



به نام خدا

دانشکده مهندسی برق،
دانشگاه صنعتی شریف

مبانی رمزنگاری و امنیت شبکه



سیستم‌های رمزنگاری کلاسیک

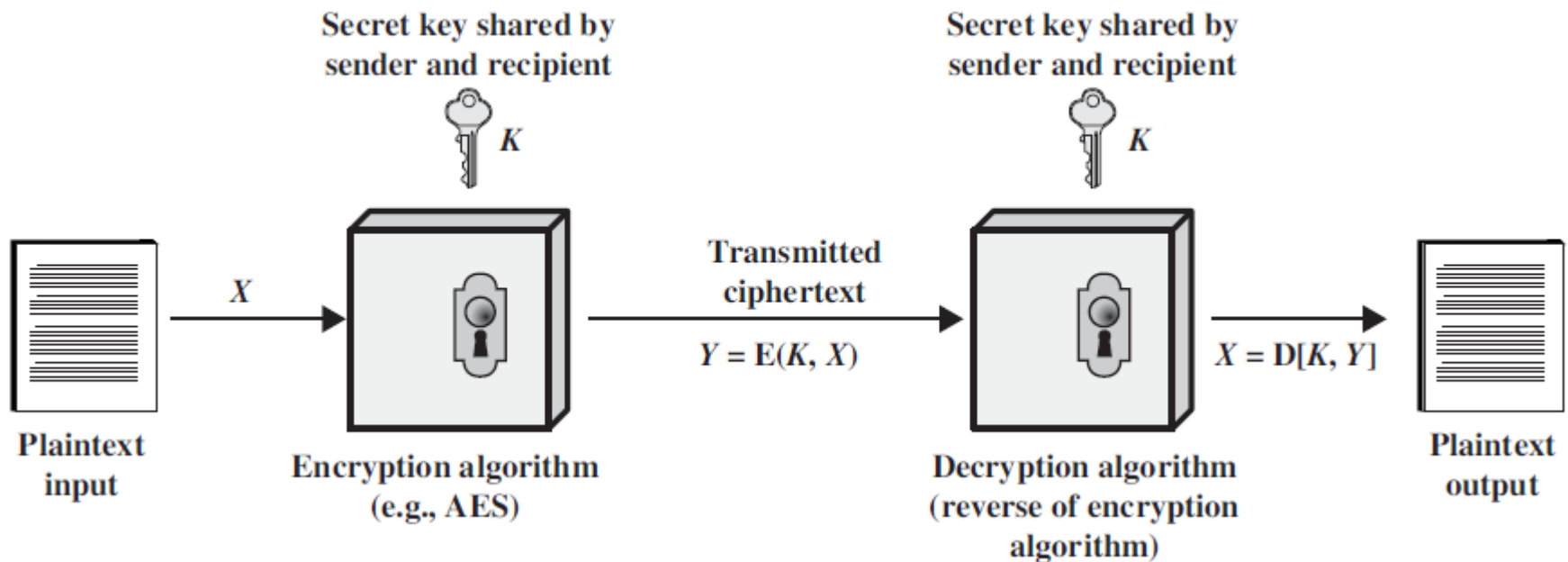
Classic Ciphers and their Cryptanalysis

مهتاب میرمحسنی

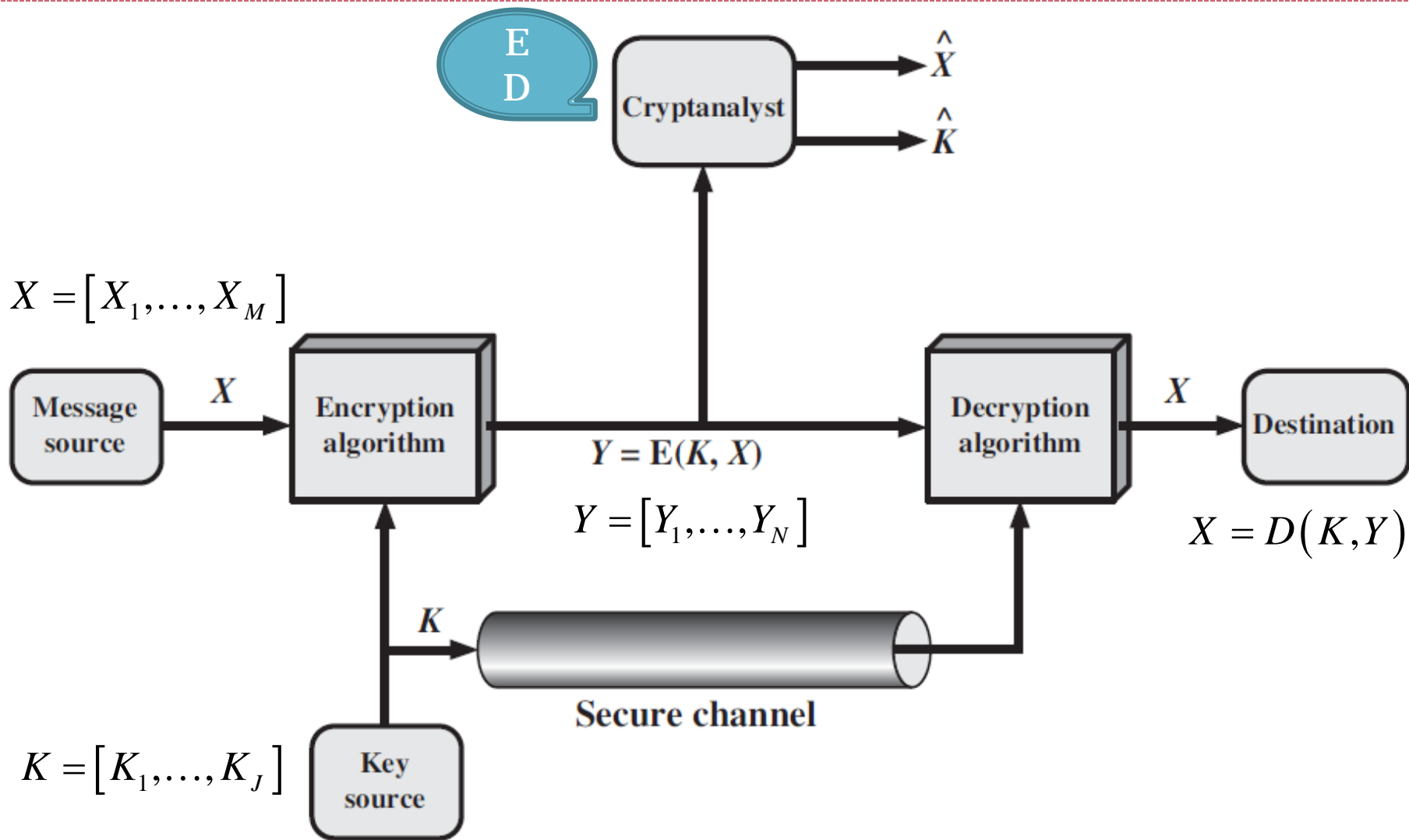
نیم‌سال دوم (بهار) ۹۸-۹۹

سیستم رمز متقارن یا تک کلیدی (Symmetric=One Key)

- کلیدهای رمزگذاری و رمزگشایی یکسان یا به راحتی از روی یکدیگر قابل محاسبه
- رابطه ساده میان تبدیلات رمزگذاری و رمزگشایی
- سیستم‌های رمز کلاسیک از نوع متقارن هستند
- حفاظت کلید



پارامترهای یک سیستم رمزنگاری متقارن (Stalling)



تقسیم‌بندی سیستم‌های رمزنگاری

1. نوع تبدیلات رمزنگاری

- جانشینی (substitution): حروف متن اصلی با حروف دیگر جایگزین می‌گردد
- جابجایی (transposition): محل قرار گرفتن حروف در متن رمز شده نسبت به متن اصلی تغییر می‌کند

2. تعداد کلیدها

- سیستم رمز متقارن یا تک کلیدی (Symmetric=One Key)، رمزهای کلاسیک
- سیستم نامتقارن یا دو کلیدی (Asymmetric=Two Key)، رمز کلیدهمگانی Public key

3. نحوه پردازش متن اصلی

- رمز قالبی (Block cipher)
- رمز جریانی (Stream cipher)

انواع حمله‌ها

- رمزشکنی (تحلیل رمز): Cryptanalysis

- مشخصه الگوریتم

- ✦ ساختار متن اصلی - کلید

- حمله فقط با متن رمز (Ciphertext Only Attack)

- حمله متن اصلی معلوم (Known Plaintext Attack)

- حمله متن اصلی منتخب (Chosen Plaintext Attack)

- حمله متن رمز منتخب (Chosen Ciphertext Attack)

- حمله متن منتخب (Chosen Text Attack)

- حمله جستجوی فراگیر: Brute-force attack

- آزمودن تمام کلیدهای ممکن (Exhaustive Key Search)

- فرض: متن اصلی قابل شناسایی است

- به طور متوسط نیمی از کلیدها باید آزموده شود

حمله جستجوی فراگیر

Brute-force attack

	Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/ μs	Time Required at 10^6 Decryptions/ μs
DES	32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu s = 35.8$ minutes	2.15 milliseconds
	56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu s = 1142$ years	10.01 hours
AES	128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
3-DES	168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
	26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

**Substitution
code**

الگوریتم‌های رمز کلاسیک

- جانشینی (substitution)

- حروف متن اصلی با حروف دیگر جایگزین می‌گردد

- تک حرفی

- ✦ تک الفبایی

- ✦ چند الفبایی

- چند حرفی

- جابجایی (transposition)

- هیچ حرفی تغییر شکل نمی‌دهد و محل قرار گرفتن آن در متن رمز شده نسبت به

- متن اصلی تغییر می‌کند

رمز جانشینی تک حرفی

- رمز جانشینی ساده:

- هر حرف به یک حرف دیگر توسط یک رابطه یک به یک تبدیل می‌شود
- کلید این سیستم الگوریتم تبدیل است

- رمز سزار (Caesar Cipher)

- به جای هر حرف، حرفی که به فاصله ۳ حرف بعد از آن قرار دارد، انتخاب و ارسال می‌شود
- رمزگشا، به جای هر حرف دریافتی، حرفی را که ۳ کلمه قبل از آن است انتخاب می‌کند

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

○ مثال:

plain	c	r	y	p	t	o	g	r	a	p	h	y
cipher	F	U	B	S	W	R	J	U	D	S	K	B

رمز سزار (ادامه)

- به هر حرف یک عدد اختصاص دهیم:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

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

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

رمز انتقال الفبا ((Direct Standard Alphabet (DSA)

- رمز سزار (کلی)
- هر حرف به اندازه K به سمت راست انتقال می یابد
- $C=E(K,p)=(p+K) \bmod n \quad (n=26)$
- $p=D(K,C)=(C-K) \bmod n \quad (n=26)$
- فاصله قابل شکست
 - کلید ۲۶ عضو دارد
 - انتخاب هر عضو کلید با احتمال مساوی صورت پذیرد
- هر عدد می تواند به عنوان کلید انتخاب شود
 - بزرگتر از ۲۶ ← هم نهشت آن در پیمانه ۲۶

$$N_0 = \frac{H(K)}{D} = \frac{\log 26}{3.2} \simeq 1.47$$

شکستن رمز DSA

- حالت اول: دشمن نوع سیستم را می‌شناسد
 - : الگوریتم رمزگذاری و رمزگشایی معلوم ← مجهول: کلید
 - کافی است یک کلمه کوتاه را بشکنیم

BPM VMOWBQIBQWVA NWZ I AMBBTMUMVB WN BPM ABZQSM
IZM IB IV QUXIAAM ZMKWUUMVL EM QVKZMIAM WCZ WNNMZ

K=	1	0	14	11	A	O	L	○ $1, 15, 12 = \text{BPM}$
	2	25	13	10	Z	N	K	
	3	24	12	9	Y	M	J	
	4	23	11	8	X	L	I	
	5	22	10	7	W	K	H	
	6	21	9	6	V	J	G	
	7	20	8	5	U	I	F	
	8	19	7	4	T	H	E	

KEY		PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1		oggv	og	chvgt	vjg	vqic	rctva
2		nffu	nf	bgufs	uif	uphb	qbsuz
3		meet	me	after	the	toga	party
4		ldds	ld	zesdq	sgd	snfz	ozqsx
5		kccr	kc	ydrpc	rfe	rmey	nyprw
6		jbbq	jb	xcqbo	qeb	qldx	mxoqv
7		iaap	ia	wbpan	pda	pkcw	lwnpu
8		hzzo	hz	vaozm	ocz	objv	kvmot
9		gyyn	gy	uznyl	nby	niau	julns
10		fxxm	fx	tymxk	max	mhzt	itkmr
11		ewwl	ew	sxlwj	lzw	lgys	hsjql
12		dvvk	dv	rwkvi	kyv	kfxr	grikp
13		cuuj	cu	qvjuh	jxu	jewq	fqhjo
14		btti	bt	puirg	iwt	idvp	epgin
15		assh	as	othsf	hvs	hcuo	dofhm
16		zrrg	zr	nsgre	gur	gbtn	cnegl
17		yqqf	yq	mrfqd	ftq	fasm	bmdfk
18		xppe	xp	lqepc	esp	ezrl	alcej
19		wood	wo	kpdob	dro	dyqk	zkbdj
20		vnnc	vn	jocna	cqn	cxpj	yjach
21		ummb	um	inbmz	bpm	bwoi	xizbg
22		tlla	tl	hmaly	aol	avnh	whyaf
23		skkz	sk	glzqx	znk	zumg	vgxze
24		rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25		qiix	qi	ejxiv	xli	xske	tevxc

شکستن رمز DSA

• حمله جستجوی فراگیر:

- ۲۵ کلید ممکن ← به سادگی می‌شکند
- الگوریتم رمزگذاری و رمزگشایی معلوم
- زبان متن اصلی قابل فهم

• زبان متن اصلی قابل فهم

○ مثالی از متن فشرده شده ZIP

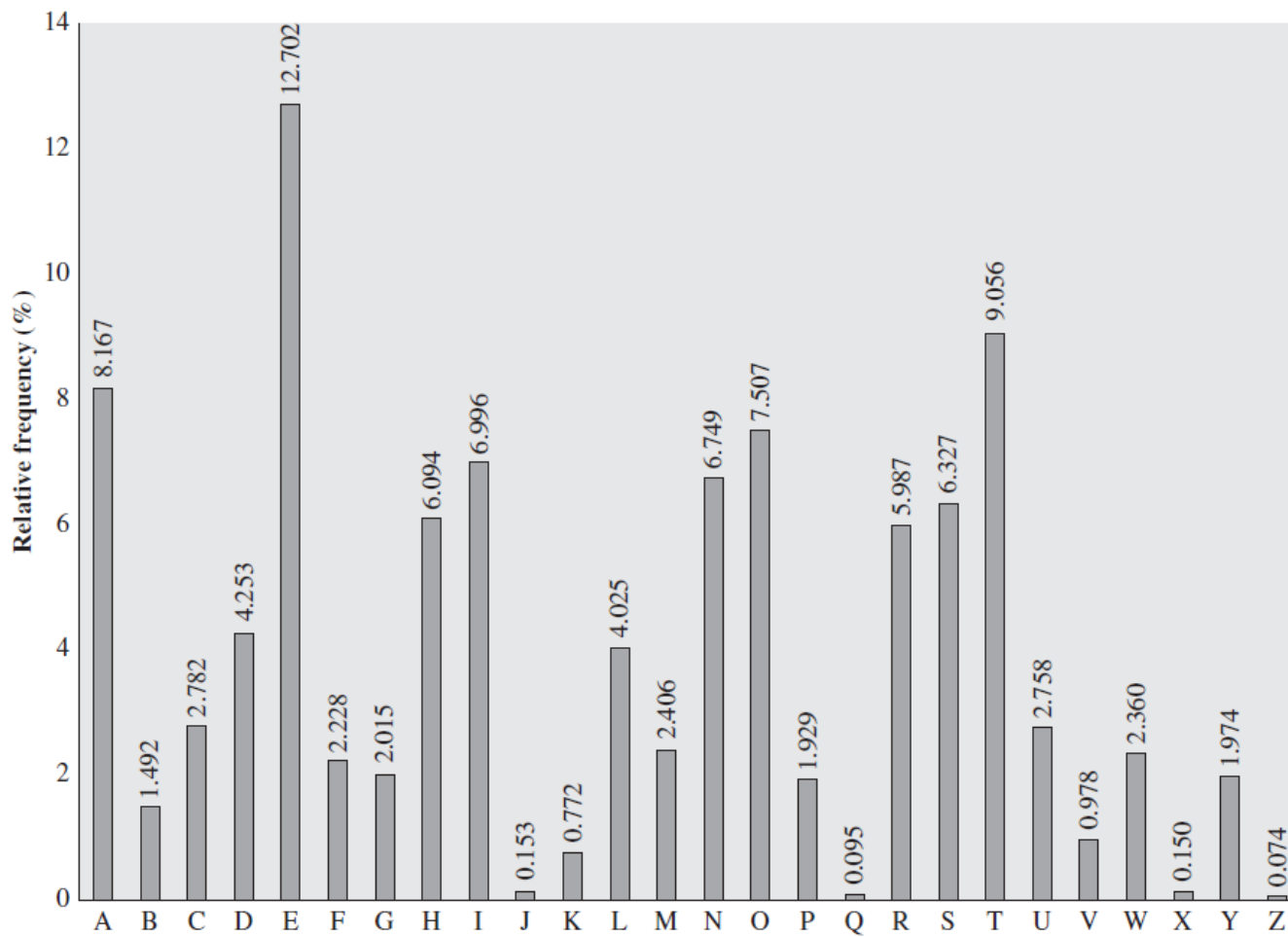
```
~+Wµ"— Ω-0)≤4{∞‡, ë~Ω%ràu.-í ◇-z-
Ú≠2Ô#Åæð æ«q7,Ωn.®3NÔÚ Œz'Y-f∞Í[±û_ èΩ,<NO-±«~xă Ääfèü3Å
x}ö§k°Â
_yÍ ^ΔÉ] ,¤ J/'iTê&1 'c<uΩ-
ÄD(G WÄC~y_iöÄW PÔ1«îÜ†ç],¤;~î^üÑπ~≈~L~9OgflO~&Œ≤ -≤ ØÔ§":
~Œ!SGqèvo^ ú\,S>h<-*6ø‡%x'~|fiÓ#≈~my%~≥ñP<,fi Áj ÅÔ¿"Zù-
Ω"Ö-6Œÿ{% „ΩÊó ,ï π÷Áî"ú02çSÿ'0-
2Äflßi /@^"ΠK°=PŒπ,úé^'3Σ~ö~ÔZÌ"Y-ÿΩæY> Ω+eô/'<Kf¿*÷~"≤û~
B ZøK~Qßÿüf,!òflîzssS/]>ÈQ ü
```

شکستن رمز DSA

- حالت دوم: در حمله نوع اول نوع سیستم نامعلوم باشد و یا حمله جستجوی فراگیر به دلیل افزایش اندازه فضای کلید ممکن نباشد (سیستم‌های جانشینی تک الفبایی کلی با 26! کلید)
 - بر اساس مشخصات آماری زبان
 - در عمل به این نتیجه می‌رسد که رمز از نوع جانشینی ساده و انتقال حروف بوده ✨ به سادگی می‌شکند

$$\sum_{i=A}^Z p_i = 1$$

- فرکانس نسبی حروف: احتمال وقوع حروف
 - هرچه متن طولانی‌تر باشد، دقت اندازه‌گیری فرکانس نسبی بیشتر است
 - وابسته به عواملی چون موضوع متن، سبک نگارش و ...



• فرکانس پایین: P, F, Y, W, G, B, V
 • نادر: J, K, Q, X, Z

• بالاترین فرکانس: E
 • فرکانس بالا: T, A, O, N, I, R, S, H
 • فرکانس متوسط: D, L, U, C, M

فرکانس مشخصه (characteristic frequency)

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
≠	-	≡	≡	≠	≡	=	≡	≠			≡	=	≠	≠	=		≠	≠	≠	≡	-	=		=	
=				≠				=					≡	=			≡	-	≡						
				≡																					

- بالاترین فرکانس نسبی: E
- سه حرف فرکانس بالا (A,E,I) به فاصله ۴ از یکدیگر قرار دارند
- دو حرف فرکانس بالای (N,O) کنار یکدیگر قرار دارند
- سه حرف فرکانس بالای (R,S,T) نیز کنار یکدیگر قرار دارند
- پنج حرف فرکانس پایین (V,W,X,Y,Z) به دنبال یکدیگر آمده‌اند
- اگر متن با DSA رمز شود: این نمودار فقط به اندازه K شیف می‌یابد

شکستن رمز DSA

- اگر در حمله نوع اول نوع سیستم نامعلوم باشد
 - رسم شمای فرکانس نسبی حروف
 - در صورت مشابهت با شمای اصلی زبان ← سیستم از نوع DSA است ← کلید ← رمز می‌شکند
 - در همان مثال:

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
\neq	\neq	-		-				\neq		=	-	\neq	\equiv	-	=	\neq		-	-	\equiv	\neq	\neq	-		\neq
-	\equiv							=				\neq									-	=			=
												\neq													
												\neq													

- بالاترین فرکانس نسبی: M
 - سه حرف فرکانس بالا (M,Q,I) به فاصله ۴ از یکدیگر قرار دارند
 - دو حرف متوالی (V,W) فرکانس بالا هستند
 - سه حرف متوالی (Z,A,B) فرکانس بالا هستند
 - پنج حرف متوالی (C,D,E,F,G,H) فرکانس پایین هستند
- $$E_p = M_c$$
- $$\Rightarrow 12 = 4 + K \bmod 26$$
- $$\Rightarrow K = 8$$

رمز جانشینی ساده ضربی (Multiplication)

- به منظور پیچیده‌تر کردن رمز: کلید را در معادل عددی حرف ضرب می‌کند
- $C = E(K, p) = pK \bmod n$ (n = تعداد حروف الفبا)
- رمزگشایی بدون ابهام: تبدیل یک به یک
- جایگشتی از مجموعه کامل مانده‌ها: $(K, n) = 1 \rightarrow pK \bmod n$

$$n = 26 \rightarrow N_0 = \frac{H(K)}{D} = \frac{\phi(26) - 1}{3.2} = \frac{\log 12}{3.2} \approx 1.12$$

- $K=3$

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

شکستن رمز جانشینی ساده ضربی

VNY BYRVEIWR BLYDYLQ VNEV OWRQOLSBVSWRQ TALSRI
VNY RYPV VNLYY MWRVNQ JY METY SR VNY EIY JLEOCYVQ
RSRYVYYR VW VKYRVU WRY

• مثال:

• فرض: حروف از ۱ تا ۲۶ شماره گذاری شده اند

• نمودار فرکانس مشخصه متن

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
-	≡	-	-	≠				≡	=	-	≠	=	≠	≡	-	≠	≠	≠	=	-	≠	≠		≠	
											-	-				≠	≠	≠			≠	-		≠	
																≡					≠			≠	
																					≠			≠	
																								≡	

• ویژگی های DSA را ندارد

• فرض: ضربی

$$Y_c = E_p, \quad V_c = T_p \text{ or } R_c = T_p$$


$$\begin{cases} Y_c = E_p \\ V_c = T_p \end{cases} \Rightarrow VNY = ? THE$$

• VNY:

شکستن رمز جانشینی ساده ضربی (ادامه)

• بدست آوردن کلید:

$$\begin{cases} T_p = 20 \rightarrow V_c = 22 \rightarrow 20K \equiv 22 \pmod{26} & \times \\ H_p = 8 \rightarrow N_c = 14 \rightarrow 8K \equiv 14 \pmod{26} & \times \\ E_p = 5 \rightarrow Y_c = 25 \rightarrow 5K \equiv 25 \pmod{26} & \rightarrow K = 5 \end{cases}$$



THE PENTAGON PREFERS THAT CONSCRIPTIONS DURING
THE NEXT THREE MONTHS BE MADE IN THE AGE BRACKETS
NINETEEN TO TWENTY ONE.

- روش فوق: حدس قسمتی از متن اصلی و تعمیم آن
- روش صرفا توزیع فرکانس: حروف فرکانس پایین متوالی و حروف فرکانس بالای متوالی (فواصل حروف در عدد ثابت K ضرب می شوند)

رمز جانشینی ساده بر اساس ترکیب خطی (مستوی): affine

- $C = pK_1 + K_2 \bmod n$

- حمله: توزیع فرکانسی ← حل معادلات هم‌نهشتی برای یافتن K_1 و K_2

$$\|K\| = n\phi(n)$$

$$n = 26 \rightarrow N_0 = \frac{H(K)}{D} = \frac{\log(12 \times 26)}{3.2} \simeq 1.47 + 1.12 = 2.59$$

- ایمنی تقریباً برابر با رمز ضربی

- مشکل اصلی: با دانستن ارتباط یک یا دو حرف از متن اصلی و متن رمز شده، رمز می‌شکند

- سوال: ارتباط تصادفی با کلید ساده؟

رمز تک الفبایی (Monoalphabetic Ciphers)

- جانشینی تصادفی

- رمز تصادفی: همه جایگشت‌های (permutation) ممکن در سطر رمز (الفبا مخلوط)

- تعداد کلیدها $= 4 \times 10^{26} > 26!$ ← مشکل مدیریت کلید

- رمزگذار و رمزگشا روی یک کلمه (یا عبارت) توافق می‌کنند

- با نوشتن کلمه کلید (بدون حروف تکراری) و بقیه حروف به دنبال کلمه کلید، الفبا رمز بدست می‌آید

- مثال: کلید = INDEPENDENCE

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

- شکستن رمز: مشکل‌تر از حالت قبل است ولی با استفاده از ساختار زبان می‌شکند

شکستن رمز تک الفبایی الفبا مخلوط

UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX
 UDBMETSX AIZ VUEPHZ HMDZSHZO WSFP APPD TSVP
 QUZW YMXUZUHSX EPYEPOPDZSZUFPO MB ZWP FUPZ
 HMDJ UD TMOHMQ

- متن رمز شده

- ابتدا جدول توزیع فرکانسی حروف:

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

- توزیع با انتقال روی توزیع نرمال قرار نمی گیرد ← سیستم DSA نیست
- با بررسی حروف فرکانس بالا یا پایین متوالی می توان دید که الگوریتم از نوع خطی نیست

فرض: الفبا مخلوط

شکستن رمز تک الفبایی الفبا مخلوط (ادامه مثال)

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

1. مشخص کردن حروف فرکانس بالا و پایین

○ حدس:

$$\{P, Z\}_c = \{E, T\}_p$$

$$\{A, B, G, I, J, Q, T, Y\}_c = \{G, J, K, Q, V, W, X, Y, Z\}_p$$

$$\{H, M, O, S, U\}_c = \{A, I, N, O, R, S\}_p$$

○ فرکانس نسبی حروف شروع و پایان در کلمات

شکستن رمز تک الفبایی الفبا مخلوط (ادامه مثال)

• بررسی آماری

تعداد کلمات	حرف شروع
2614	T
1802	A
1213	S
1176	O
922	I
918	C
833	W
768	P
757	B
666	F

تعداد کلمات	حرف پایانی
3325	E
2077	S
1649	D
1592	N
1687	T
906	R
903	Y
745	F
744	O
599	L

$$\begin{cases} Z_c = T_p \\ P_c = E_p \end{cases}$$

شکستن رمز تک الفبایی الفبا مخلوط (ادامه مثال)

2. تشخیص حروف صدا دار از بی صدا

ویژگی ساختاری: در هر کلمه حداقل یک حرف صدا دار داریم

کلمات ۲، ۳ یا ۴ حرفی

$$\begin{cases} M_c B_c \rightarrow M_c : \text{frequent} \rightarrow \text{vowel} \\ U_c D_c \\ U_c Z_c \end{cases}$$

$$\begin{cases} U_c D_c \\ U_c Z_c \end{cases} \rightarrow \begin{cases} U_c : \text{vowel} \\ \text{or} \\ D_c \text{ and } Z_c : \text{vowel} \end{cases} \Rightarrow \begin{cases} BY, BE \\ \text{or} \\ MY, ME \end{cases} \Rightarrow \begin{cases} U_c = B_p \\ \text{or} \\ U_c = M_p \end{cases}$$

$$Z_c W_c P_c \rightarrow W_c \text{ or } P_c \rightarrow P_c : \text{frequent} \rightarrow \text{vowel}$$

شکستن رمز تک الفبایی الفبا مخلوط (ادامه مثال)

- استناد به نمادهای موجود در زبان مانند ساختمان خاص کلمات، تکرار حروف در کلمات

$$\begin{cases} Z_c = T_p \\ P_c = E_p \end{cases} \quad \dots \text{و}$$

○ کلماتی مثل: THE ،WHERE ،WHICH ،THAT

$$(ZWP)_c \leftrightarrow (T?E)_p \Rightarrow W_c = H_p$$

فرکانس متوسط

$$(ZWSZ)_c \leftrightarrow (TH?T)_p \Rightarrow S_c = A_p$$

فرکانس بالا

$$(WSFP \text{ APPD})_c \leftrightarrow (HA?E?EE?)_p \Rightarrow HAVE \text{ BEEN} \Rightarrow \begin{cases} F_c = V_p \\ A_c = B_p \\ D_c = N_p \end{cases}$$

$$\begin{cases} (UZ)_c \leftrightarrow (?T)_p \\ (UD)_c \leftrightarrow (?N)_p \end{cases} \Rightarrow U_c = I_p \text{ or } A_p \Rightarrow U_c = I_p$$

شکستن رمز تک الفبایی الفبا مخلوط (ادامه مثال)

UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX
UDBMETSX AIZ VUEPHZ HMDZSHZO WSFP APPD TSVP
QUZW YMXUZUHSX EPYEPOPDZSZUFPO MB ZWP FUPZ
HMDJ UD TMOHMQ

- متن رمز شده

it was disclosed yesterday that several informal but direct
contacts have been made with political representatives of the
viet cong in moscow

- متن اصلی

شکستن رمز تک الفبایی الفبا مخلوط

- اطلاعات فاصله

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- قابل شکست

○ فرکانس نسبی دو حرفی‌ها (Digram)، سه حرفی‌ها و ...

- محتمل‌ترین دو حرفی: TH

$$(ZW)_c \leftrightarrow (TH)_p$$

- Stallings, sec. 2.2

رمز تک حرفی (Homophonic)

- تک الفبایی: قابل شکست

○ تبدیل یک به یک ← حفظ فرکانس نسبی حروف

- حل: استفاده از تبدیلات یک به چند

○ آشکارسازی بدون ابهام: از هر سمبل یک بار استفاده کنیم

$$100 \text{ symbols : } \{00, 01, \dots, 99\} \Rightarrow \begin{cases} E : 13 \text{ symbols} \\ T : 9 \text{ symbols} \end{cases} \dots$$

- انتخاب سمبلها تصادفی و متناسب با فرکانس نسبی حروف

○ توزیع فرکانسی نسبی تک حرفیها یکنواخت

Carl Friedrich Gauss ○

رمز تک حرفی Homophonic

- هر عنصر متن اصلی تنها بر روی یک عنصر متن رمز شده تاثیر می گذارد و یا هر هر عنصر متن رمز شده تنها از یک عنصر متن اصلی تاثیر می پذیرد
 - توزیع فرکانس نسبی دو حرفی ها (Digram)، سه حرفی ها و ... همانند متن اصلی باقی می ماند و در نتیجه قابل شکست است
 - مدیریت کلید پیچیده تر
- حل: بر هم زدن ساختار زبان
 - رمز چند الفبایی Polyalphabetic substitution Ciphers
 - رمز چند حرفی Polygraphic substitution Ciphers

رمز جانشینی چند الفبایی (Polyalphabetic substitution Ciphers)

- هدف: برهم زدن ساختار زبان (فرکانس نسبی حروف)

1. مجموعه‌ای از رمزهای جانشینی تک الفبایی به کار می‌رود
2. کلید (به طول d) مشخص می‌کند کدام رمز تک الفبایی به کار رفته است

- هر حرف به تعدادی سمبل تبدیل می‌شود
- هر سمبل از متن رمز شده متعلق به بیش از یک سمبل در متن اصلی است
- آشکارسازی بدون ابهام:
 - سمبل رمز شده و محل قرار گرفتن آن در متن به طور یکتا سمبل متن اصلی متناظر را بیان می‌کنند
 - فاصله قابل شکست d برابر رمز تک الفبایی

رمز جانشینی چند الفبایی (Polyalphabetic substitution Ciphers)

- سیستم‌های جانشینی متناوب با دوره تناوب d (طول کلید)
- اگر M الفبای متن اصلی و C_1, \dots, C_d الفبای مختلف رمز شده باشند:
$$f_i : M \rightarrow C_i, \quad i = 1, \dots, d$$
- در این صورت پیام $M = m_1 \cdots m_d m_{d+1} \cdots m_{2d} \cdots$ به صورت زیر رمز می‌شود:
$$E_k(M) = f_1(m_1) f_2(m_2) \cdots f_d(m_d) f_1(m_{d+1}) \cdots f_d(m_{2d}) \cdots$$
- اگر $d=1$: رمز جانشینی تک‌الفبایی

Vigenère cipher

- رمز چند الفبایی با کلید $K = K_1 \cdots K_d$
- زیرسیستم‌های تک الفبایی: DSA (سزار کلی)

$$C_i = f_i(p) = (p_i + K_i) \bmod 26 \quad i = 1, \dots, d$$

$$C_i = f_i(p) = (p_i + K_{i \bmod d}) \bmod 26, \quad K_0 = K_d$$

key:	<i>deceptivedeceptivedeceptive</i>
plaintext:	<i>wearediscoveredsaveyourself</i>
ciphertext:	<i>ZICVTWQNGRZGVTWAVZHCQYGLMGJ</i>

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

جدول رمز Vigenère

		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

فاصله قابل شکست رمز Vigenère

- تعداد کل کلیدها 26^d

○ با صرفنظر از نامناسب بودن برخی کلیدها

○ احتمال انتخاب یکسان

$$N_0 = \frac{H(K)}{D} = \frac{\log(26^d)}{3.2} = d \frac{\log(26)}{3.2} \approx 1.47d$$

- رمز گشایی: سطرهای متناظر کلید در جدول Vigenère

- شکستن رمز چند الفبایی: ابتدا بدست آوردن دوره تناوب (طول کلید d)

○ هر حرف متن رمز شده می تواند بیان گر یکی از d حرف ممکن در متن اصلی باشد

○ کلمات تکراری به یک کلمه رمز نمی شوند، مگر آن که فاصله آن ها در متن اصلی مضربی از دوره تناوب (d) باشد.

○ فرکانس نسبی هر حرف در متن رمز شده = متوسط فرکانس نسبی d حرف

شکستن رمز چند الفبایی

APWVC	DKPAK	BCECY	WXBBK	CYVSE	FVTLV	MXGRG	KKGFD	LRLZK
TFVKH	SAGUK	YEXSR	SIQTW	JXVFL	LALUI	KYABZ	XGRKL	BAFSJ
CCMJT	ZDGST	AHBJM	MLGEZ	RPZIJ	XPVGU	OJXHL	PUMVM	CKYEX
SRSIQ	KCWMC	KFLQJ	FWJRH	SWLOX	YPVKM	HYCTA	WEJVQ	DPAVV
KFLKG	FDLRL	ZKIWT	IBXSG	RTPLL	AMHFR	OMEMV	ZQZGK	MSDFH
ATXSE	ELVWK	OCJFQ	FLHRJ	SMVMV	IMBOZ	HIKRO	MUHIE	RYG



• توزیع فرکانسی حروف

• هموارتر از توزیع الفبای نرمال

• اطمینان از بکارگیری رمز چندالفبایی با استفاده از محاسبه اندازه ناهمواری
توزیع (Measure of Roughness) و ضریب انطباق (Index of Coincidence)

تشخیص دوره تناوب d

روش Kasiski

- کلمات تکراری به یک کلمه رمز نمی‌شوند، مگر آن که فاصله آن‌ها در متن اصلی مضربی از دوره تناوب (d) باشد
 - اگر متن رمز شده را در تعداد d ستون قرار دهیم
 - حروف هر ستون با یک کلید ثابت رمز شده‌اند
 - اگر کلمات تکراری در ستون مشابه قرار گیرند، متن رمز شده یکسان است ← فاصله تکرار مضربی از دوره تناوب (d)
 - در متن رمز شده به دنبال کلمات تکراری می‌گردیم ← با محاسبه فاصله بین کلمات تکراری و تعیین مقسوم علیه مشترک میان فاصله‌ها، دوره تناوب را پیش‌بینی می‌کنیم
- با دانستن دوره تناوب، d سیستم جانشینی تک الفبایی داریم که قابل شکستن است

بهبود رمز Vigenère

- استفاده از رمز تک الفبایی با کلید مخلوط به جای رمز DSA (سزار کلی)

✓ شکستن

- تعیین دوره تناوب (d)

- پیچیده‌تر از گذشته: قرار نگرفتن حروف هر ستون در متن اصلی در کنار هم (بررسی دوحرفی‌ها، ...)، کم بودن تعداد حروف در هر ستون

- انطباق الفباها

○ با فرض این که همه ستون‌ها از یک نوع تک الفبایی (با انتقال) بوده است. یعنی کلید انتقال در میان الفباها را مشخص می‌کند

- سیستم‌های پیچیده‌تر چندالفبایی نیز با تحلیل فرکانس نسبی حروف می‌شکند!

رمز جانشینی چندحرفی (Polygraphic)

- Multiple-letter cipher
- هدف: برهم زدن خواص آماری حروف متن اصلی
- هر n حرف از متن اصلی به عنوان یک واحد در نظر گرفته شده و به طور یک جا و با یک تبدیل به n حرف از متن رمز شده تبدیل می شود
- $n=2$: رمز دوحرفی (digraphic)
- جدول دو حرفی های ممکن: $26 \times 26 = 676$
- $$N_0 = \frac{\log(676!)}{3.2} \simeq 1700$$
- دو نوع مهم: رمز Playfair و رمز Hill

رمز Playfair

- ۲۵ حرف از حروف زبان انگلیسی (به جز J) در یک جدول 5×5 درج می گردند

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

○ تصادفی

○ با استفاده از کلید : monarchy

- حرف P_1P_2 از متن اصلی به صورت زیر رمز می شود:

1. اگر $P_1 = P_2$ باشد، یک حرف مجازی (X) بین آنها قرار می گیرد

2. اگر P_1P_2 متعلق به یک سطر باشند، C_1C_2 حروف بعد از P_1P_2 در همان سطر است.

حرف بعد از ستون آخر، ستون اول خواهد بود: $AR \rightarrow RM$

3. اگر P_1P_2 متعلق به یک ستون باشند، C_1C_2 حروف پایین P_1P_2 در همان ستون است.

حرف پایین سطر آخر، سطر اول خواهد بود $MU \rightarrow CM$

4. اگر P_1P_2 در دو راس متقابل یک مستطیل قرار گیرند، C_1C_2 دو راس دیگر این $HS \rightarrow BP$

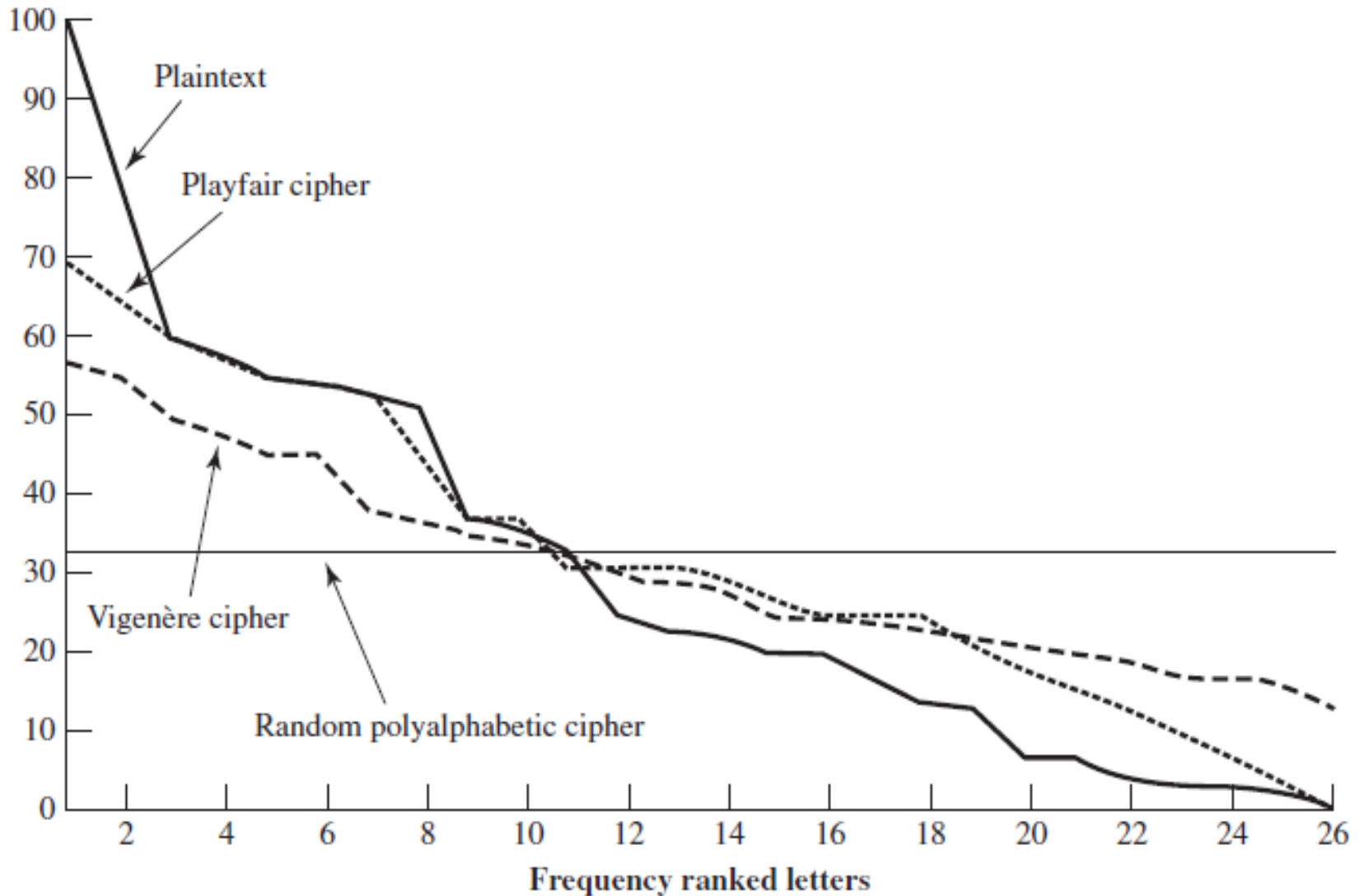
مستطیل خواهند بود. C_1, P_1 در یک سطر و C_2, P_2 در سطر دیگر قرار دارند $EA \rightarrow IM$

5. اگر تعداد کل حروف متن اصلی فرد باشد، یک حرف مجازی به آخر متن اضافه می شود

شکستن رمز Playfair

- دو حرفی‌های ممکن: $26 \times 26 = 676$
- تحلیل فرکانسی مشکل‌تر
- تا مدت‌ها غیر قابل شکست به نظر می‌رسید
 - سیستم رمز استاندارد در جنگ‌های جهانی اول و دوم
- با استفاده از چند صد حرف متن رمز شده می‌شکند!
 - ساختار آماری متن اصلی تا حدود زیادی حفظ می‌شود

فرکانس نسبی وقوع حروف



مروری بر ماتریس معکوس

- دو ماتریس A و B را معکوس یکدیگر گویند، هرگاه حاصلضرب آنها برابر ماتریس واحد گردد: $AB=BA=I$

$$A = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} \quad A^{-1} \bmod 26 = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$$

$$\begin{aligned} AA^{-1} &= \begin{pmatrix} (5 \times 9) + (8 \times 1) & (5 \times 2) + (8 \times 15) \\ (17 \times 9) + (3 \times 1) & (17 \times 2) + (3 \times 15) \end{pmatrix} \\ &= \begin{pmatrix} 53 & 130 \\ 156 & 79 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

- در پیمانه ۲۶

○ برای محاسبه معکوس دترمینان، می‌بایست دترمینان نسبت به ۲۶ اول باشد

$$\det \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} = (5 \times 3) - (8 \times 17) = -121 \bmod 26 = 9$$

$$9^{-1} \bmod 26 = 3$$

$$A^{-1} \bmod 26 = 3 \begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix} = 3 \begin{pmatrix} 3 & 18 \\ 9 & 5 \end{pmatrix} = \begin{pmatrix} 9 & 54 \\ 27 & 15 \end{pmatrix} = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$$

مروری بر ماتریس معکوس (ادامه)

- برای سادگی در عمل رمزگذاری و رمزگشایی می توان از ماتریس هایی استفاده کرد که معکوس شان با خودشان برابرند (یا دوره تناوب ۲ دارند):

$$M^2 = I$$

$$M = \begin{pmatrix} 2 & 3 \\ 25 & 24 \end{pmatrix} \rightarrow M^2 = \begin{pmatrix} 79 & 78 \\ 650 & 651 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\det(M) = 1 \text{ or } 25 \bmod 26$$

رمز Hill

- این روش هر m حرف متن اصلی را با هم در نظر گرفته و برای بدست آوردن m حرف معادل متن رمز شده از m ترکیب خطی (معادل عددی) حروف متن اصلی استفاده می شود

• $m=3$

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$$

$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$$

$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26$$

$$(c_1 \ c_2 \ c_3) = (p \ p_2 \ p_3) \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

$$\mathbf{C} = \mathbf{PK} \bmod 26$$

مثال رمز Hill

- متن اصلی: paymoremoney

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

$$pay \rightarrow (15 \ 0 \ 24)$$

$$\Rightarrow (15 \ 0 \ 24)\mathbf{K} = (303 \ 303 \ 531) \bmod 26 = (17 \ 17 \ 11) \rightarrow RRL$$

- متن رمز شده: RRLMWBKASPDH

- هر حرف رمز شده تابعی از m حرف متناظر در متن اصلی است و اگر یک حرف در متن اصلی تغییر یابد، m حرف در متن رمز شده تغییر می یابند
○ در $m=3$ ، فرکانس تک حرفی و دو حرفی ها مخفی شده

رمز Hill (ادامه)

$$\mathbf{C} = E(\mathbf{K}, \mathbf{P}) = \mathbf{PK} \bmod 26$$

• رمز گذاری

$$\mathbf{P} = D(\mathbf{K}, \mathbf{C}) = \mathbf{CK}^{-1} \bmod 26 = \mathbf{PKK}^{-1} \bmod 26 = \mathbf{P}$$

• رمز گشایی

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

$$\det(\mathbf{K}) = 23 \rightarrow (\det(\mathbf{K}))^{-1} \bmod 26 = 17$$

$$\mathbf{K}^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

شکستن رمز Hill

- حمله نوع دوم: حمله متن اصلی معلوم (Known Plaintext Attack)
- رمز Hill m تایی

$$\begin{cases} \mathbf{P}_j = (p_{1j} p_{2j} \dots p_{mj}) \\ \mathbf{C}_j = (c_{1j} c_{2j} \dots c_{mj}) \end{cases} \rightarrow \mathbf{C}_j = \mathbf{P}_j \mathbf{K}, \quad 1 \leq j \leq m$$

○ m جفت متن اصلی - متن رمز شده

$$\begin{cases} \mathbf{X}_{m \times m} = (p_{ij}) \\ \mathbf{Y}_{m \times m} = (c_{ij}) \end{cases} \rightarrow \mathbf{Y} = \mathbf{XK}$$

○ اگر \mathbf{X} معکوس پذیر باشد: $\mathbf{K} = \mathbf{X}^{-1} \mathbf{Y}$

- اگر \mathbf{X} معکوس پذیر نباشد ← استفاده از جفت‌های جدیدتر متن اصلی - متن رمز شده تا معکوس پذیر شود

مثالی از شکستن رمز Hill

- متن اصلی: hillcipher
- متن رمز شده: HCRZSSXNSP توسط یک رمز hill ۲ تایی

$$\begin{aligned} \begin{pmatrix} 7 & 8 \end{pmatrix} \mathbf{K} \bmod 26 &= \begin{pmatrix} 7 & 2 \end{pmatrix} \\ \begin{pmatrix} 11 & 11 \end{pmatrix} \mathbf{K} \bmod 26 &= \begin{pmatrix} 17 & 25 \end{pmatrix} \end{aligned} \Rightarrow \begin{pmatrix} 7 & 2 \\ 17 & 25 \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \mathbf{K} \bmod 26$$

$$\mathbf{X}^{-1} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}^{-1} \bmod 26 = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}$$

$$\Rightarrow \mathbf{K} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 7 & 2 \\ 17 & 25 \end{pmatrix} = \begin{pmatrix} 549 & 600 \\ 398 & 577 \end{pmatrix} \bmod 26 = \begin{pmatrix} 3 & 2 \\ 8 & 5 \end{pmatrix}$$

- نتیجه با بررسی سایر جفت‌ها تایید می‌شود

شکستن رمز Hill

- حمله نوع اول: حمله فقط با متن رمز (Ciphertext Only Attack)
- در برابر حمله نوع اول نیز می‌شکند، ولی پیچیده‌تر است.
- [Sinkov, Sec 4.5-4.6]

- مثلاً برای $m=2$:

1. تشخیص نوع سیستم رمزنگاری با محاسبه ضریب انطباق
2. دوحرفی‌های فرکانس بالا: TH, HE, IN, ER
3. دوحرفی‌های فرکانس پایین: شامل Q که بعد از آن U نیاید
4. حدس دو رابطه میان دو جفت

سیستم‌های جابجایی (transposition)

- هیچ حرفی تغییر شکل نمی‌دهد و محل قرار گرفتن آن در متن رمز شده نسبت به متن اصلی تغییر می‌کند
- ابتدا تعداد d حرف از متن اصلی انتخاب شده (قالب) و سپس یک جایگشت (permutation) بین این d حرف صورت می‌پذیرد (d : دوره تناوب سیستم)

$$Z_d = \{1, \dots, d\}, \quad f: Z_d \rightarrow Z_d, \quad K = (d, f)$$

$$P = p_1 \dots p_d p_{d+1} \dots p_{2d} \dots$$

$$C = E(K, P) = p_{f(1)} \dots p_{f(d)} p_{d+f(1)} \dots p_{d+f(d)} \dots$$

- رمزگشایی: جایگشت معکوس

$$f(1) = 2, \quad f(2) = 4, \quad f(3) = 1, \quad f(4) = 3$$

- مثال: $d=4$

○ متن اصلی: P=RENAISSANCE

○ متن رمز شده: C=EARN SAIS CNE

سیستم‌های جابجایی (transposition)

- فرکانس مشخصه حروف ثابت باقی می‌ماند
- تشخیص سیستم‌های جابجایی در شکستن رمز
 - تنها نمودار توزیع فرکانسی سیستم‌های جابجایی است که بدون انتقال منطبق بر توزیع نرمال است.
- فاصله قابل شکست

$$N_0 = \frac{H(K)}{D} = \frac{\log(d!)}{3.2} = 0.3d \log \frac{d}{e}$$

رمز جابجایی معکوس

- معکوس کردن ترتیب قرار گرفتن حروف
- I CAME I SAW I CONQUERED : متن اصلی
- DEREU QNOCI WASIE MACI : متن رمز شده

رمز rail fence

- متن اصلی در دو سطر نوشته می‌شود، به طوری که حروف یک در میان در سطرها قرار گیرند
 - سپس، متن به صورت سطری خوانده می‌شود
 - متن اصلی : I CAME I SAW I CONQUERED
- | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| I | A | E | S | W | C | N | U | R | D |
| C | M | I | A | I | O | Q | E | E | |
- متن رمز شده : IAESW CNURD CMIAI OQEE

جایگشت

- در مثال رمز جابجایی معکوس:

متن اصلی	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
متن رمز شده	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

- زنجیره:

(1,19),(2,18), (3,17), (4,16), (5,15), (6,14), (7,13), (8,12), (9,11), (10)

- رمز rail fence:

متن اصلی	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
متن رمز شده	1	3	5	7	9	11	13	15	17	19	2	4	6	8	10	12	14	16	18

- زنجیره:

(1),(2,3,5,9,17,14,8,15,10,19,18,16,12,4,7,13,6,11)

جایگشت (ادامه)

- آیا با تکرار عمل جایگشت به همان طریق اول می توان به متن اصلی رسید؟
- زنجیره: (1),(2,3,5,9,17,14,8,15,10,19,18,16,12,4,7,13,6,11)
- تکرار جایگشت: (1),(2,5,17,8,10,18,12,7,6),(3,9,14,15,19,16,4,13,11)
- برای این که هر حلقه به وضعیت اولیه خود بازگردد، می بایست به اندازه طول آن حلقه جایگشت انجام پذیرد
 - رمز جابجایی معکوس: با دوبار جایگشت متن اصلی حاصل می شود
 - کوچک ترین مضرب مشترک حلقه های مختلف

ماتریس جایگشت

$$f(1) = 2, f(2) = 4, f(3) = 1, f(4) = 3$$

$$(p_1 p_2 p_3 p_4) \rightarrow (p_2 p_4 p_1 p_3) = (c_1 c_2 c_3 c_4)$$

$$T^4 = \mathbf{I}$$

$$1, 2, 3, 4 \rightarrow 2, 4, 1, 3 \rightarrow 4, 3, 2, 1 \rightarrow 3, 1, 4, 2 \rightarrow 1, 2, 3, 4$$

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix} = \underbrace{\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}}_{T=\text{permutation matrix}} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{pmatrix}$$

- ماتریس جایگشت: ماتریس مربعی که در هر سطر و هر ستون دقیقاً یک ۱ دارد و توانی از آن همانی است.

$$C = T P, \quad T^l = \mathbf{I}$$

- سیستم‌های رمزنگاری مدرن تلفیقی از ایده‌های
 - ماتریس جایگشت، diffusion و confusion

دو روش پیشنهادی شانون برای کاهش اثرات حمله‌های آماری (تکرار)

- پراکنش (Diffusion): تبدیلاتی را شامل می‌شود که خواص آماری متن اصلی را در طول متن رمز شده پراکنده می‌کند
 - هر سمبل متن اصلی روی تعداد زیادی از سمبل‌های متن رمز شده تاثیر گذارد یا به طور معادل هر سمبل متن رمز شده از تعداد زیادی از سمبل‌های متن اصلی تاثیر پذیرد
 - رابطه بین متن اصلی و متن رمز شده پیچیده می‌شود
 - تغییر فرکانس نسبی
- آشفته‌سازی (Confusion): رابطه بین کلید و متن رمز شده پیچیده شود
 - الگوریتم جانشینی (substitution) پیچیده
- اساس طراحی رمزهای قالبی مدرن

رمز جابجایی ستونی

- نوشتن متن اصلی در ماتریس d ستونی \leftarrow به صورت سطری نوشته و به صورت ستونی خوانده می شود
- ترتیب خوانده شدن ستون ها و تعداد ستون ها توسط کلید مشخص می شود
- کلید: دنباله عددی یا حرفی
- مثال: کلید = SORCERY معادل 6341257
- ترتیب خوانده شدن: ستون ۴، ستون ۵، ستون ۲، ستون ۳، ستون ۶، ستون ۱ و ستون ۷
- در صورتی که سطر آخر تکمیل نشود، می توان چند حرف مجازی اضافه کرد.

مثال رمز جابجایی ستونی

Key:	4 3 1 2 5 6 7
Plaintext:	a t t a c k p o s t p o n e d u n t i l t w o a m x y z
Ciphertext:	TTNAAPTMTSUOAODWCOIXKNLYPETZ

شکستن رمز جابجایی ستونی

- اگر جدول کامل باشد (با متن اصلی یا حروف مجازی): شکستن ساده‌تر
- حالت جدول ناقص: [Sinkov, Sec. 5.3-5.5]

1. جدول توزیع فرکانسی منطبق بر الفبای نرمال: نوع سیستم جابجایی است
2. اگر طول کلید d و طول متن N باشد: $N=rd \leftarrow$ تجزیه
3. برای d های ممکن ستون‌ها را تشکیل داده و خواص آماری را بررسی می‌کنیم
 - تکرار حروف صدادار، پیدا کردن کلمات ممکن و ...
4. پس از یافتن d ، ترتیب قرارگرفتن را تعیین می‌کنیم
 - همه ترتیب‌های ممکن
 - فرکانس نسبی دوحرفی‌ها، سه حرفی‌ها و همچنین دوحرفی‌ها و سه حرفی‌های محتمل

بالا بردن امنیت در رمز جابجایی

• تکرار جایگشت

Key: 4 3 1 2 5 6 7
Plaintext: a t t a c k p
o s t p o n e
d u n t i l t
w o a m x y z
Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

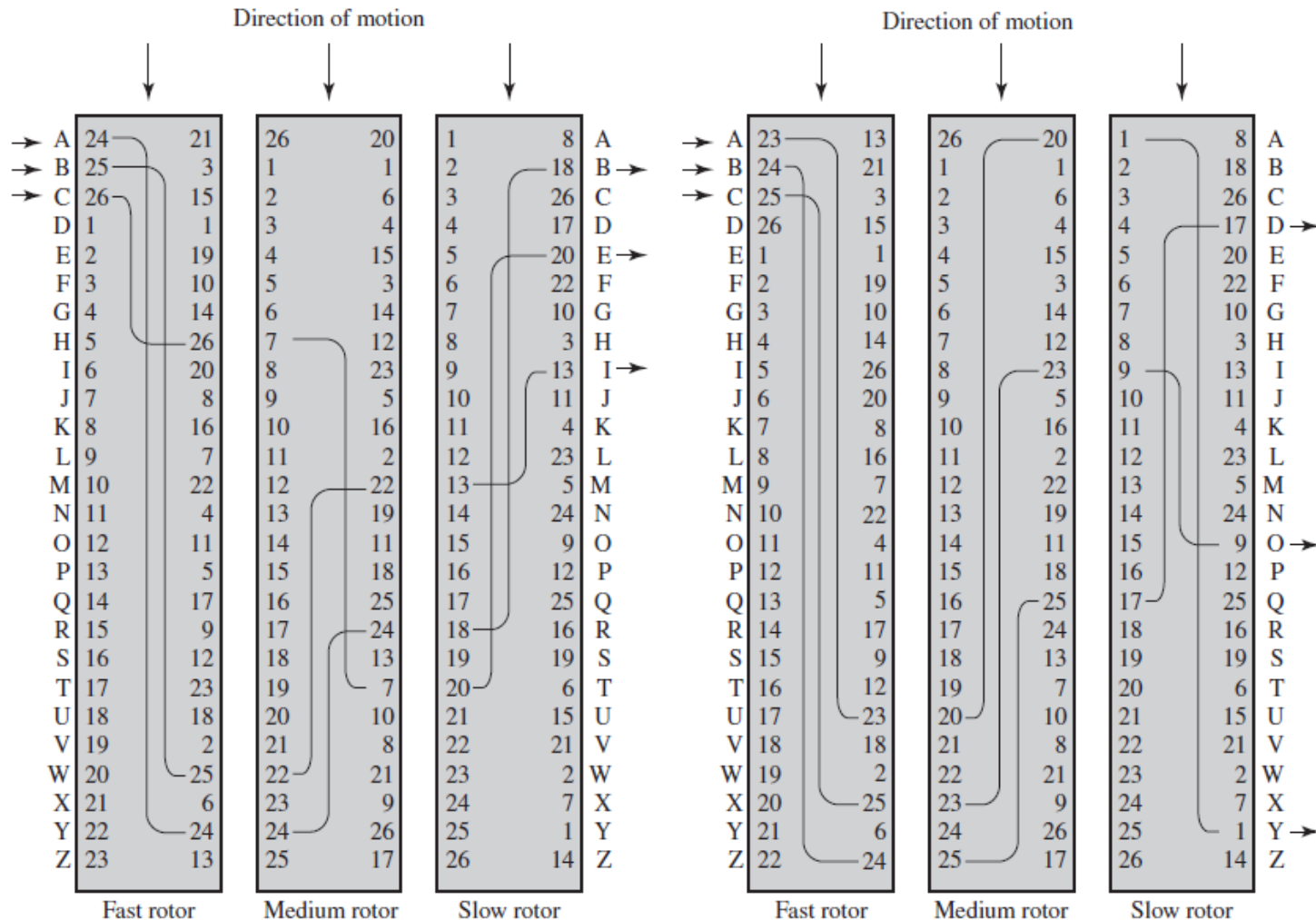
Key: 4 3 1 2 5 6 7
Input: t t n a a p t
m t s u o a o
d w c o i x k
n l y p e t z
Output: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28

03 10 17 24 04 11 18 25 02 09 16 23 01 08
15 22 05 12 19 26 06 13 20 27 07 14 21 28

17 09 05 27 24 16 12 07 10 02 22 20 03 25
15 13 04 23 19 14 11 01 26 21 18 08 06 28

ماشین روتور



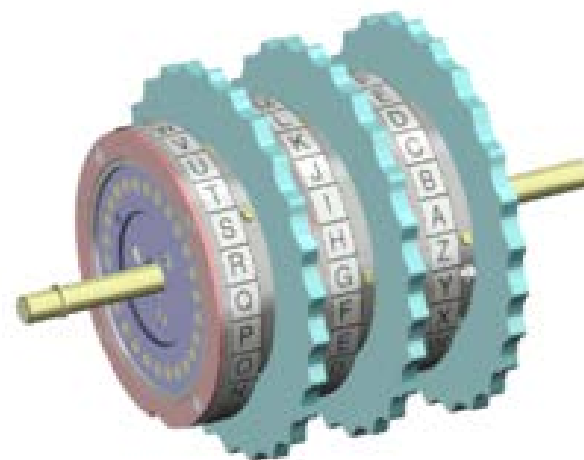
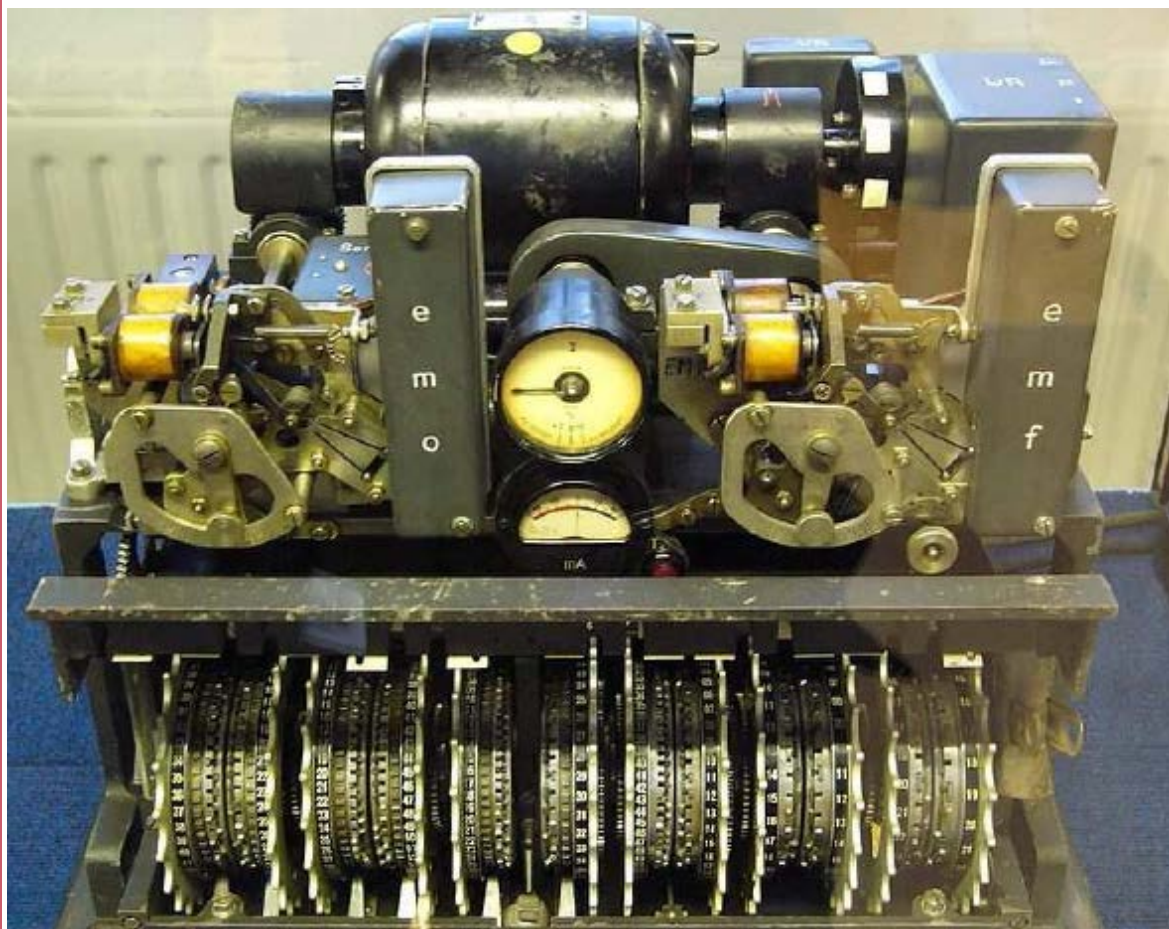
تکرار چند مرحله‌ای
رمزنگاری (چندین
سیلندر)

پیاده‌سازی رمز چند
الفبایی با دوره
تناوب ۲۶

هر موقعیت سیلندر
یک رمز تک الفبایی

بعد از هر اعمال
ورودی، سیلندر یک
موقعیت می‌چرخد

ماشین روتور

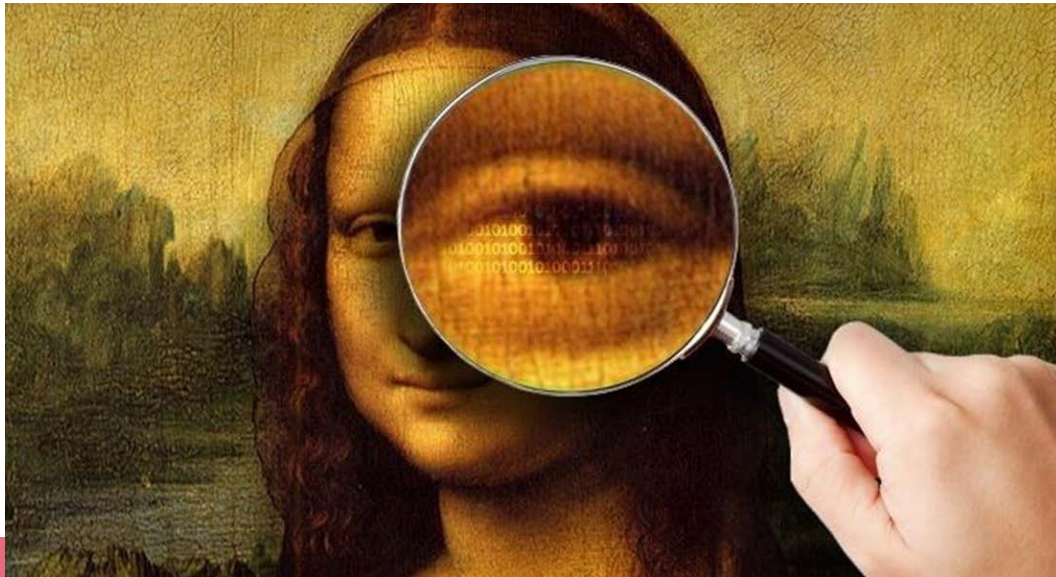


ماشین روتور

- سه روتور (دوره تناوب چندالفبایی) $26 \times 26 \times 26 = 17576$ substitution alphabets
- چهار روتور = 456976
- پنج روتور = 11881376
- جنگ جهانی دوم
 - آلمان (Enigma)
 - ژاپن (Purple)
- شکسته شد!
- ایده رمزهای مدرن مانند DES

Steganography نهان نگاری

- رمزنگاری پیام را برای مهاجم غیر قابل فهم می کند
- نهان نگاری وجود پیام را پنهان می کند، با استفاده از
 - زیرمجموعه‌ای از حروف/کلمات در یک پیام طولانی تر که به شیوه‌ای علامت گذاری شده‌اند
 - جوهر بی‌رنگ!، سوراخ روی حروف و ...
 - استفاده از LSB در فایل‌های صوتی و تصویری



- چالش: سربار زیاد
- مزیت: پنهان بودن