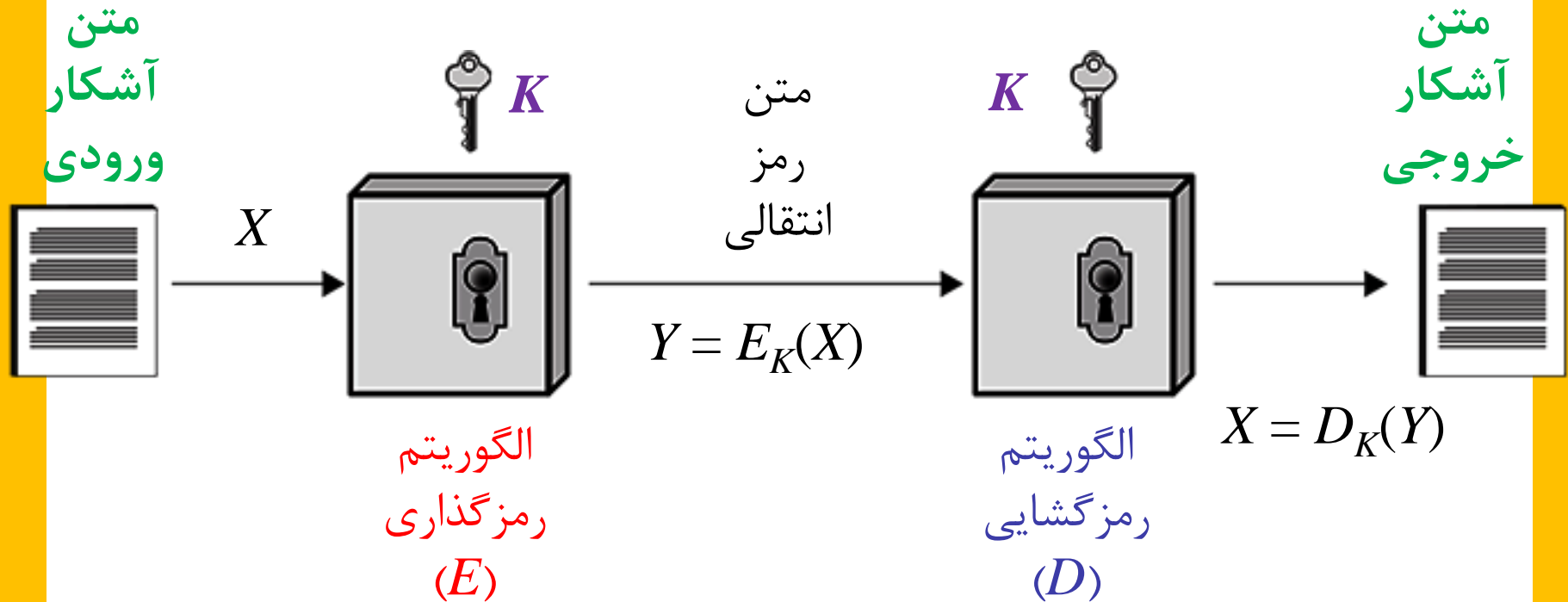
تک کلیدی

□ فرستنده و گیرنده از یک کلید مشترک استفاده می کنند.

□ تمام رمزنگاری های کلاسیک از نوع متقارن هستند.

□ تنها نوع رمزنگاری تا قبل از ۱۹۷۷

مدل رمزنگاری متقارن



- تعاریف
- حملات علیه رمزنگاری
- رمز کلاسیک - جانشینی
- رمز کلاسیک - جابه جایی

حمله جستجوی جامع (Brute-Force Search)

□ ابتدایی ترین حمله

□ «طراحی رمز» + «متن رمز» همواره در اختیار تحلیلگر رمز

□ امتحان تمام کلیدهای ممکن جهت رسیدن به متن آشکار

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

□ منابع مورد نیاز برای جستجوی جامع با طول کلید رابطه **نمایی** دارد.

زمان لازم برای جستجوی جامع

□ با فرض اینکه امتحان هر کلید فقط به ۱ نانو ثانیه زمان نیاز دارد:

طول کلید (بیت)	زمان تقریبی
۳۰	۱ ثانیه
۳۶	۱ دقیقه
۴۲	۱ ساعت
۴۶	۱ روز
۵۱	۱ ماه
۵۵	۱ سال
۶۲	۱۵۰ سال
۸۰	۳۸ میلیون سال
۱۲۸	۱۰ هزار میلیارد میلیارد سال
۱۹۲	2×10^{41} سال
۲۵۶	$3/7 \times 10^{60}$ سال

□ منابع محاسباتی: زمان، حافظه، انرژی، ...

□ محرمانگی مطلق (Perfect Secrecy)

👉 حتی با منابع محاسباتی نامحدود نتوان رمز را شکست.

□ محرمانگی محاسباتی (Computational Secrecy)

👉 با فرض محدودیت روی منابع محاسباتی، رمز قابل شکستن نباشد.

□ با One-Time Password اشتباه نشود!

□ این رمز محرمانگی مطلق دارد.

☞ فضای پیام، کلید، و رمز: رشته‌های بیتی

☞ از XOR به عنوان عملگر استفاده می‌شود.

□ برای رمز هر پیام، کلید (Pad) جدیدی با طول مساوی پیام و

به تصادف انتخاب می‌شود.

□ رمز گذاری: $C_i = P_i \oplus K_i$

□ رمز گشایی: $P_i = C_i \oplus K_i$

ایراد؟؟؟

□ آگوست کِرکِهفَس (Auguste Kerckhoffs)

👉 ۱۸۳۵ تا ۱۹۰۳ میلادی

👉 زبان شناس و رمزنگار هلندی

□ مقاله در ۱۸۸۳ در مجله علوم جنگی

👉 عنوان: La Cryptographie Militaire

👉 شش اصل طراحی رمز



- ❑ اگر سیستم به طور مطلق امن نیست، باید در عمل امن باشد.
- ❑ طراحی سیستم نباید نیاز به مخفی کاری داشته باشد، و افشای طراحی نباید مکاتبه کنندگان را به زحمت بیندازد. (مشهورترین اصل)
- ❑ طرفین باید بتوانند کلید را به سادگی به خاطر بسپارند و تغییر دهند.
- ❑ باید بتوان رمزها را با تلگراف مخابره کرد.
- ❑ باید اسناد و ابزارهای رمزنگاری را یک نفر به تنهایی بتواند حمل و استفاده کند.
- ❑ استفاده از سیستم باید آسان باشد، و نیاز به لیست طولانی از قوانین یا تلاش ذهنی زیاد نداشته باشد.

نیازمندی‌های امنیتی رمزنگاری متقارن

□ یک الگوریتم رمزنگاری قوی

□ یک کلید مخفی که تنها فرستنده و گیرنده از آن آگاه هستند.

$$Y = E_K(X) \quad X = D_K(Y)$$

□ اصل کرکهففس: الگوریتم رمزنگاری برای همه مشخص است.

👉 نفی امنیت از طریق ابهام (Security through Obscurity)

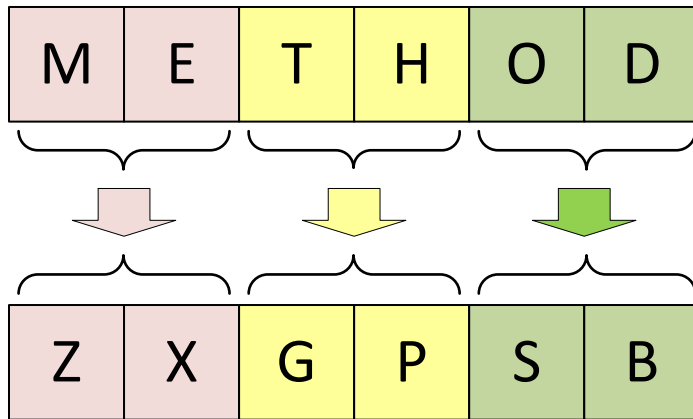
👉 امنیت فقط وابسته به مخفی بودن کلید است.

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

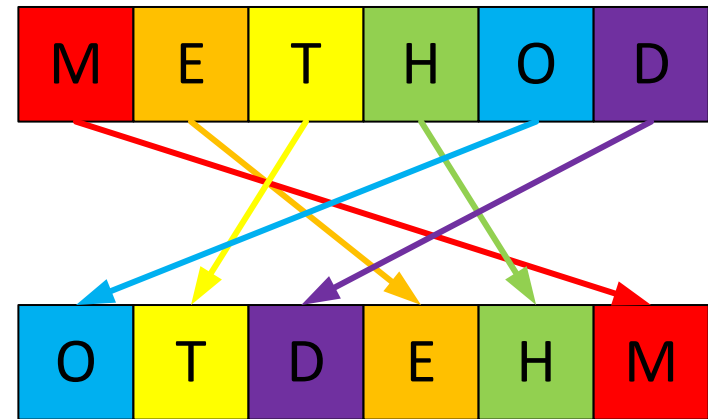
□ اعمال مورد استفاده برای رمزگذاری:

👉 جابه‌جایی (Transposition): جایگشت عناصر ورودی

👉 جانشینی (Substitution): جایگزینی عناصر ورودی با عناصری دیگر



جانشینی



جابه‌جایی

□ تعداد کلیدهای مورد استفاده:

☞ یک کلید خصوصی مشترک

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

□ روش پردازش متن آشکار:

☞ قالبی (Block): بلوکی از عناصر متن پردازش و رمز می‌شوند.

☞ جریانی (Stream): عناصر متن به طور پیوسته به ورودی داده شده و در هر لحظه یک عنصر رمز شده خارج می‌شود.

□ هدف از حمله:

☞ استخراج بخشی (یا کل) متن آشکار از متن رمز شده

☞ در صورت امکان، استخراج کلید

□ نحوه حمله:

☞ بررسی طراحی الگوریتم رمز

☞ بررسی مجموعه‌ای از متن‌های آشکار و رمز شده آنها

انواع حملات تحلیل رمزنگاری بر اساس اطلاعات در اختیار

□ «طراحی رمز» + «متن رمز» همواره در اختیار تحلیلگر رمز

نوع حمله	سایر اطلاعات در اختیار تحلیلگر رمز
فقط متن رمز Ciphertext Only	-
متن آشکار معلوم Known Plaintext	مجموعه‌ای از «متون آشکار و رمز شده آنها»
متن آشکار انتخابی Chosen Plaintext	متون آشکار انتخاب شده توسط تحلیلگر و متون رمز معادل آنها
متن رمز انتخابی Chosen Ciphertext	متون رمز انتخاب شده توسط تحلیلگر و متون آشکار حاصل از رمزگشایی آنها
متن انتخابی Chosen Text	ترکیب دو مورد فوق

- تعاریف
- حملات علیه رمزنگاری
- رمز کلاسیک - جانشینی
- رمز کلاسیک - جابه جایی

□ تا جنگ جهانی دوم و حین آن مورد استفاده قرار می گرفتند.

☞ در این جنگ، ضعف آنها مشخص شد.

☞ حین جنگ و پس از آن: مطالعه ریاضی رمزها و خواص آنها

☞ طراحی اصولی رمزها

□ معمولاً مبتنی بر یکی از دو روش اصلی جانشینی و جابه جایی هستند، ولی نه هر دو.

□ جایگزینی حروف متن آشکار با حروف دیگر

👉 **تک الفبایی (Monoalphabetic):** یک حرف همواره با یک حرف مشخص جایگزین می شود.

👉 **چند الفبایی (Polyalphabetic):** ممکن است یک حرف هر بار با یک حرف جدید جایگزین شود.

👉 **هم آوایی (Homophonic):** ممکن است یک حرف با چند حرف جایگزین شود.

👉 **چند نگاری (Polygraphic):** چند حرف با چند حرف جایگزین می شود.

رمزهای جانشینی - ۲

چند الفبایی

A	A	A
---	---	---



X	Y	Z
---	---	---

تک الفبایی

A	A	A
---	---	---



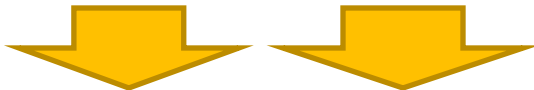
Z	Z	Z
---	---	---

متن آشکار:

متن رمز:

چند نگاری

A	B	A	C
---	---	---	---



X	Y	Z	W
---	---	---	---

هم آوایی

A	B	C
---	---	---



P	B	X	Z
---	---	---	---

متن آشکار:

متن رمز:

رمز سزار (قیصر – Caesar)



□ ساده‌ترین رمز جانشینی تک الفبایی

□ شماره حروف در الفبا: $a = 0$ ، $b = 1$ ، $c = 2$ ، ...

□ کلید یک حرف تصادفی در الفبا است

□ محاسبه رمز: به ازای هر حرف M در پیام و کلید K :

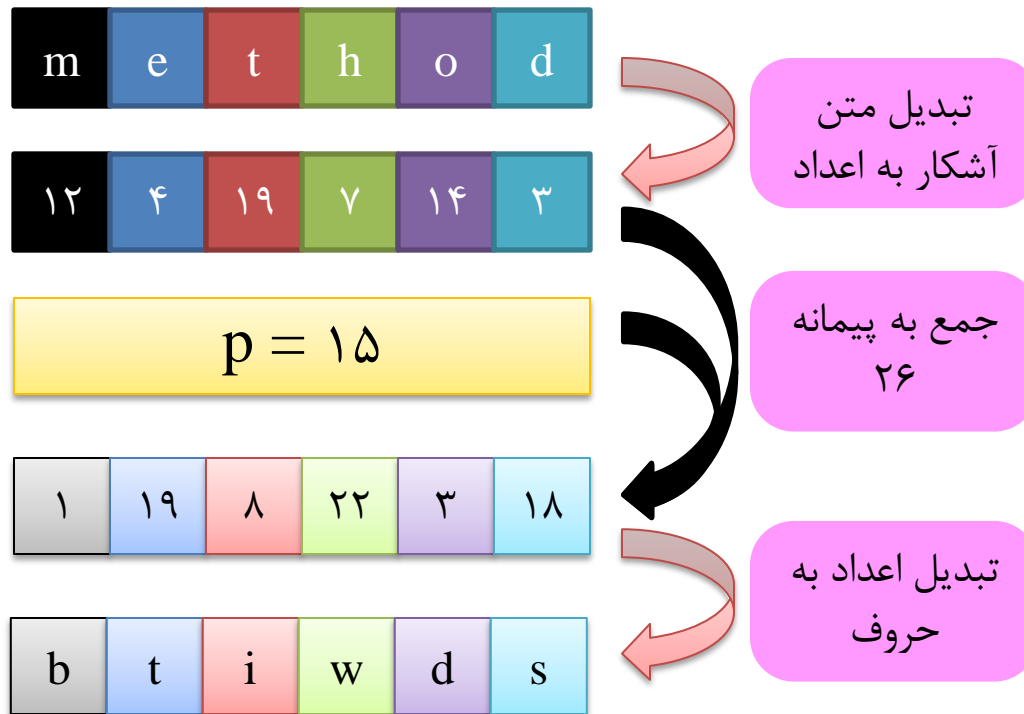
➡ محاسبه جمع شماره M و شماره K به پیمانه ۲۶

➡ تبدیل عدد حاصل به حرف معادل در الفبا

مثال از رمز سزار

□ متن آشکار: method

□ کلید: حرف p



□ رمز سزار به سادگی با آزمون جامع می شکند.

رمز جانشینی تک الفبایی – بهبود رمز سزار

□ کلید رمز سزار فقط یک حرف بود.

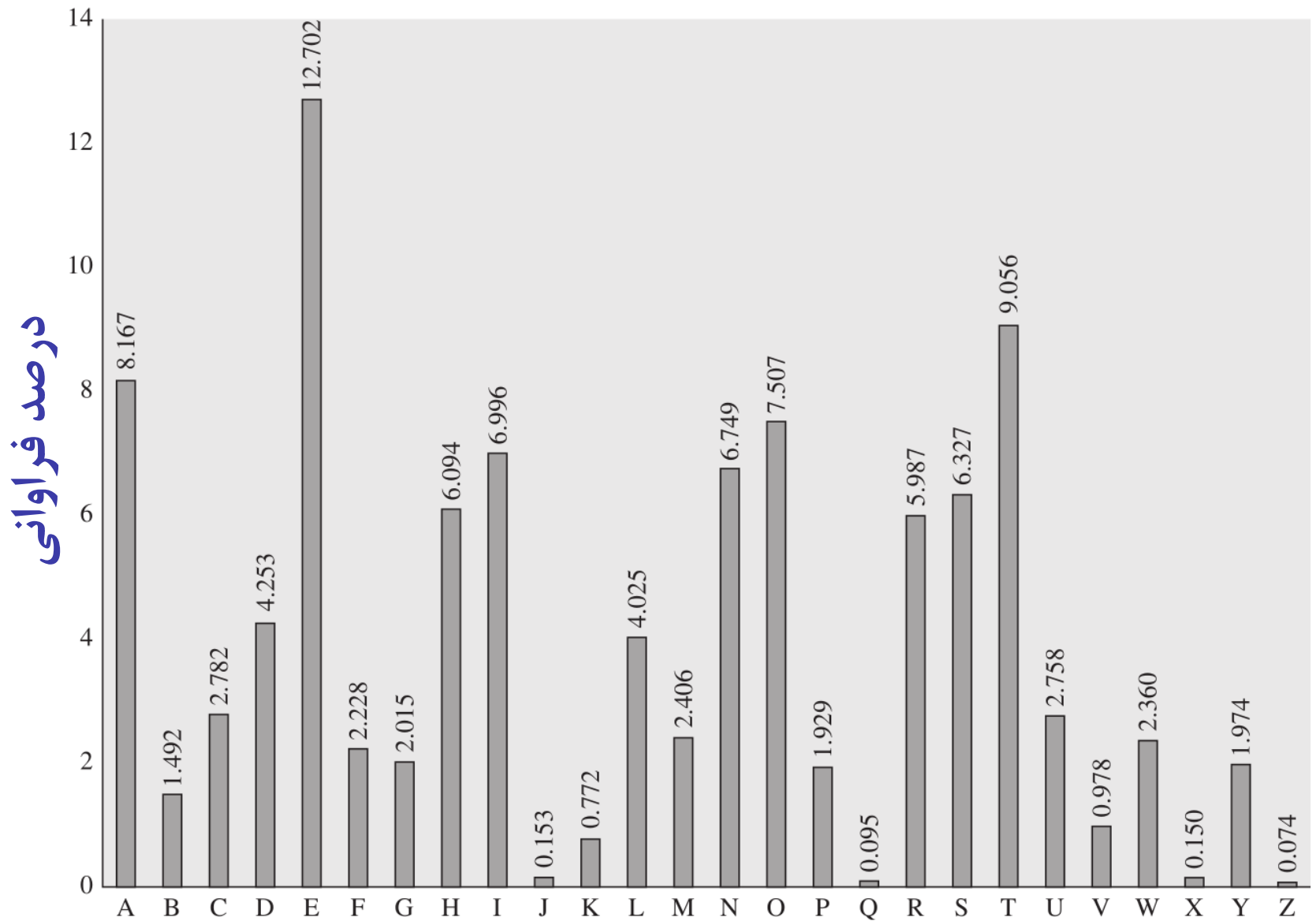
□ می‌توان رمزی ساخت که در آن هر حرف با حرف دیگری در الفبا جایگزین می‌شود.

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

□ مثال: رمز شده «method» ← «VQIYZC».

□ تعداد کلیدهای ممکن $26!$ (۲۶ فاکتوریل)؛ معادل کلید به طول ۸۸ بیت. ← جستجوی جامع هزاران سال طول می‌کشد.

فراوانی حروف انگلیسی در متون



تحلیل رمز جانشینی تک الفبایی

□ امکان حمله فراوانی (فرکانسی)

☞ با مقایسه نمودار فراوانی حروف در متن رمز با نمودار استاندارد فراوانی حروف، می توان تناظر احتمالی حروف را پیدا کرد.

□ مثال: در اسلاید بعد داریم:

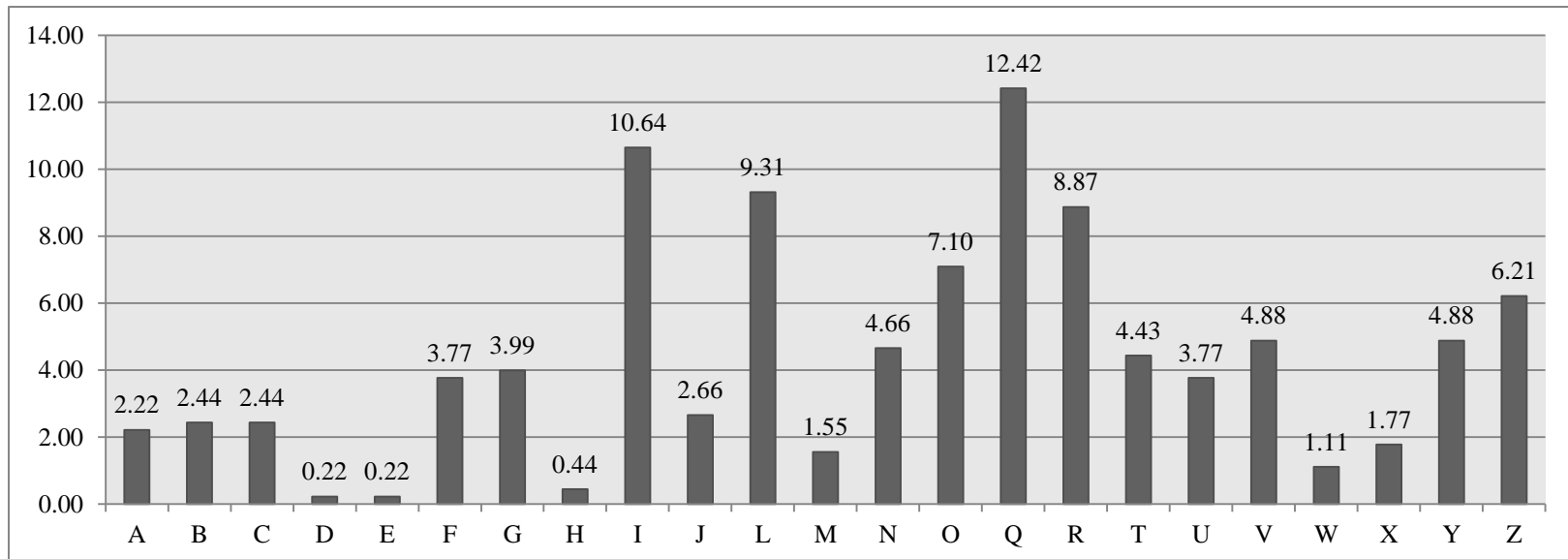
☞ احتمالاً Q رمز شده e است.

☞ احتمالاً I رمز شده t است.

☞ ...

تحليل رمز جانشینی تک الفبایی (مثال)

IYQCQILTARZJLRBVVQIOTNNOBUIZMOLUYBVLWQTIAQRRFRQJFAIYLGRBV
VQIOTNNOBUIZMOLUYBJZOLNIFLAABRQGCTGMVQRRLMQRTGRIQLCTITRZJ
IQGFRQCJZONZVUFIQORTMGLIFOQRXYQGLNZVUFIQOVFRIWGZXIYLILJTA
QXLRRQGIJOZVLNQOILTGRQGCQOJZOQELVUAQNZVUFIQORZJIXLOQNZVUL
GTQRIYLIQQAQLRQFUCLIQRJZOIYQTORZJIXLOQNLGRTMGIYZRQFUCLIQR
IZUOZHQIYLIYQFUCLIQXLRVLCQDBIYQVRZIIYLIYLNWQORNLGZIVLWQI
YQTOZXGFUCLIQRIYLIIXZFACNLFRQYLOVNZVUFIQORNGLARZFRQLRBVVQ
IOTNNTUYQORIZMTHQQLNYZIIYQOIYQWQBRJZORBVVQIOTNNTUYQOR



رمز جانشینی چند الفبایی

□ 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.

□ نمونه‌ها:

👉 رمز وِیژنِر (Vigenère)

👉 ماشینِ اَنِگِما (Enigma)

رمز ویژنر (Vigenère)

□ بلز دو ویژنر (۱۵۲۳ تا ۱۵۹۶)

☞ دیپلمات، رمزنگار، مترجم، و کیمیاگر فرانسوی

□ پیش از ویژنر، این رمز توسط یک ایتالیایی (جوان باتیستا بلّاس) در سال ۱۵۵۳ ابداع شده است.

□ رمز ویژنر = چندین رمز سزار.

☞ هر رمز سزار، کلید خود را دارد.

☞ کلید پس از مدتی تکرار می‌شود.



□ متن آشکار = ATTACKATDAWN

□ کلید = LEMON

👉 کلید را زیر متن آشکار نوشته و تکرار می کنیم.

👉 هر حرف متن آشکار با حرف کلید در زیر آن به روش سزار رمز می شود.

متن آشکار	A	T	T	A	C	K	A	T	D	A	W	N
کلید	L	E	M	O	N	L	E	M	O	N	L	E
متن رمز	L	X	F	O	P	V	E	F	R	N	H	R

تابلو (Tableau) در رمز ویتز

	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

استفاده از تابلو جهت تسهیل رمزنگاری و یژنر

□ رمزگذاری:

ستون = حرف متن آشکار

سطر = حرف کلید

محل تقاطع = حرف رمز شده

□ رمزگشایی:

سطر = حرف کلید

محل تقاطع = حرف رمز شده

ستون = حرف متن آشکار

□ فردریش ویلهلم کاسیسکی (۱۸۰۵ تا ۱۸۸۱)

☞ سرگرد پیاده نظام در ارتش آلمان

□ ایده کاسیسکی: گاه ممکن است **واژگان تکراری** با **حروف یکسانی** از **کلید** رمز شوند.

☞ نتیجه: تکرار در متن رمز شده

□ روش کاسیسکی

☞ یافتن الگوهای تکراری در متن رمز شده

☞ حدس زدن طول کلید



P: CRYPTOISSHORTFORCRYPTOGRAPHY

K: ABCDABCDABCDABCDABCDABCDABCD

C: CSASTPKVSIQUTGQUCSASTPIUAQJB



فاصله = ۱۶ حرف

□ فرض: بخش تکرار شده از C معادل بخش تکرار شده از P است:

☞ طول کلید یکی از عوامل ۱۶ خواهد بود (۱، ۲، ۴، ۸، یا ۱۶).

□ با مشاهده چند الگوی تکرار شده می توان حدس را دقیقتر کرد.

□ روش کاسیسی

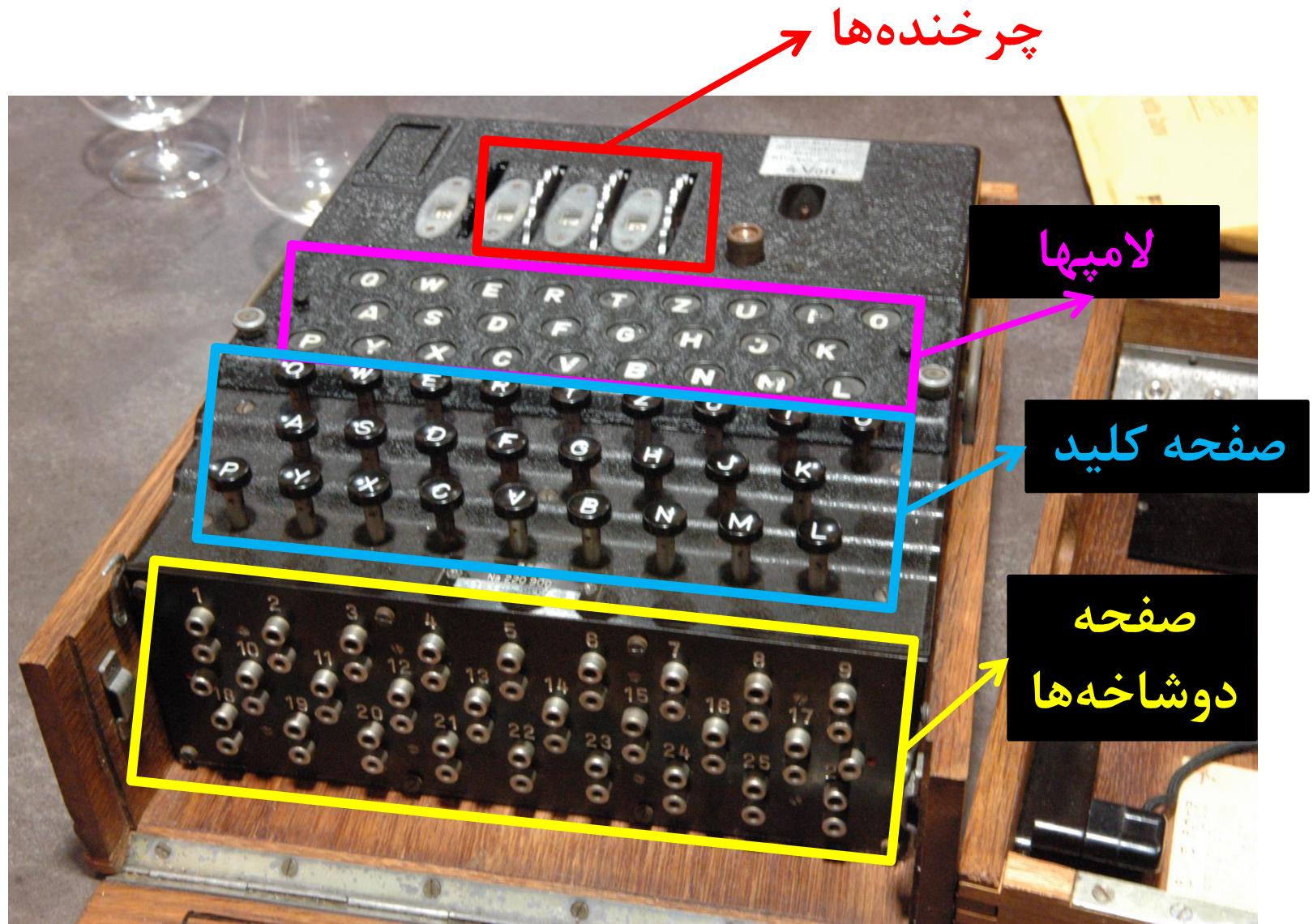
□ آزمون فریدمن (Friedman)

□ روش واژه محتمل (Probable Word)

☞ واژه‌ای که با توجه به محتوا، احتمال وقوع آن در متن زیاد است.

□ با استفاده از حملاتی نظیر «متن آشکار معلوم» کلید به سادگی استخراج می‌شود.

ماشینهای انیگما (Enigma Machines)



□ یک پیاده‌سازی الکترونیکی-مکانیکی از رمز چند الفبایی. شامل:

☞ یک صفحه کلید (برای تایپ متن آشکار / متن رمز)

☞ صفحه دوشاخه‌ها و تعدادی چرخنده (انجام رمزنگاری)

☞ تعدادی لامپ (مشاهده متن رمز / متن آشکار)

□ متن رمز حرف به حرف یادداشت و مخابره می‌شد.

☞ این ایده که ماشین خودش پیام را مخابره کند، سبب می‌شد که

وزن ماشین ۸ برابر شود ← نقض اصل ۵ کِرکهُفس

تایپ متن آشکار و روشن شدن لامپ متناظر در متن رمز



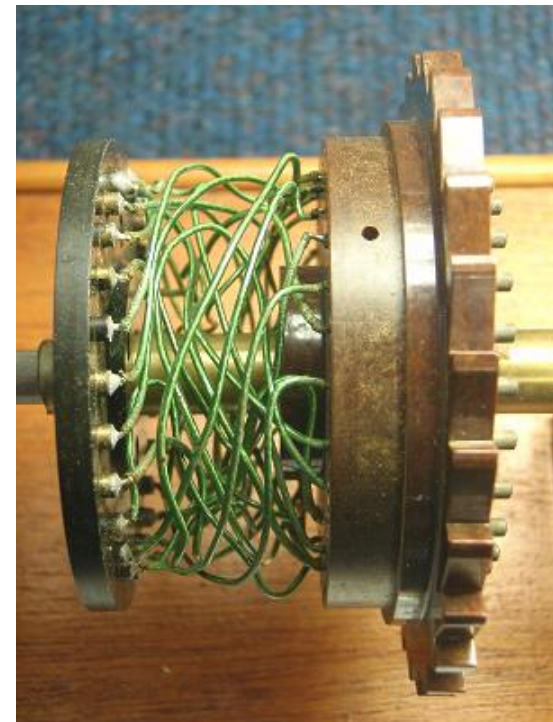
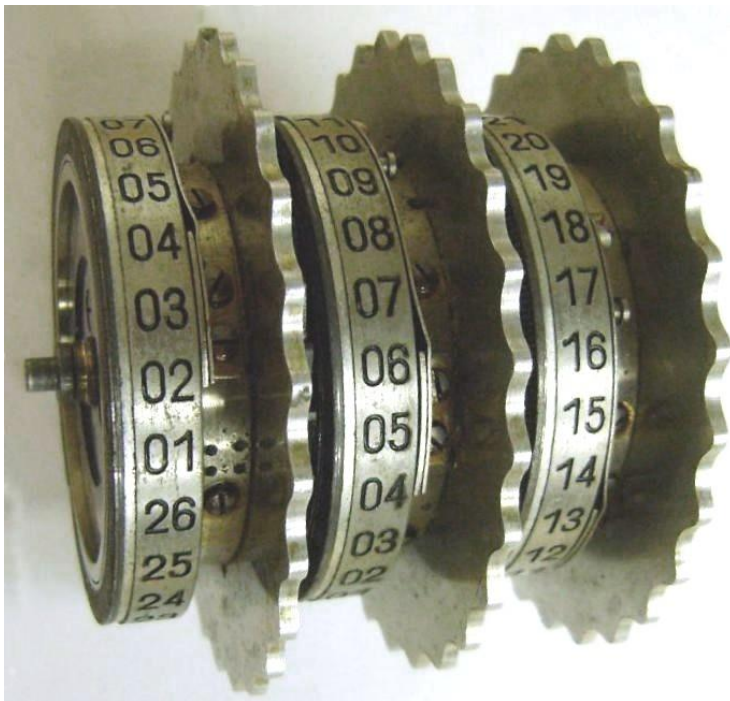
اهداف صفحه دوشاخه‌ها

□ جایگزینی حروف با هم

□ قابلیت تغییر جایگزینی به صورت دلخواه



- جایگزینی حروف با هم (نگاشت درونی هر چرخنده ثابت است)
- تغییر جایگزینی پس از تایپ هر حرف به وسیله چرخش



چگونگی عملکرد چرخنده‌ها

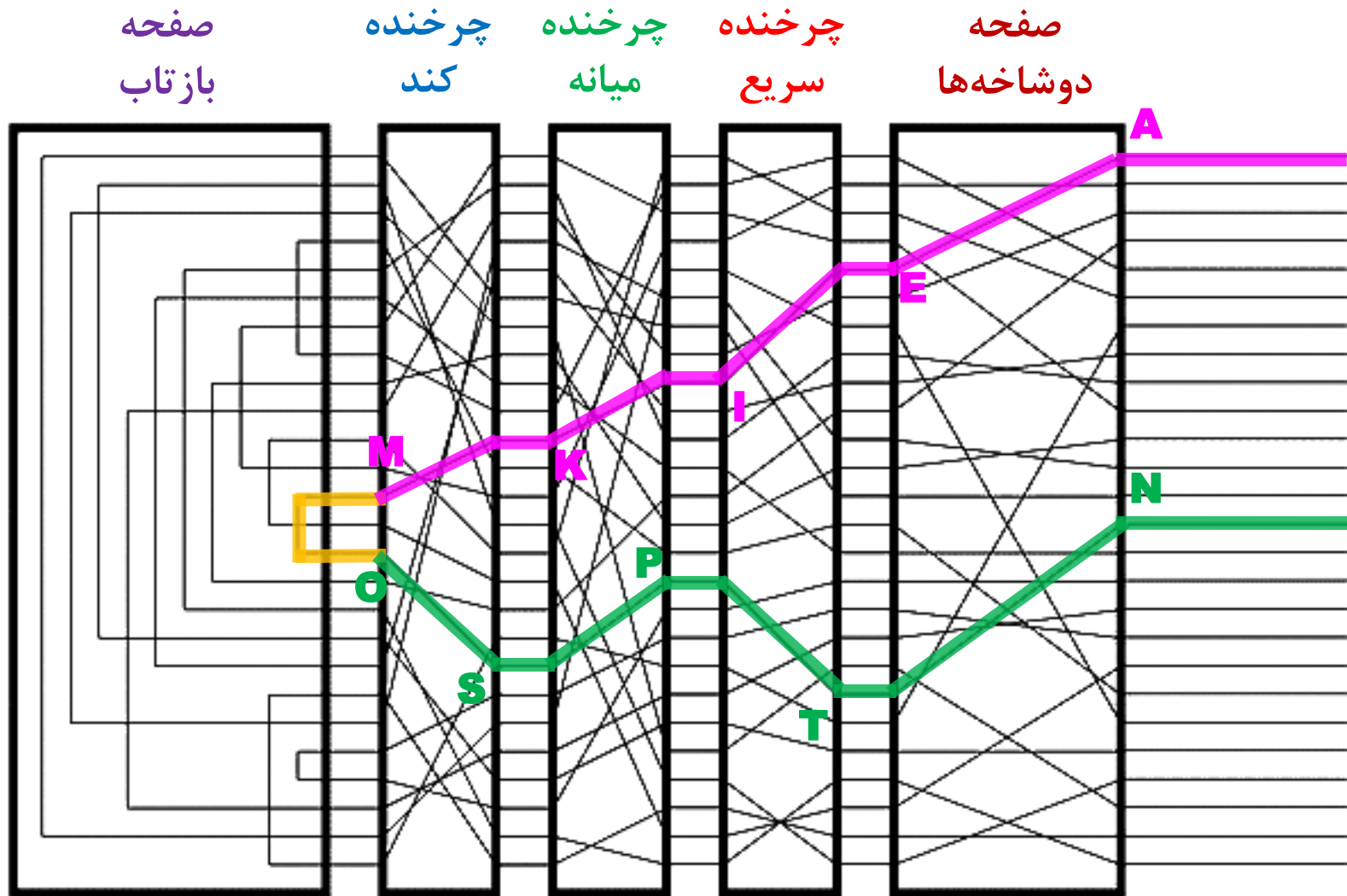
□ با تایپ هر حرف، چرخنده سمت راست (معروف به سریع) یک واحد می‌چرخد.

□ 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 چرخنده‌ها سبب می‌شود که سیم‌بندی تغییر کرده و جریان الکتریکی هر بار به نحو جدیدی هدایت شود.

نحوه عملکرد اینگما



ایجاد پیچیدگی بیشتر در عملکرد انیگما

□ آلمانها هر روز صبح انیگما را با کلید جدیدی پیکربندی می کردند:

☞ انتخاب ۳ چرخنده از بین چرخنده های موجود

☞ تنظیم صفحه دو شاخه ها

□ پیکربندی های هر روز از قبل روی دفترچه کد نوشته شده بود.

☞ با جوهر حل پذیر در آب برای زیر نیروی دریایی!

□ تولید **کلید نشست** برای هر پیام و ارسال آن با کلید اصلی.

تاریخ	موقعیت چرخنده ها	اتصالات صفحه دوشاخه ها
31 .	I II V	BF SD AY HG OU QC WI RL XP ZK
30 .	V IV I	DI ZK RX UH QK PC VY GA SO EM
29 .	III V II	ZM BQ TP YX FK AR WH SO NJ DG
...		

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 پیچیده تر کرد.
- ❑ نسخه های مختلفی از انیگما توسط آلمانها ابداع شد، که پیچیده ترین 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

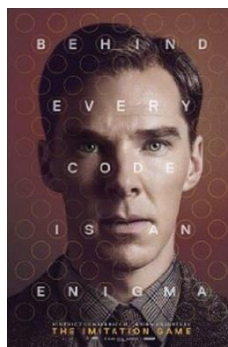
□ ایده‌های آلن تورینگ در ساخت ماشینی برای شکستن انیگما

➡ **حمله واژه محتمل:** انیگما هرگز یک حرف را به خودش نمی‌نگاشت.

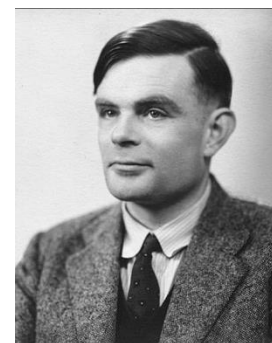
➡ **ماشین برنامه‌پذیر (عام):** شکستن انیگما ظرف ۲۰ دقیقه!



Codebreaker
(2011)



The Imitation
Game (2014)



آلن تورینگ
(۱۹۱۲ تا ۱۹۵۴)

ماشینهای انیگما: تاریخچه – ۴

□ آلمانیها به حدی به کد خود مطمئن بودند که شواهد دال بر لو رفتن کدهای خود را نادیده گرفتند.

□ انگلیس در حد امکان از متنون لو رفته استفاده نمی کرد، تا بتواند آلمانیها 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 می شود.

□ پس از جنگ، به دستور چرچیل تمامی تجهیزات و مستندات پارک بلچلی نابود شد ← از ترس دست یافتن جاسوسان شوروی بر آن!

خلاصه‌ای از ایده‌های تحلیل فراوانی

□ فراوانی ترکیبات حروف

👉 تک حرفی‌ها: e, t, a, o, i, n, s, ...

👉 دو حرفی‌ها: th, he, in, er, an, ...

👉 سه حرفی‌ها: the, ing, and, ion, ent, ...

□ فراوانی ترکیب واژگان: the, of, to, and, a, in, ...

□ حمله واژه محتمل

□ ...

رمزهای هم‌آوایی (Homophonic)

□ برای متوازن ساختن فراوانی حروف

☞ حروف با فراوانی زیاد (مثلاً e) با چند نماد جایگزین می‌شوند.

☞ حروف با فراوانی کم (مثلاً z) با یک نماد جایگزین می‌شوند.

□ نمادها می‌توانند نام اشخاص، موقعیتها، و ... باشند.

□ برخی رمزهای هم‌آوایی از ۵۰,۰۰۰ نماد استفاده می‌کردند!

رمزهای چند نگاری (Polygraphic)

□ حالت ساده: دو نگاری (Digraphic)

👉 جایگزینی دو حرف با دو حرف.

👉 نمونه: رمز Playfair

• ماتریس 5×5 بر اساس کلید و ۴ قانون ساده

□ حالت کلی: جایگزینی چند حرف با چند حرف

👉 نمونه: رمز Hill.

• استفاده از جبر خطی برای رمزنگاری.

□ در تمارین با رمزهای Playfair و Hill آشنا می شوید.

- تعاریف
- حملات علیه رمزنگاری
- رمز کلاسیک - جانشینی
- رمز کلاسیک - جابه جایی

□ جابه‌جایی حروف در متن آشکار

➡ حروف متن رمز همان حروف متن آشکار هستند.

➡ فراوانی حروف متن رمز و متن آشکار دقیقاً یکی است.

➡ نمی‌توان از تحلیل فراوانی استفاده نمود.

رمز پرچین نرده‌ای (Rail Fence Cipher)

□ ساده‌ترین مثال رمز جابه‌جایی

□ متن آشکار از بالا به پایین و به صورت قطری روی نرده‌های 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 جابه‌جایی ستونی (Columnar)

□ متن را بصورت سطری بنویسیم و بصورت ستونی بخوانیم.

👉 **کلید:** تعداد ستون‌ها و ترتیب نوشتن آنها در متن رمز

□ مثال:

👉 **متن آشکار:** «we are discovered; flee at once»

6 3 2 4 1 5

W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E	Q	K	J	E	U

👉 **کلید:** ۶ ستون با ترتیب ۶۳۲۴۱۵

👉 استفاده از padding تصادفی در انتها

👉 **متن رمز:**

EVLNEACDTKESEAQROFOJDEECUWIREE

تقویت رمز جابه‌جایی

□ با دو یا چند بار تکرار رمز جابه‌جایی، معمولاً دشواری شکستن آن افزایش می‌یابد.

WE ARE DISCOVERED FLEE AT ONCE



6 3 2 4 1 5

W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E	Q	K	J	E	U



EVLNEACDTKESEAQROFOJDEECUWIREE



6 3 2 4 1 5

E	V	L	N	E	A
C	D	T	K	E	S
E	A	Q	R	O	F
O	J	D	E	E	C
U	W	I	R	E	E

در بار دوم، کلید
می‌تواند متفاوت
باشد.



EEOEELTQDIVDAJWNKRERASFCEECEOU