

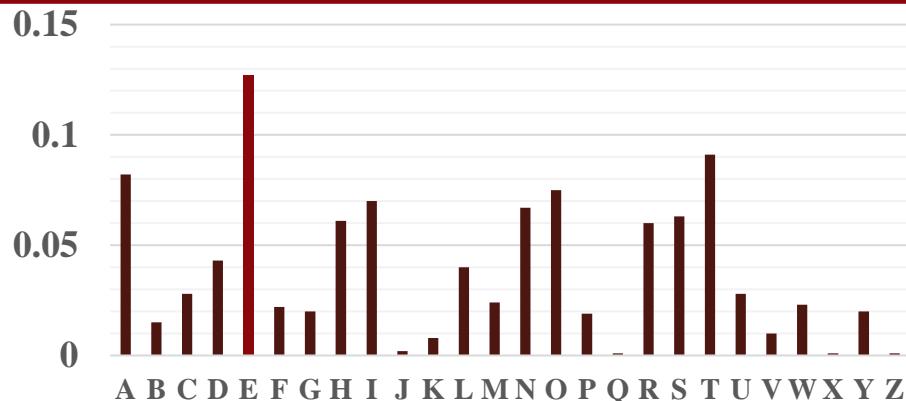

第2章 恩尼格玛密码机的破解

回顾

- 计算安全
- Kerckhoffs假设
- 不随机现象导致区分及密钥恢复攻击

古典密码的安全性分析

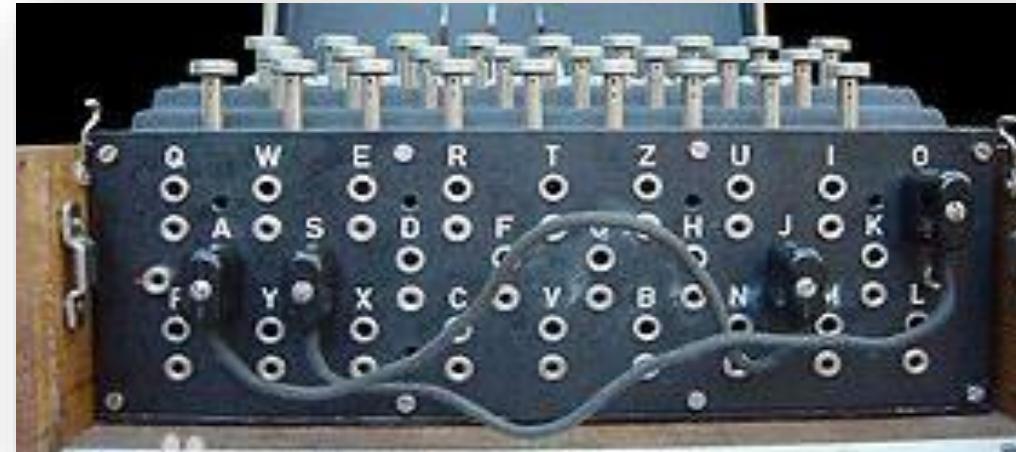
- 凯撒密码
 - 穷举攻击
 - 适用于小的密钥空间
- 单表代换
 - 频率统计
- 多表代换
 - 维吉尼亚密码（Kasiski测试法、重合指数法）



Probabilities of Occurrence of the 26 Letters			
letter	probability	letter	probability
A	.082	N	.067
B	.015	O	.075
C	.028	P	.019
D	.043	Q	.001
E	.127	R	.060
F	.022	S	.063
G	.020	T	.091
H	.061	U	.028
I	.070	V	.010
J	.002	W	.023
K	.008	X	.001
L	.040	Y	.020
M	.024	Z	.001

恩尼格玛 (ENIGMA)

- 1918年，德国发明家亚瑟·谢尔比乌斯 (Arthur Scherbius) 设计，最初商用
- 二战期间，被纳粹德国采用并改进，逐步发展出不同的型号，是通过无线电进行秘密通讯的手段



教学目标

- Enigma加密流程
- 利用区分器发现明密文关系
- 利用不随机现象进行密钥恢复

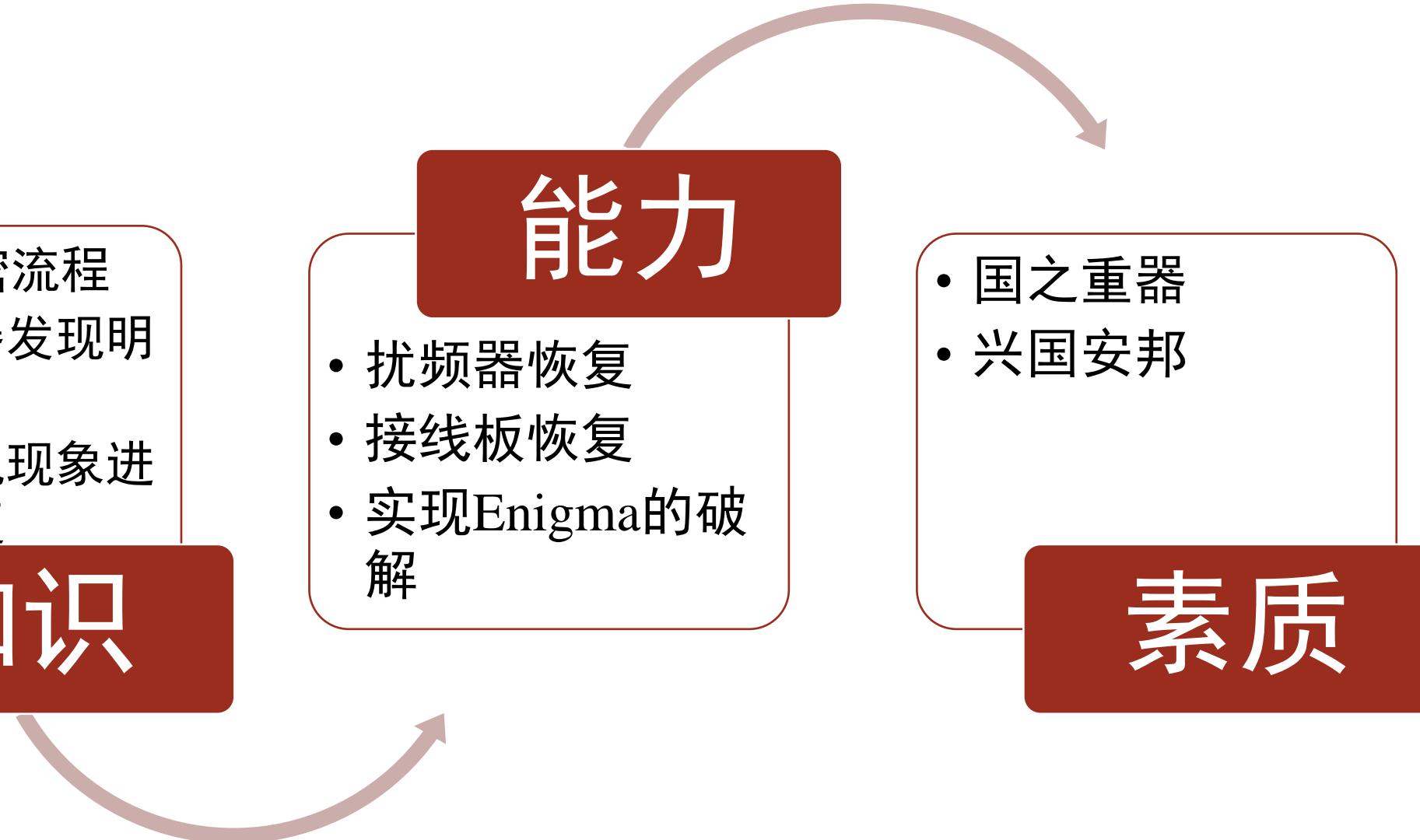
知识

- 扰频器恢复
- 接线板恢复
- 实现Enigma的破解

能力

- 国之重器
- 兴国安邦

素质



第2章 恩尼格玛密码机的破解



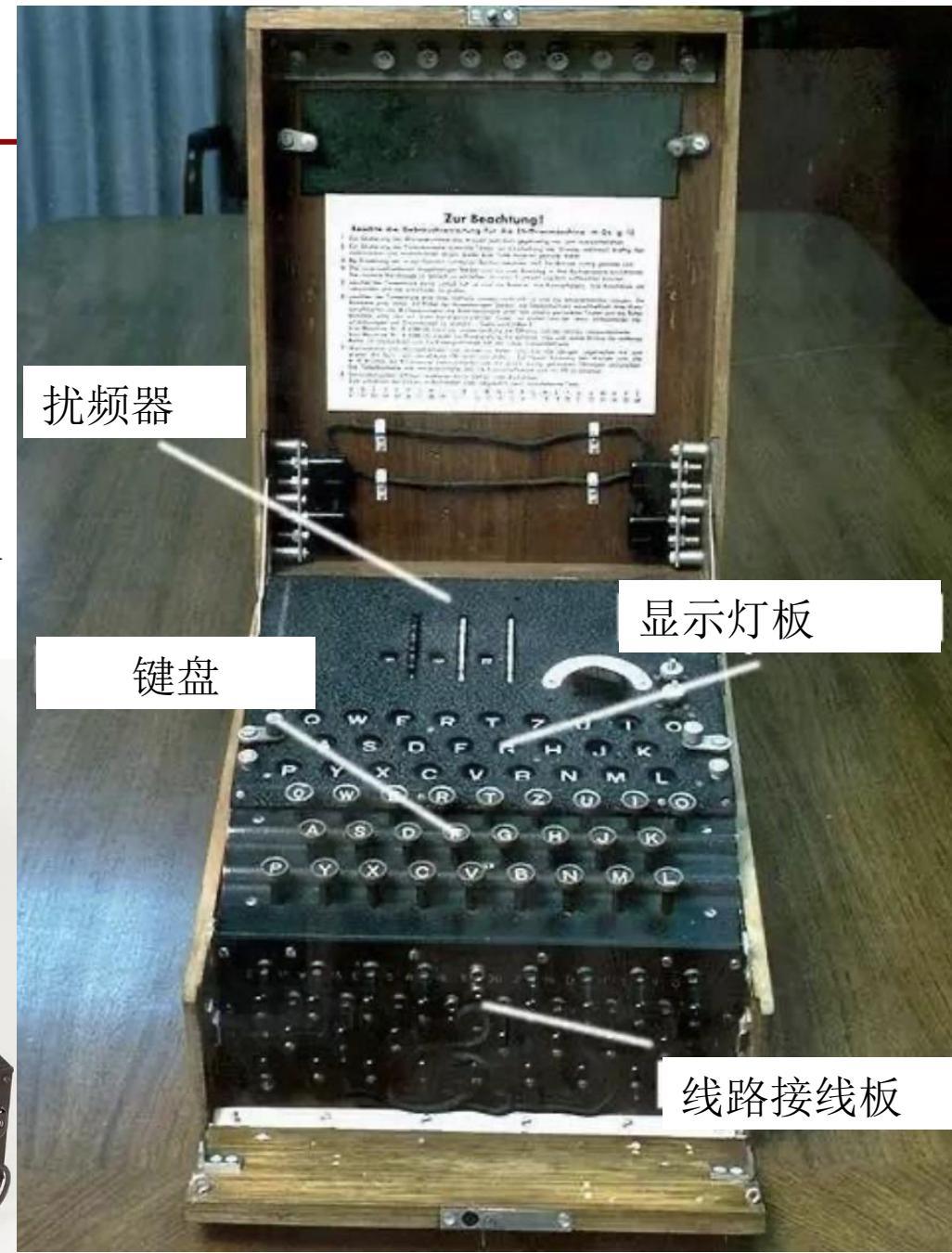
2.1 恩尼格玛密码机的工作原理



2.2 恩尼格玛密码机的破解

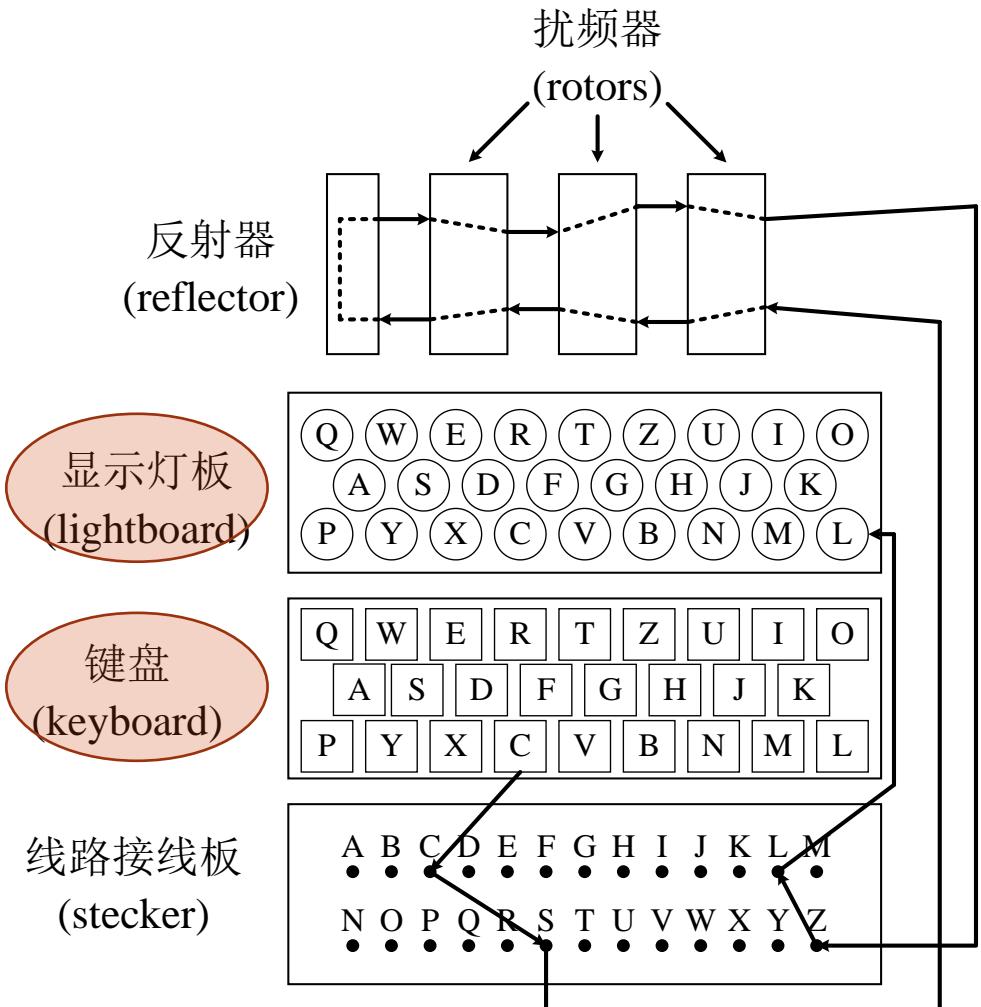
ENIGMA的主要部件

- 附录A.1
- 五个部件
 - 输入：包含26个英文字母的键盘
 - 输出：包含26个英文字母显示灯的显示灯板
 - 标有26个英文字母的线路接线板（Stecker）
 - 扰频器组合（Rotors）
 - 反射器（Reflector）



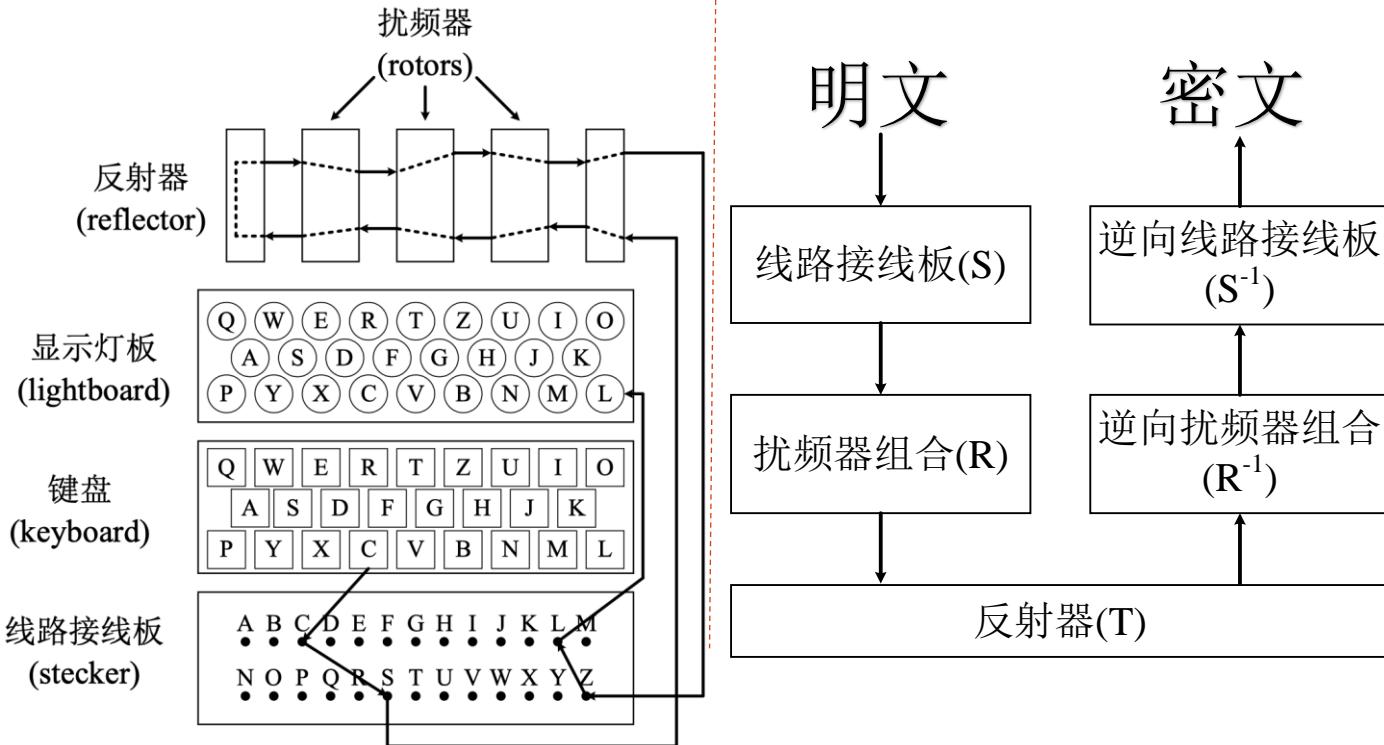
ENIGMA的工作原理

- 逐字母加密
- 输入端：包含26个英文字母的键盘（明文）
- 输出端：包含26个英文字母显示灯的显示灯板（密文）



ENIGMA的工作原理

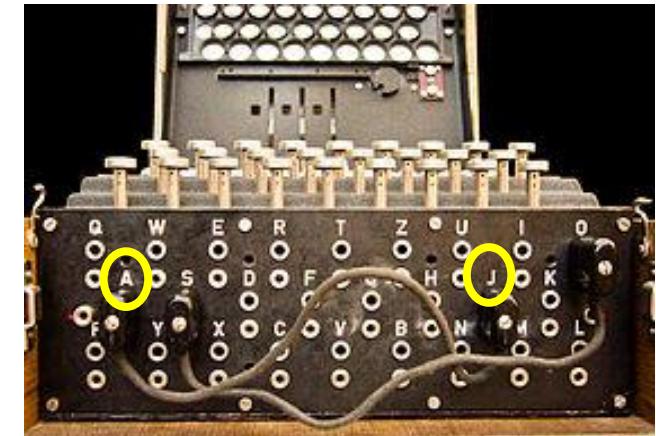
- 输入的单字母依次经过
 1. 线路接线板 (Stecker)
 2. 扰频器组合 (转子, Rotors)
 3. 反射器 (Reflector, T)
 4. 逆向扰频器组合
 5. 逆向线路接线板
- $C = S^{-1} \circ R^{-1} \circ T \circ R \circ S(P)$



- 加解密一致性: $P = S^{-1} \circ R^{-1} \circ T \circ R \circ S(C)$ (要求 $T \circ T = I$, 练习)

线路接线板： l 条连接线

- 从26个字母中，选择 l 对字母连接起来
- 例： $l = 2$: A \leftrightarrow J, O \leftrightarrow S, 无连线的到自身
- 注意：同一字母不能有两条及以上连线
- 由连接线情况决定的单表置换
- 连接线设置：密钥 K_1
- 假设使用了 l 条连接线，那么此处所有可能的置换表的总数 ($|K_1|$) 为



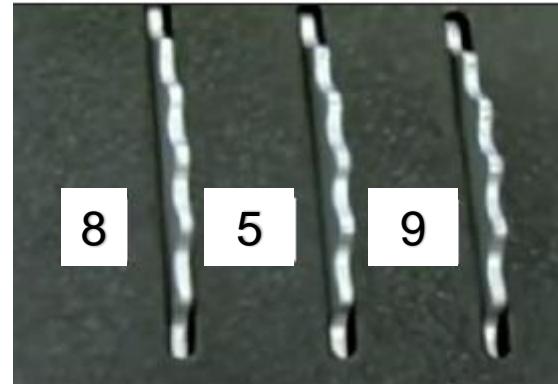
输入	A	B	C	D	E	F	G	H	I	J	K	L	M
输出	J	B	C	D	E	F	G	H	I	A	K	L	M
输入	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
输出	N	S	P	Q	R	O	T	U	V	W	X	Y	Z

$$\frac{26!}{(26-2l)! \times l! \times 2^l}$$

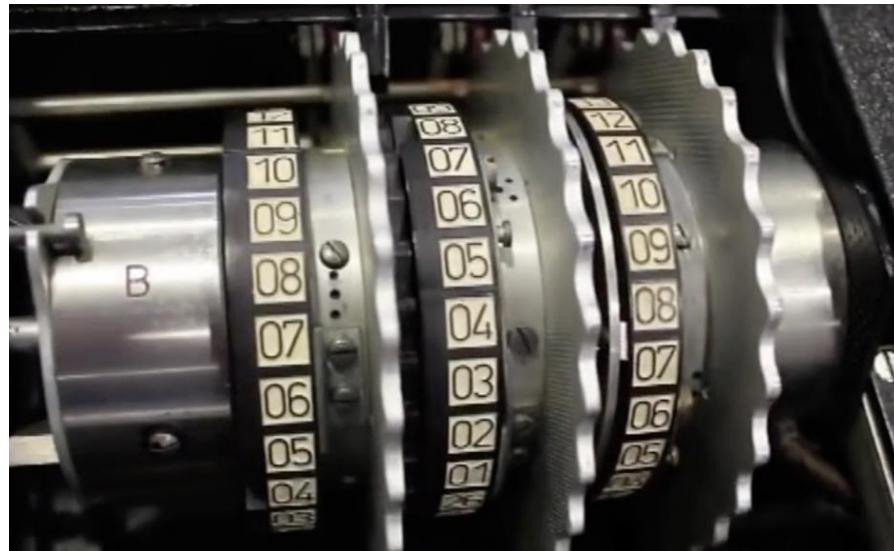
- $l = 10$ 时， $|K_1| = 2^{47.1}$

扰频器组合

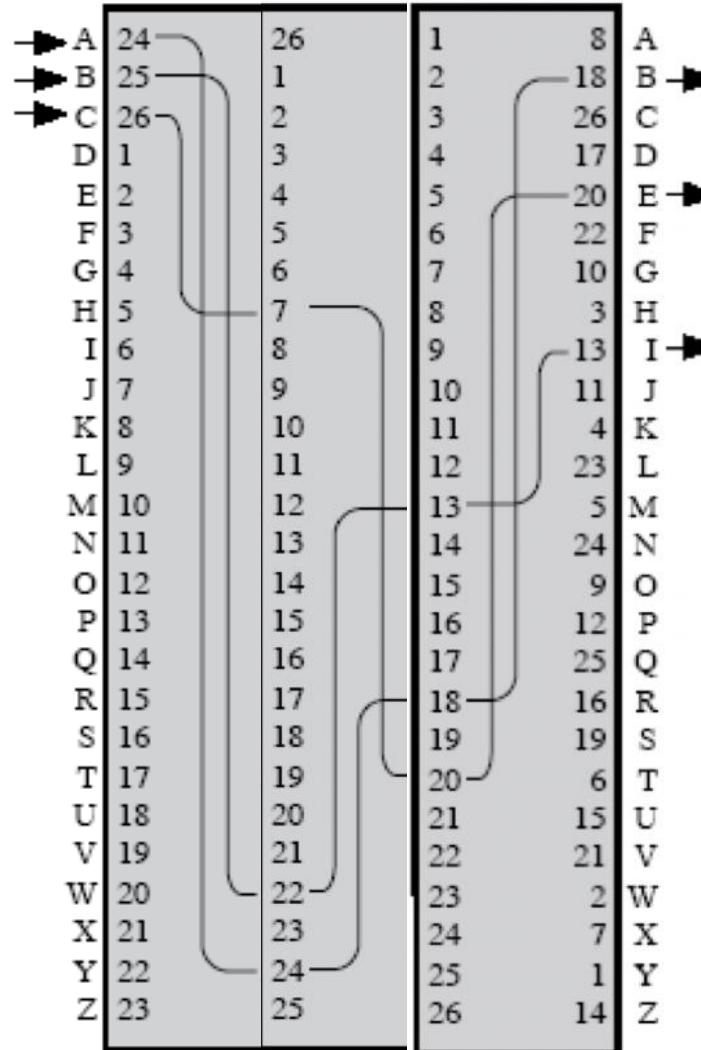
- 若干转子组成
- 最初版本：三个转子
- 显示：三个数字+转子（扰频器）
- 内部：快速、中速、慢速三个转子



扰频器组合



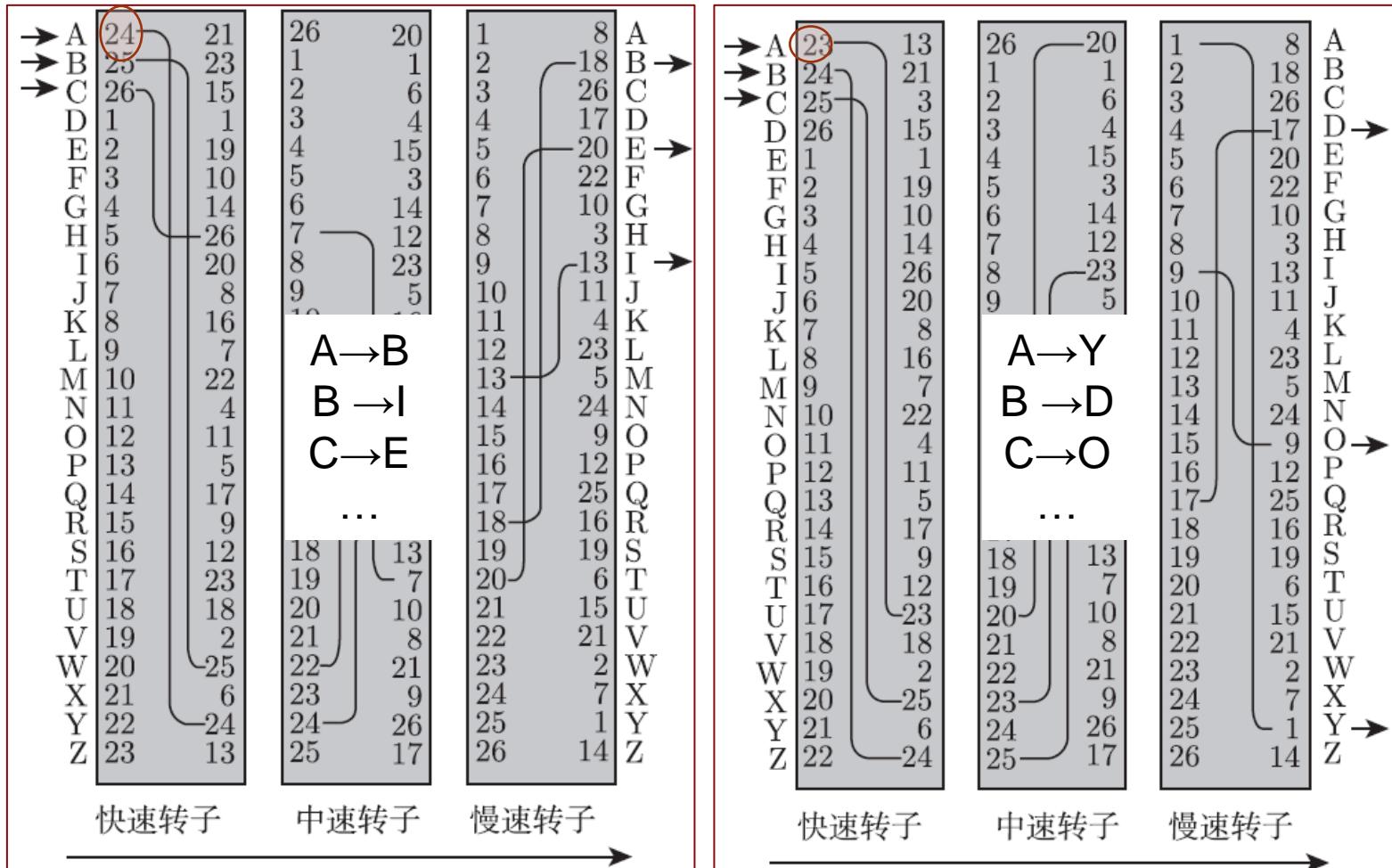
A→B
B→I
C→E
...
A→B
B→I
C→E
...
A→B
B→I
C→E
...



- 每个转子两侧都有26个数字，一侧顺序排列，另一侧乱序，而内部则是事先固定好的连接两侧数字的电路
- 每个转子是一个单表置换
- 3个转子合起来呢？
- 还是一个单表置换！怎么提高安全性？

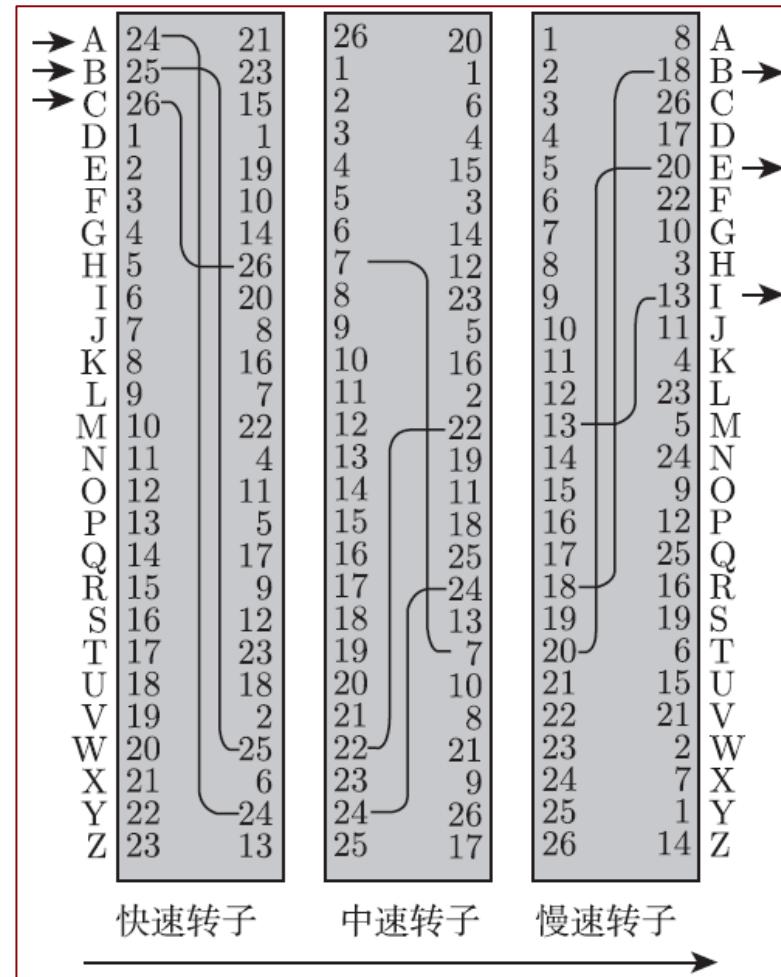
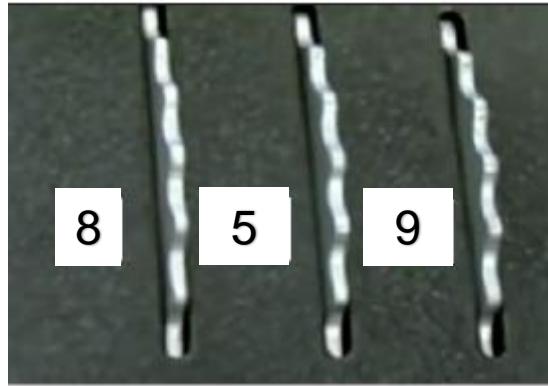
扰频器组合

- 单表 \Rightarrow 多表：转子转动
- 每输入一个字母，快速转子转动一次
- 快速转子转动一圈（26次），中速转子转动一次
- 中速转子转动一圈（26次），慢速转子转动一次
- 刻痕触发转动



扰频器组合

- 每个扰频器内部是事先固定好的电路
- ? 决定了所有可能的置换表?
- 每个扰频器的起始点
- 密钥 K_2 !
- 多少种?
- $26^3 = 17576$
- 密钥空间怎么才能更大?



- 若共有 t 个转子，使用时，从 t 个中选择3个放入机器再进行加密处理，则此时 K_2 的大小为（ ）。

A

$$26^3$$

B

$$C_t^3 \times 26^3$$

C



$$P_t^3 \times 26^3$$

D

$$26!$$

提交

扰频器组合（加强版）

- 共有 t 个转子，从 t 个中选择 s 个
- K_2 :
 - 选择哪 s 个转子
 - 转子的排列顺序
 - 每个转子的起始点

- 可能置换表的个数 ($|K_2|$) :

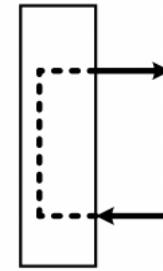
$$P_t^s \times 26^s$$

- $t = 5, s = 3$ 时， $P_5^3 \times 26^3 \approx 2^{20}$



反射器

- 26个字母由13条连接线两两连接，事先固定
- 固定的单表置换，没有密钥
- 为保证加解密一致性，需满足自反特性 $T \circ T = I$
- 例：假设 $T(A) = B, T(B) = A$ ，则 $T(T(A)) = A$
- 不随机现象（不可能事件）



记Enigma密码机的反射器为 T ，对任意输入 α ，计算 $\beta = T(\alpha)$ ，则 $\beta \neq \alpha$ 。

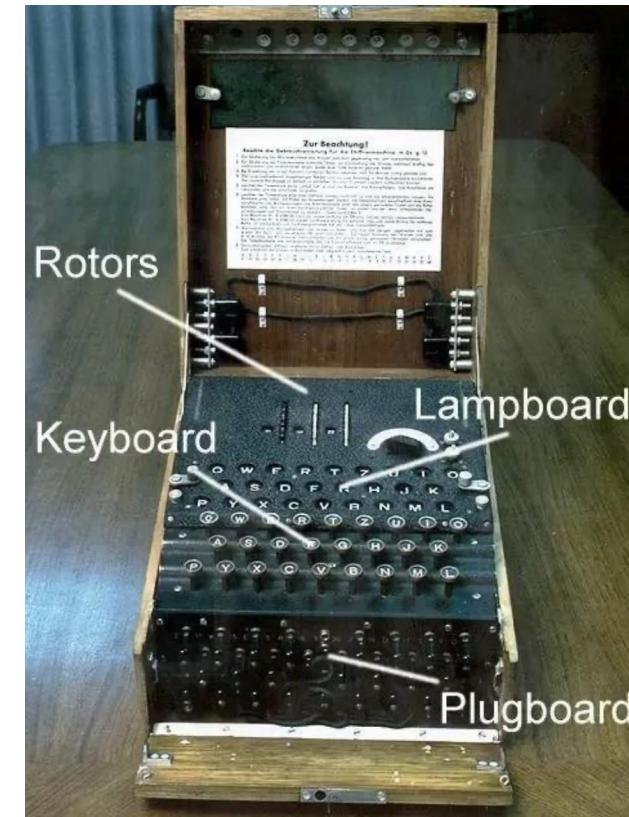
ENIGMA密码机的具体使用

- 对称密码算法，**多表代换密码**
- 加解密双方将Enigma密码机的线路接线板和扰频器组合 ($K_1 \times K_2$) 设置成相同的
- 每天更新密钥：纳粹军队每个月都会给Enigma密码机操作员一本新的密码薄，指定这一月中的每一天的密钥（破解时效性！）

纸上的密钥信息：从左往右分别是1. 轮子的类型(五具轮子) 2. 轮子初始位置 3. 插线板设置																				
Datum	Wälzerlage			Ringstellung			Steckerverbindungen							Kenzgruppen						
31.	I	II	V	10	14	02	EF	SD	AY	HG	OU	QC	WI	RL	XP	ZK	yqv	vuc	xxo	gvf
30.	V	IV	I	04	25	01	DI	ZL	RX	UH	QE	FC	VY	GA	SO	EM	mqy	vts	gvt	cax
29.	III	V	II	13	11	06	ZM	BQ	TP	YX	FE	AR	WH	SO	NJ	DG	aky	vav	oya	tzt
28.	I	III	II	09	16	12	NE	MT	RL	OY	HV	IU	GK	FW	PZ	XO	nfh	vco	tur	wnb
27.	III	II	I	06	03	15	BW	GR	SZ	OM	WQ	TY	HE	JU	XN	KD	bec	jmv	vtp	xdb
26.	I	III	V	19	26	08	GS	VD	CQ	LR	HI	BO	JP	UZ	FT	RN	wvu	yem	buz	rjk
25.	II	I	IV	05	01	16	KA	ZH	QP	GR	MF	LJ	OT	EN	BD	YW	ktv	muq	cqm	cpn
24.	III	II	IV	22	02	06	PI	KM	JB	YU	QS	OY	ZA	GW	CH	XF	zcd	iwo	urp	glg
23.	IV	III	II	08	11	07	SX	TD	QP	HU	FB	YN	CO	IK	WE	GZ	epm	mgs	vqg	vsm
22.	I	V	II	13	02	26	GP	XH	IW	BO	SU	MD	SA	ZK	QR	LT	aam	mvy	jqq	wqm
21.	IV	I	V	17	24	03	XG	AQ	OT	UZ	HD	RG	KM	BL	NS	JW	ltl	blu	frk	xrh
20.	IV	I	III	15	22	12	PO	TV	QC	ZS	XX	WR	BJ	DE	FU	LA	non	lic	oxr	usr
19.	V	I	III	13	24	21	HA	GM	DI	VK	JP	YU	EF	TB	ZL	XQ	ecd	ciq	uvr	ppt
18.	IV	V	I	23	09	00	KF	PZ	SQ	GR	AJ	OO	CN	BV	TM	KI	fjb	sts	uqu	cft
17.	III	II	V	21	24	15	UT	ZC	YN	BE	PK	JX	RS	GF	IA	QH	cub	sci	pyf	rqi
16.	IV	III	V	07	01	13	IN	YJ	SD	UV	GF	BH	TK	QE	AR	OP	kex	paw	flw	onw
15.	I	IV	II	15	04	25	TM	IJ	VK	OY	NX	FR	WL	GA	BU	SF	sdr	pbu	byv	khb
14.	III	II	IV	10	23	21	WT	RE	PC	FY	JA	VD	OI	HK	NX	ZS	mhz	iff	lnq	giy
13.	V	I	II	14	04	12	AN	IV	LH	YP	WM	TR	XU	FO	ZB	ED	rqh	ucm	ldi	ods
12.	II	V	I	07	19	02	HR	NC	IU	DM	TW	GV	FB	ZL	EQ	OK	asy	xza	uvc	fmr
11.	I	V	IV	13	15	11	NX	EC	RV	GP	SU	DK	IT	FY	EL	AZ	gyd	iuq	oeb	vef
10.	Y	II	I	09	20	19	FN	TA	YJ	EO	EG	PC	VD	KI	XH	WZ	pyz	ace	pru	uyc
9.	I	IV	V	14	10	25	VK	DW	LH	RF	JS	CX	PT	YB	ZG	MU	nyh	fbd	ohn	jrp
8.	IV	V	I	22	04	16	PV	XG	ZU	EQ	BW	CH	AO	RL	JN	TD	tck	rts	nro	mkl
7.	V	I	IV	18	11	25	TS	IK	AV	QP	HW	FM	DX	NG	CY	UE	mhw	lwb	mdm	sha

对于一个给定的Enigma机，以下哪些部件是固定不变的（）

- A 接线板的接线方式
- B 转子的起始位置
- C ✓ 反射器的接线方式
- D ✓ 每个转子的内部连线

**提交**

密钥空间

- K_1 : 接线板的设置
- K_2 : 扰频器组合的设置
- 密钥空间: $K_1 \times K_2$
- 若接线板有10条连接线, 扰频器5选3, 则此时可能的密钥个数为

$$\frac{26!}{(26-20)! \times 10! \times 2^{10}} \times P_5^3 \times 26^3 \approx 1.59 \times 10^{20} \approx 2^{67.1}$$

- $\frac{26!}{(26-20)! \times 10! \times 2^{10}} \approx 2^{47.1}$ 接线板对扩大密钥空间起到关键作用
- 恢复密钥? 穷举? 区分? 分割?

第2章 恩尼格玛密码机的破解



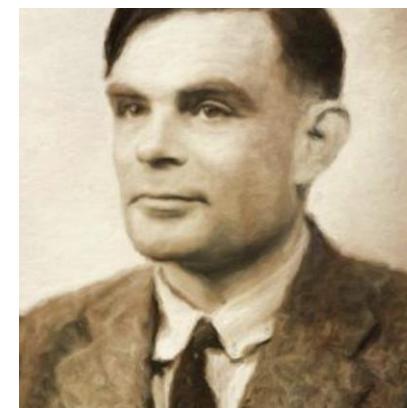
2.1 恩尼格玛密码机的工作原理



2.2 恩尼格玛密码机的破解

ENIGMA的破解

- 密码分析主力军：语言学家和人文学者⇒ 科学家
- 波兰的马里安·雷耶夫斯基（Marian Rejewski）对军方最初使用的简单版本的Enigma密码机进行了有效的破解
- 纳粹军方增加了两个新的扰频器，使得扰频器的排列变成从5个可能的扰频器中选择3个放入Enigma密码机中；同时，把线路接线板的连接线从6条增加到10条，大大增强了可能密钥的个数
- 得益于前期的研究工作和纳粹军队的人为失误，图灵才能做到对Enigma密码机的致命一击



1. 预测特殊明密文的对应关系 (CRIB) $P \leftrightarrow C$

- 唯密文攻击
- 哪怕是强力攻击，要想建立密钥有关的方程，也须知道明密文的对应关系
- 难题1：截获一段密文AETJWPXER，如何判断对应的明文？

解题关键1：不随机现象

- 记Enigma密码机的加密算法为 E , 对任意输入 α , 计算 $\beta = E(\alpha)$, 则 $\beta \neq \alpha$.

证明 反证法. 设存在输入 α , 满足 $\alpha = E(\alpha)$.

根据 Enigma 密码机的加密过程

不可能事件!

特殊现象!

$$\alpha = S^{-1} \circ R^{-1} \circ T \circ R \circ S(\alpha), \text{字母不能加密为自身}$$

对上式移项, 等价于

$$R \circ S(\alpha) = T \circ R \circ S(\alpha).$$

不妨记 $\gamma = R \circ S(\alpha)$, 则上式简化为

$$\gamma = T(\gamma).$$

与反射器的构造相矛盾. 证毕.

1. 预测特殊明密文的对应关系 (CRIB) $P \leftrightarrow C$

- 解题关键2：人为失误，语言习惯，例如 WETTER等特殊单词的使用
- 例：若截获包含单词WETTER的明文对应的密文为AETJWPXER，则WETTER对应的密文可能为？

猜测的明文	W E T T E R
已知的密文	A E T J W P X E R

?

猜测的明文	W E T T E R
已知的密文	A E T J W P X E R

- 判断依据：明文字母不会加密为自身（区分，概率的）
- 在获知密文的位置之后，我们便可以将明文与密文联系起来，这种明密文组合被称作克利巴 (Crib)，获得明密文对

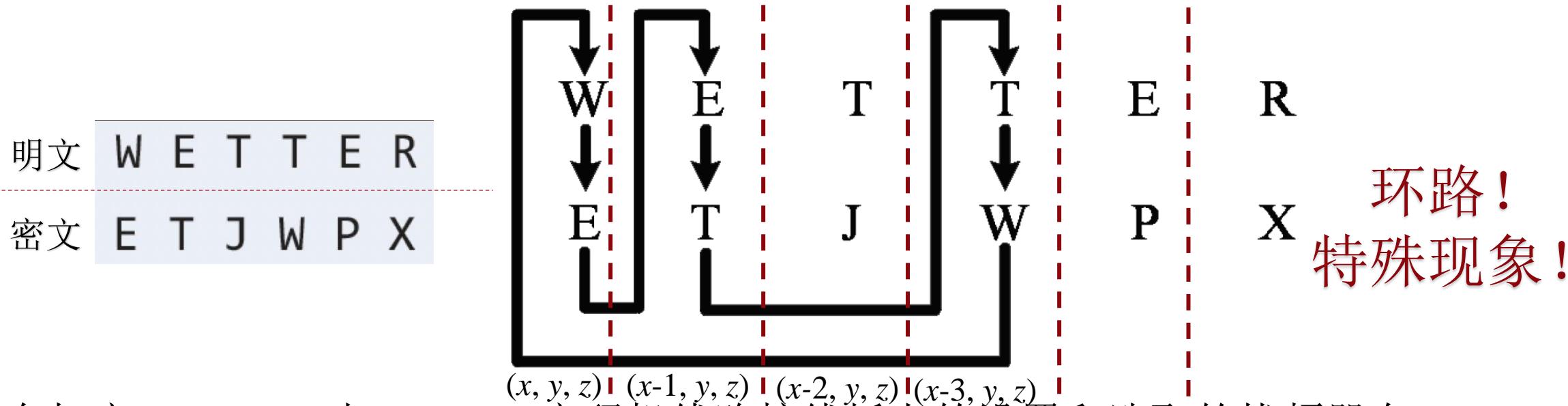
并不唯一！可能有误，需多个克利巴共同判断

难题2

- 如何找到不用穷举攻击整个密钥空间的新的正确密钥判定依据？
- 如何实现搜索空间的分割？

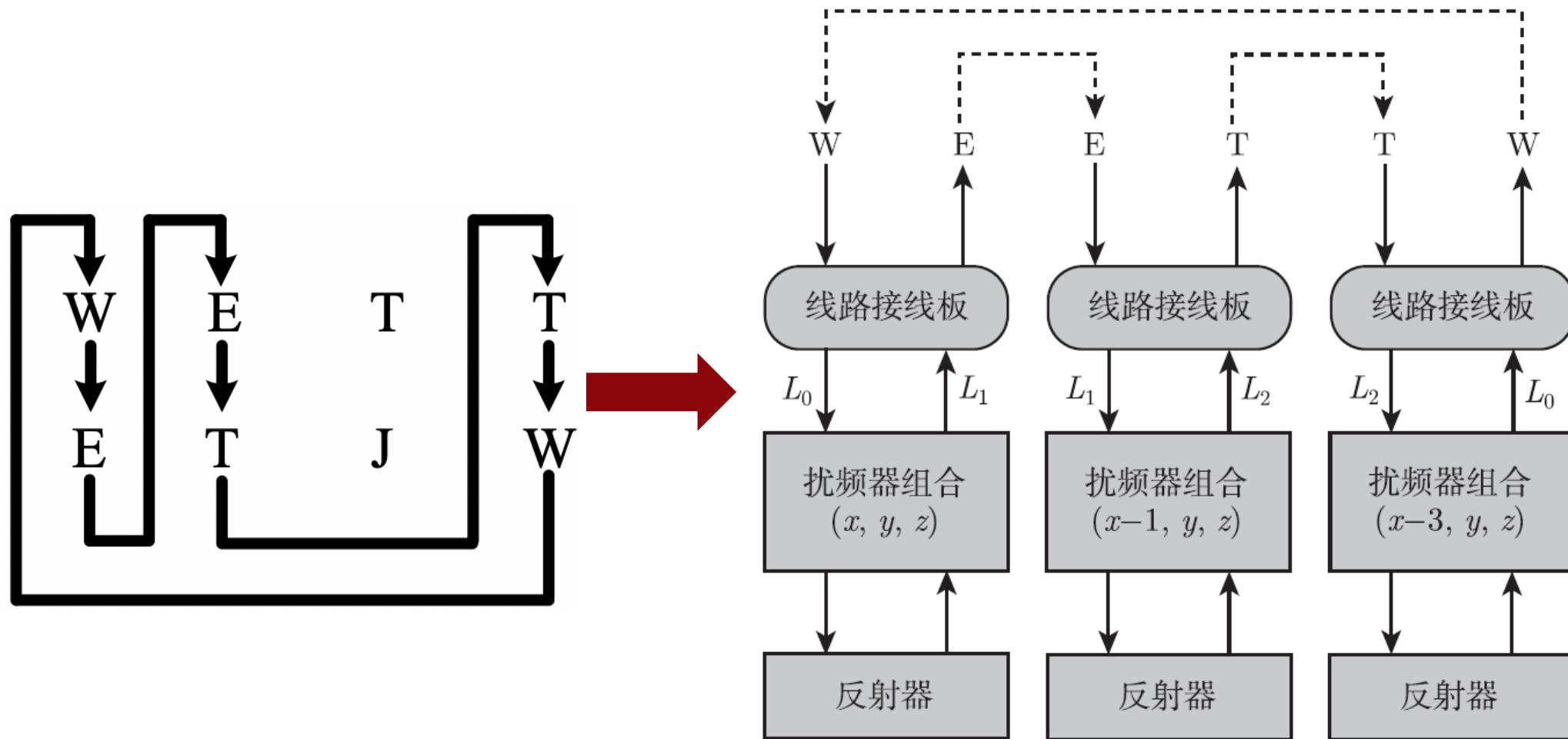
2. 恢复扰频器设置——分割

- 解题关键：发现特殊的Crib，内部能形成一个环路



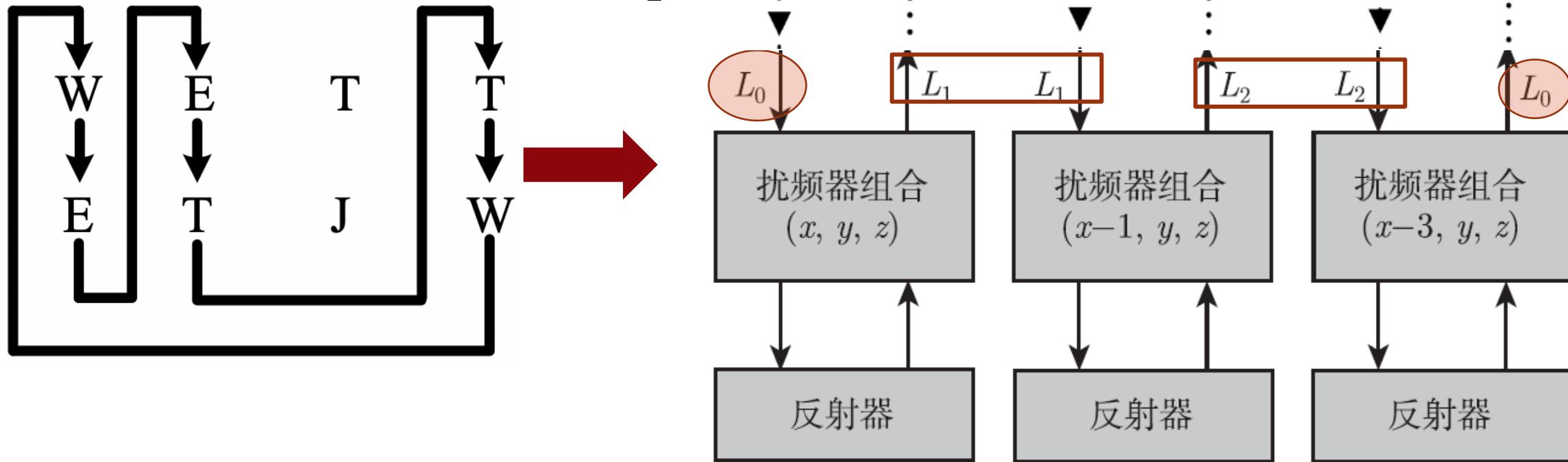
- 在加密W、E、T时，Enigma密码机线路接线板上的设置和选取的扰频器在一天内是不变的，且WETTER单词出现较早，在加密WET三个字母时，很可能只有快速扰频器发生转动，唯一的不同很可能仅在于快速扰频器的取值
- 设加密W时扰频器组合的初始值为 (x, y, z)

环路克利巴导致组件的分割



环路克利巴导致组件的分割

- 线路接线板的作用被消除了！
- 注意 L_0 、 L_1 、 L_2 的具体值未知，无法直接建立只与 K_2 有关的方程
- 难题3：如何判定正确的 K_2 ？



环路识别

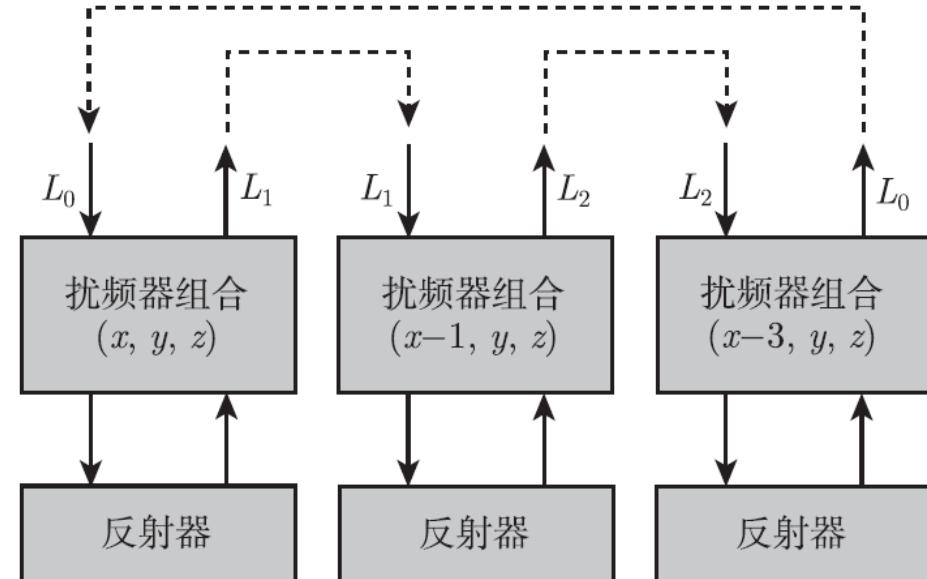
■解题关键：不随机现象—— L_0 进 L_0 出（内部环路）

■正确的 K_2 ：一定形成回路

■错误的 K_2 ：不一定形成回路

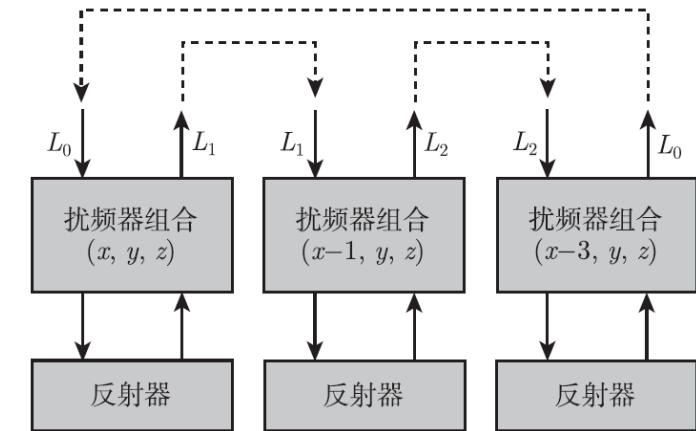
■如何识别回路？

■亮灯测试



环路识别

- 将第一台逆向扰频器组合的26个输出字母与第二台扰频器组合的相对应的26个输入字母用导线连接起来 (A-A, B-B, ……, Z-Z)，类似连接第二三台；第三一台
- 检验：在这26条回路上各安装一个灯泡
- 穷举 K_2 ：选、排、起点
- 正确的 K_2 ：26条回路至少存在一条灯亮
- 错误的 K_2 ：26条回路中以一定的概率至少一条灯亮



可观测到的结果

如何转换为正误密钥的判定条件？

已知结果求原因

环路识别——亮灯测试

- 检验：在这 26 条回路上各安装一个灯泡
 - 从 5 个转子中有序选择 3 个，放入三台连接好的扰频器 穷举密钥 K_2
 - 穷举第一个扰频器组合起始点 (x, y, z) 的所有可能，相应调整后面两个转子的起始点
 - 当这 26 个灯泡有亮灯的情况出现时，即表明此时的设置可能是正确的，同时获知了此时 L_0 、 L_1 、 L_2 的具体的值，记录此时的转子选择及 (x, y, z) 和 L_0 、 L_1 、 L_2 筛选候选密钥
- 穷搜扰频器设置： $P_5^3 \times 26^3 \approx 2^{20}$ 种可能
- 需结合多个环路进行验证或结合线路接线板的恢复继续筛选

练习

- 以上亮灯测试中，错误密钥（随机选取的密钥）也使回路亮灯的概率
- 提示：错排问题
- 答案：63.2%

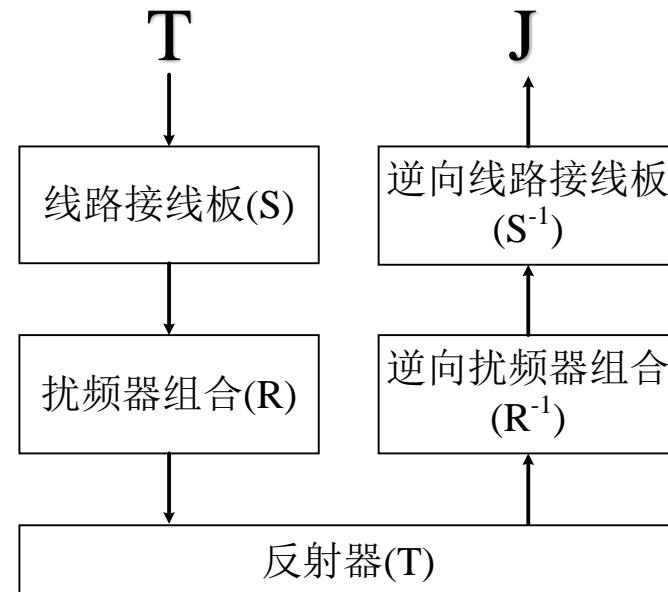
进一步优化

- 并行测试
- 同时开展 $P_5^3 = 60$ 组这样的测试，每组测试 $26^3 = 17576$ 种可能。
或更多组.....
- 实现密钥空间的分割：
$$2^{67.1} \Rightarrow \begin{cases} 2^{20} \\ 2^{47.1} \end{cases}$$
- 难题4：如何更有效的恢复 K_1 ？

3. 恢复线路接线板的设置（依据1）

- 克利巴中的其它字母
- 根据已确定的T、E的连线情况，推出线路连接板上字母J、P的连线情况！

明文	W	E	T	T	E	R
密文	E	T	J	W	P	X



R^{-1} 之后输出为 l_3 , $l_3 <= > J$

- 对于字母R 和X，若前面并没有确定与这两个字母相关的连接情况，则猜测R的连线情况，即可确定X的连线情况

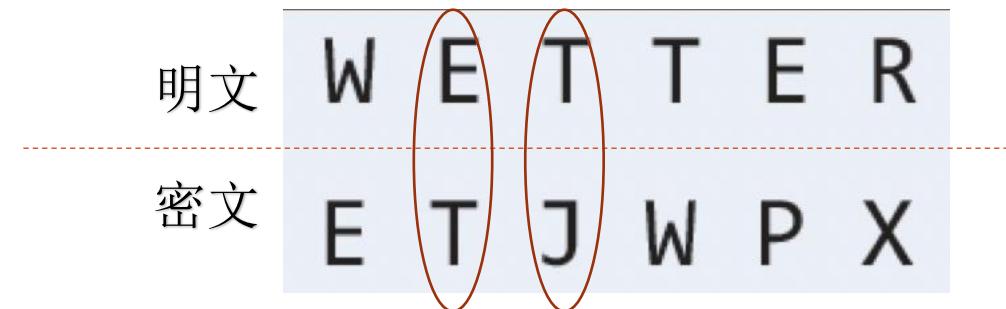
3. 恢复线路接线板的设置（依据2）

命题 2.3. 线路接线板的连线情况的判定依据

线路接线板的连接线条数已知，且一根接线只能连接两个字母，即不能出现 $\alpha \leftrightarrow \beta$, $\beta \leftrightarrow \gamma$ 且 $\alpha \neq \gamma$ 的情况。



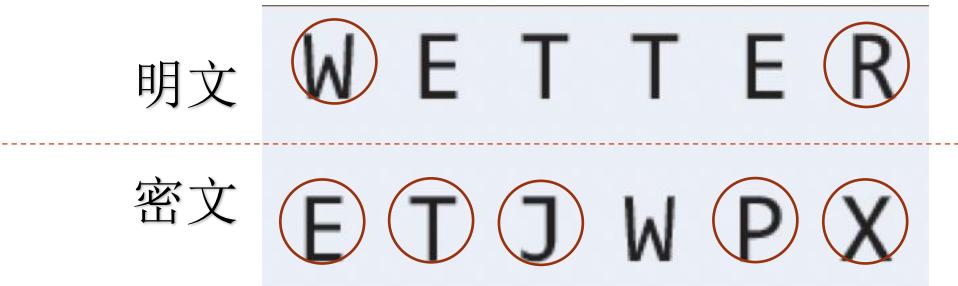
- 例如：若前面扰频器的信息已经猜测T与C连接，后面又推导出J与C连接，这就导致接线板的冲突



- 猜测R的连线情况时，不能与已有的冲突，减少需猜测的可能性

3. 恢复线路接线板的设置

- 一个克利巴可确定部分（例子中至多7条）连接线的对应情况
- 其余连接线？
- 继续猜测或者更多的克利巴
- 正确的线路接线板设置需满足：
 - 字符之间要符合加解密的对应关系
 - 接线不冲突
 - 接线条数为10
 - 恢复出的明文是有意义的
- 若测遍所有可能的连线情况以上有一条不满足，说明哪个环节可能出了问题？
- 扰频器，甚至最初的明密文对应关系
- 猜测+排除法：利用矛盾事件和环路克利巴，排除错误的连接线或扰频器起点



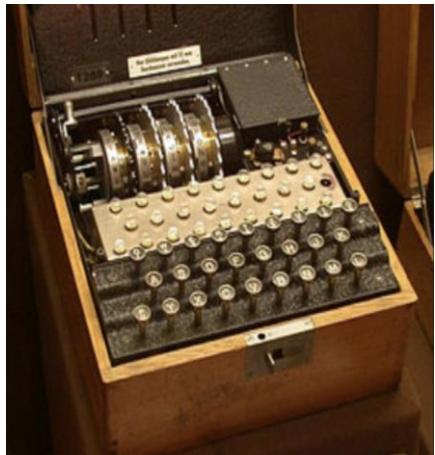
ENIGMA的破解——BOMBE

- 图灵建造出了能够快速检测的实际破解机械装置“炸弹（Bombe）”
- 每个“炸弹”由12组相连的Enigma密码机组成，因此可以处理更长的字母环。
- 整个装置高2米，宽2米
- “炸弹”投入战场使用后，大约需要20分钟就能发现Enigma密码机的设置



ENIGMA破解的影响

- 雷耶夫斯基、图灵等对Enigma机的破解大大缩短了二战的进程，拯救了上千万人的生命
- 在英国布莱切利园安放着一块基石，上面刻着丘吉尔的名言“Never in the field of human conflict was so much owed by so many to so few”



小结

- Enigma的实现及破解

根据语言习惯，发现明密文对应关系
(Crib)

- 思考：能否去掉反射器？Enigma算法可以如何改进？
- 作业：编程练习

利用特殊的crib发现环路

消除线路接线板影响，实现分割，恢复扰频器设置

恢复线路接线板设置

破解
Enigma

思维导图

