

古典密码学的巅峰对决

——图灵机 vs 恩尼格玛

缘起

1939年秋天，德军集中强大的兵力，在大批飞机、坦克的配合下，对波兰发动了突然袭击。波兰军队节节败退，并迅速沦陷。德军强大的军事势力震惊了英法等欧洲各国，一场席卷全球的世界大战就此拉开序幕！



缘起

同年，一名28岁的英国青年应召来到英国外交部通讯处从事密码破译工作，他将面对的是当时号称永远无法被破解的密码机，代号“奇谜”的恩尼格玛密码机。



缘起



艾伦·麦席森·图灵



恩尼格玛

恩尼格玛



中文名：恩尼格玛

英文名：Enigma

发明者：亚瑟·谢尔比乌斯

加密类型：对称加密

加密方式：机械转子，插线板

密钥长度： 10^{16} 个

古典密码术 - 凯撒密码

恺撒密码（英语：Caesar cipher），或称恺撒加密、恺撒变换、变换加密，是一种最简单且最广为人知的加密技术。它是一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。例如，当偏移量是3的时候，所有的字母A将被替换成D，B变成E，以此类推。这个加密方法是以罗马共和时期恺撒的名字命名的，当年恺撒曾用此方法与其将军们进行联系。



古典密码术 - 替代密码

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z
o	†	^	‡	α	□	θ	∞		ö	η		ø	∇	5	m	f	Δ	ε	c	7	8	9

Nulles ff. — . — . d .

Dowbleth σ

and	for	with	that	if	but	where	as	of	the	from	by
z	3	4	4	4	3	7	η	m	8	x	σ

so	not	when	there	this	in	wich	is	what	say	me	my	wyrt
8	x	++	Hy	6	x	6	6	m	n	m	m	d

send	lře	receave	bearer	I	pray	you	Mte	your name	myne
9	8	†	T	1	1	—	3	3	ss

古典密码术 - 多表替代密码

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

近代密码术的巅峰 - 恩尼格玛

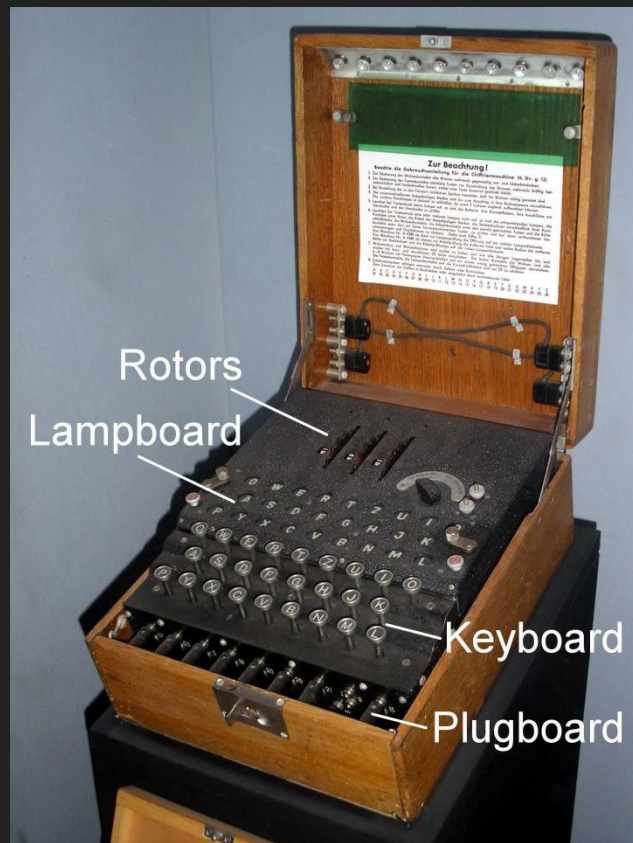
键盘 (Keyboard)： 输入明文/密文用的键盘

灯盘 (Lampboard)： 在键盘上输入一个字母后，灯盘上有一个字母会亮起，代表经过**加密/解密**后的字母

转子 (Rotor)： 进行加密的部件

插线板 (Plugboard)： 进行字母替换的部件

特点： 加密算法复杂的同时兼顾**操作简单**



恩尼格玛 - 操作流程



恩尼格玛 - 操作流程



1. 将转子调整到密码本指定刻度



2. 根据密码本连接插线板

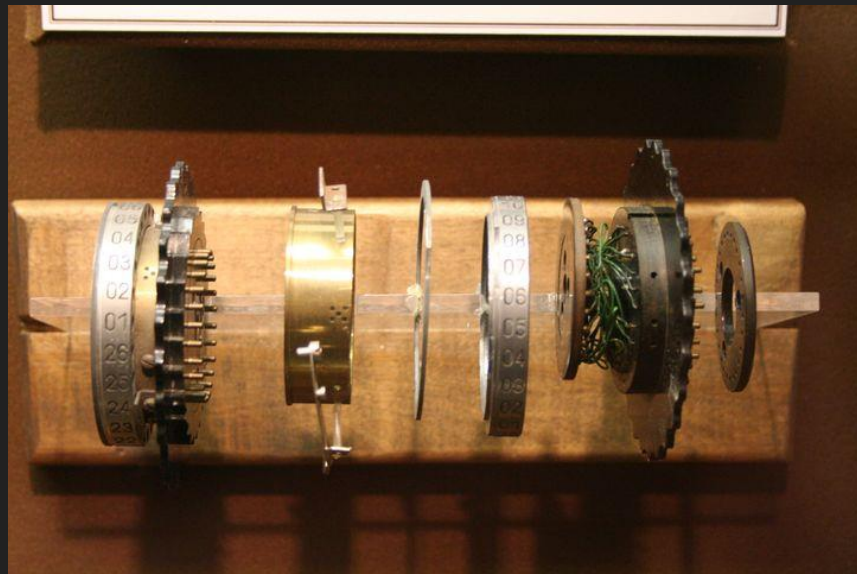


3. 输入明文/密文



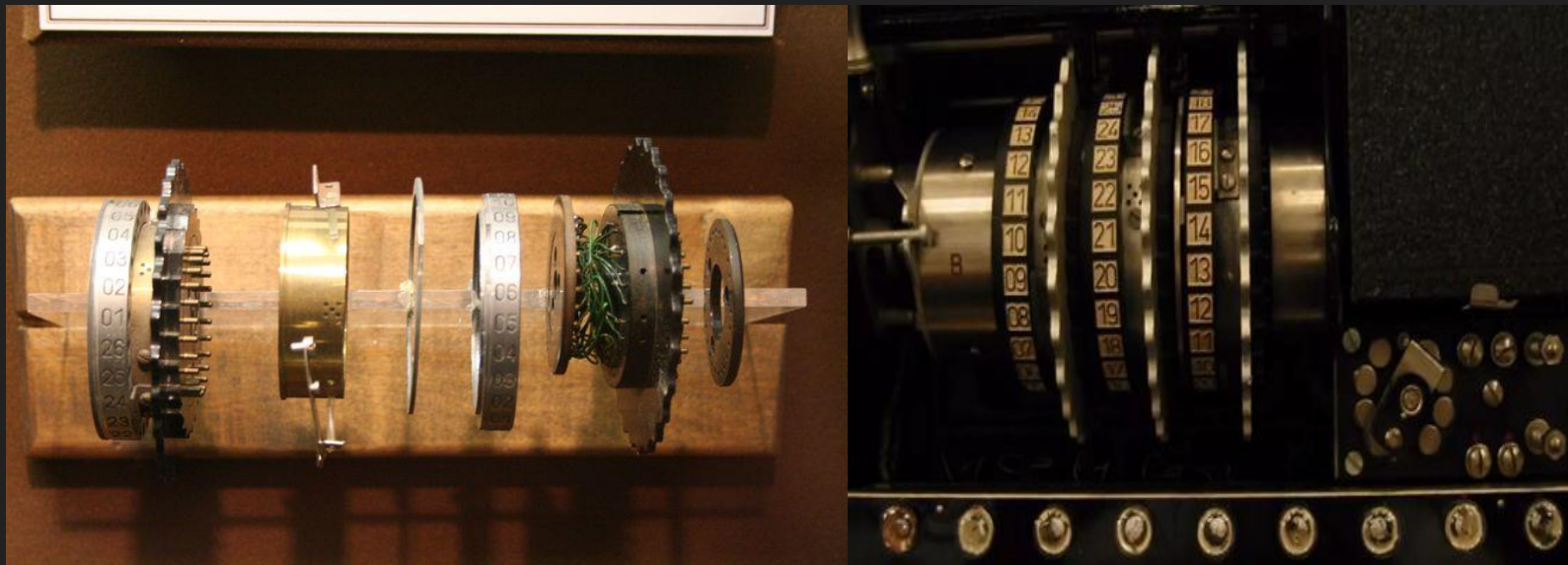
4. 记录指示灯亮起的字母，即加密/解密的结果

恩尼格玛 - 转子



转子的左右两侧分别有26个点，代表A-Z的对应关系，信号从一侧进入，从另一侧变换为对应的字母。

恩尼格玛 - 转子



三个转子串联起来之后，操作员输入一个字母，会经过三个转子的字母替换。每加密一个字母，最右侧转子会转动一格，最右侧转子转动一圈，中间转子转动一格，以此类推。从而实现每加密一个字母，自动更新字母表的效果。

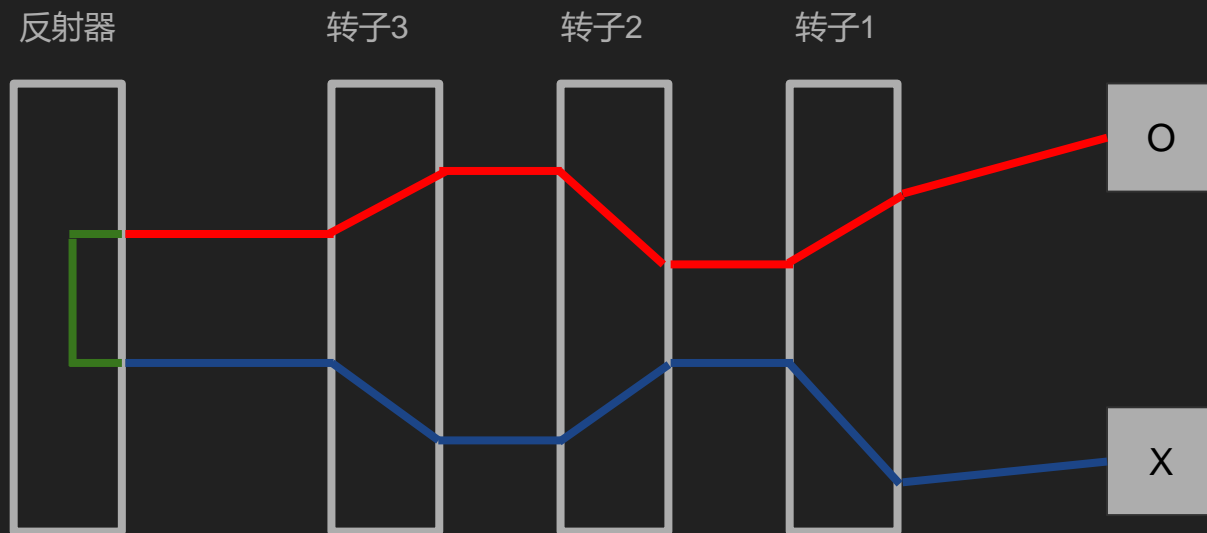
恩尼格玛 - 转子密钥空间

德军提供了5种不同的转子，加密时操作员会根据密码表挑选其中3个，**每个转子有26个可能的位置，5个转子有60种排列方式**，因此转子可以提供的密钥空间为： $26^5 * 60$

共18,534,946,560种可能



恩尼格玛 - 反射机制

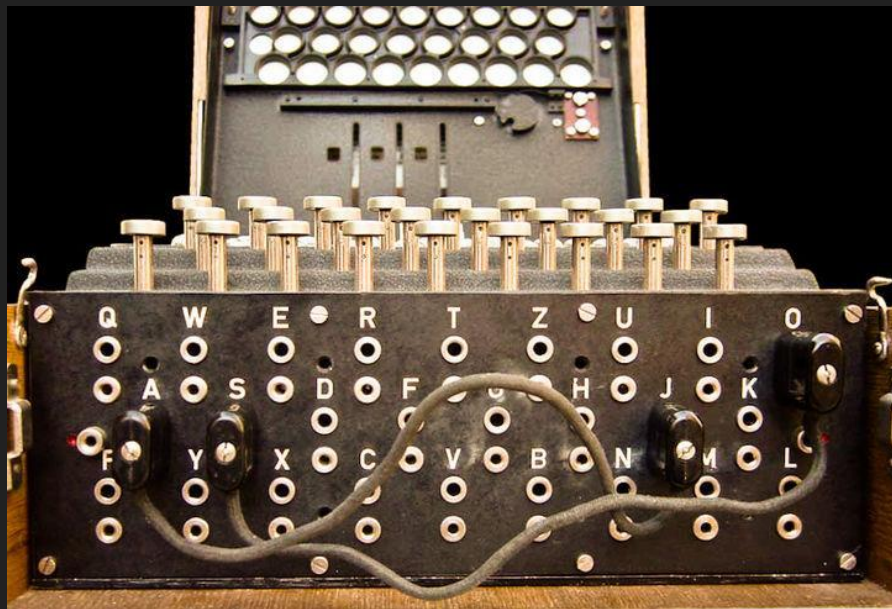


性质一：反射器使得恩尼格玛的加密过程时**自反的**（输入o得到x，输入x得到o）

性质二：一个字母加密后不可能等于它本身

恩尼格玛 - 插线板

插线板是在转子加密后，再做一次字母替换，插线板上的26个字母，操作员如果将某两个字母相连，则转子加密后会将这两个字母**互换**。例如当前转子映射后，输入O得到X，如果操作员将X与A相连，则X会被替换成A



恩尼格玛 - 插线板密钥空间

德军初期提供了**6根插线**，因此操作员最多可以替换6对字母，26个字母交换6对字母，其可能的组合超过100万种，加上转子的不同配置，其密钥空间为 $26^5 * 60 * 1,000,000$



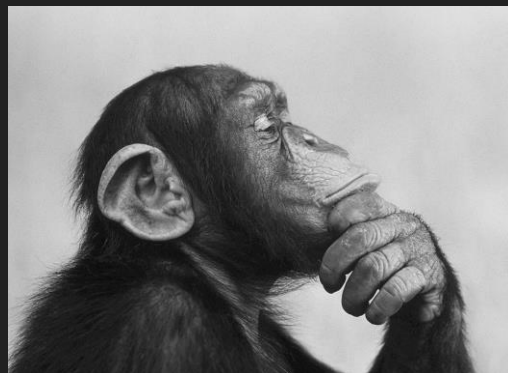
共**18,534,946,560,000,000**种可能。若一个人每秒尝试100种配置，需要**60万年**

恩尼格玛 - 德军使用条例



恩尼格玛 - 加密流程

Geheim		SONDER MASCHINENSCHLÜSSEL		Dresden 1939	
				May 1941	
Tag	Halbeslage	Ringstellung	Stecherverbindungen	Kanngruppaa	
1	V	IV	AT BE CS DP DM PE QK RP SS TT	SGL DFD GMA GMP	
2	V	III	AV CE DY FM GS HU JG KP TW	VIT REX GMA YPD	
3	III	I	AV DG OT XT YH IW LM OS QP	OPI QNO ZQH ZDT	
4	III	I	AV DT CL HS FE HM JG KP TW	DOP AJP DLP ZTS	
5	III	I	AV DT CL HS FE HM JG KP TW	DOP AJP DLP ZTS	
6	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
7	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
8	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
9	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
10	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
11	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
12	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
13	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
14	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
15	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
16	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
17	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
18	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
19	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
20	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
21	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
22	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
23	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
24	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
25	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
26	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
27	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
28	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
29	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
30	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	
31	I	IV	AN DY DS ET JL MO PE QS RT	WIT OTD YEX REX	



1. 每个月操作员会收到一本密码本（转子顺序、转子配置、插线板配置）

2. 根据当日的日密钥配置
恩尼格玛

3. 操作员从脑海中随机选取3个转子的配置（字母）作为次密钥

恩尼格玛 - 德军密码本

GEHEIM!

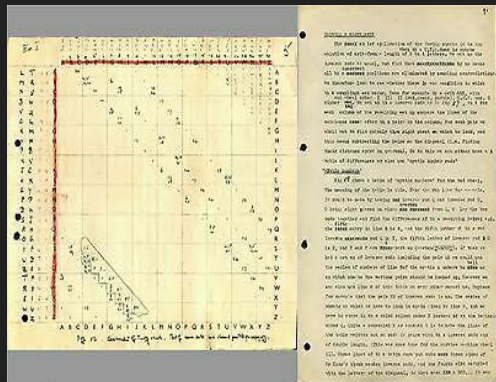
SONDER MASCHINENSCHLÜSSEL

DECEMBER 1939

May 1941

Tag	Walzenlage			Ringstellung	Steckerverbindungen	Kenngruppen
31	I	V	IV	01 13 04	AV BI CJ DP EM FK GQ HU SZ TY	REJ RFP DNM OAM
30	V	III	IV	09 01 03	BV CE DY FM GS HU IR JZ KP TW	VIV EKK GMA VPG
29	III	IV	I	10 08 26	AV BG CT EY FH IW LM NS OP QR	OFR QWB EQR NNN
28	II	III	I	02 05 01	AN BT CL ES FK HM IR JW QV YZ	BOP ABF GLV ZYR
27	III	I	IV	08 01 03	AH BV DR ET JL MN PX QS UY WZ	MYI OTU FZK HKG
26	I	III	IV	15 23 19	AJ CG DF EI KO LM PZ QV RX SW	AOT HYC NAX HDB
25	II	V	I	10 12 07	AY BK DN FI GM HU OW QV RT XZ	FHB UMD VVV DDH
24	III	II	IV	17 05 11	AB GT DL FO GW HV IU JX MR NP	RIJ SCH LPE IGW
23	III	IV	I	13 23 10	AH BG CK DV FZ JO LW NP SX TU	LPA FKH HJN SBH
22	II	IV	V	13 07 18	AR BX GO EN FL GQ HZ KS TY UV	MFT DUP OEO XVR
21	II	IV	V	15 12 20	AH BK DS EP FG IX JU LO QT WZ	MHJ EFR VBW XLI
20	I	IV	III	03 24 26	AO BU CJ DE GQ HP KW MX NV ST	KPF LJA JBQ EHM
19	II	I	III	22 04 24	AY BX FZ GJ HW IU KT LV OR QS	OFV PSZ GHZ CGU
18	III	I	II	15 14 08	AV CI DO ES FK HY JT MR PW QX	VOH VXM JHM CTR
17	I	V	IV	01 24 11	AI BW CF DY EU GV JO KP NS RT	AOK OOT IXN FOK
16	III	IV	I	04 07 13	AL BQ DN EI FJ MY PW RX ST UZ	WDU URI KNA AQK
15	IV	III	I	16 23 17	AY BW CG DK EO FT HJ IX PQ UZ	EPH ICM ZHE QPQ
14	V	III	I	11 11 15	AR DU EP GY IL JV KT MW NQ SX	ZCM QZK VDA VJG
13	IV	III	V	04 10 08	AL BD CN FY HX JS MR OT QU VZ	UMJ JXO WPG VSP
12	V	IV	I	13 02 16	AG BH DW EK FQ IM LO PZ SV TU	YBM EAX CDW BNN
11	II	IV	I	02 09 20	AN BW CO FL GK IX MZ PV RT SU	REW EIX RXZ XGT
10	V	I	III	09 09 11	AI DM FK GX JQ LP OR TU VZ WY	FZY AVR VXX HJE
09	IV	III	II	05 02 22	AB CE DT FG HY IX JO KV MN RW	COK ABQ MBD YGW
08	III	IV	V	05 26 06	BE CI DU FK GM HV JR LO NZ QT	JZV WXL MZK KEJ
07	I	IV	V	04 01 08	BU CE DS GX IV KL MT NW OP QE	OTG LWG WMI HOH
06	V	IV	I	16 19 06	AX CE DM GR HN IO JT KZ PW UY	FUP VSD NRQ IIE
05	IV	V	I	04 06 05	AZ BH DO EQ FV GR IW KM LU NX	NIL OAQ PHM KWZ
04	II	IV	III	07 12 02	AM BQ CR DU GO HP IT JK LZ VX	WJL QEW VDE UGP
03	IV	II	III	18 03 23	AH BS CX DO ER FW JV LP MZ UY	HWJ KBO RLF IWW
02	II	I	III	24 02 21	AY BZ CQ EX FI GJ KW MS NP RT	HAS NKD CJB MFT
01	V	I	IV	16 12 25	AU BY CH DQ EF IO JN KL MR PW	WZA HGK FOB FGM

恩尼格玛 - 加密流程



4. 用日密钥配置输入次密钥2次，作为报文开头



5. 使用次密钥输入明文，记录密文，作为报文内容



6. 发送报文

恩尼格玛 - 加密流程优缺点

- 日密钥保证了一个密钥配置最多只有24小时有效，英军破译小组截获德军的电报后也只有24小时的破解时间。
- 次密钥保证了即使当日的德军电报，正文中的密钥也都不相同，大大降低了英军截获日密钥加密的样本数量。
- 这个流程有没有漏洞呢？

波兰人的遗产

最早从事破译密码工作的是被称为密码研究“波兰三杰”的马里安·雷杰夫斯基（Marian Rejewski），杰尔兹·罗佐基（Jerzy Rozycki）和亨里克·佐加尔斯基（Henryk Zygański）。他们通过一些间谍活动得到了一部恩尼格玛，并了解到德军的使用条例。在经过一番研究后，他们发现了在德国人严谨使用条例背后隐藏的**重大漏洞**。



现在各位和几十年前的密码破译人员站在**同一起跑线**上，请思考一下恩尼格玛真的存在**漏洞**吗？

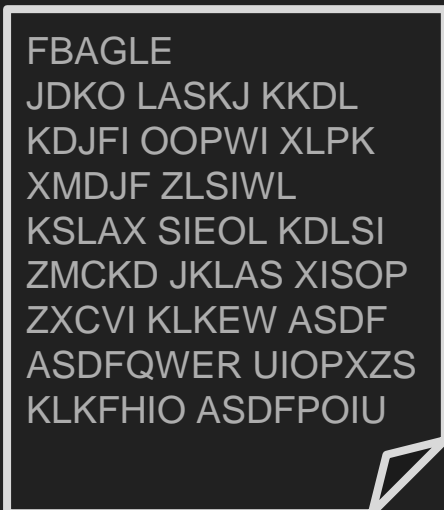
波兰人的遗产 - 德国人的破绽

右图为我们截获的报文，根据德国加密
条例，我们知道FBA GLE是三个字母**连续输入两次**的结果。

F - G

B - L

A - E



```
FBAGLE  
JDKO LASKJ KKDL  
KDJFI OOPWI XLPK  
XMDJF ZLSIWL  
KSLAX SIEOL KDLSI  
ZMCKD JKLAS XISOP  
ZXCVI KLKEW ASDF  
ASDFQWER UIOPXZS  
KLKFHIO ASDFPOIU
```


波兰人的遗产 - 德国人的破绽

假设次密钥为XYZ，转子的转换为 A_x (第 x 次加密)，我们可以得到：

$X(A_0) = F$ $Y(A_1) = B$ $Z(A_2) = A$
 $X(A_3) = G$ $Y(A_4) = L$ $Z(A_5) = E$

$X(A_0) = F$
 $X(A_0)(A_0) = X$
 $X(A_0)(A_0)(A_3) = G$
 $F(A_0)(A_3) = G$

FBAGLE
JDKO LASKJ KKDL
KDJFI OOPWI XLPK
XMDJF ZLSIWL
KSLAX SIEOL KDLSI
ZMCKD JKLAS XISOP
ZXCVI KLKEW ASDF
ASDFQWER UIOPXZS
KLKFHIO ASDFPOIU

X被消掉了！！

波兰人的遗产

我们将A0A3看作一种替换，可以通过多份电报收集到A0A3完整的替换表：

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

波兰人的遗产 - 链式表示

字母E在密码表中会被替换成U，U替换成F，F替换成G，G又替换成了E，这就形成了一个替换链。整个替换表的链式表示为：

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

我们将链的长度作为替换表的特征值，因此该替换表的特征值为：(11,5,4,6)

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

波兰人的遗产 - 链式表示

雷杰夫斯基对所有转子配置的密码链条的**数量和长度**进行了分类，做了一份查找表。波兰人破解恩尼格玛的步骤如下：

- 1.尽可能截获更多德军电报，将前6个字母提出，推到密码表的链式表示
- 2.根据链式查找表查找所有可能的转子，进行暴力破解
- 3.破解成功后，通过语法分析猜出插线板的配置

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

德军的反击

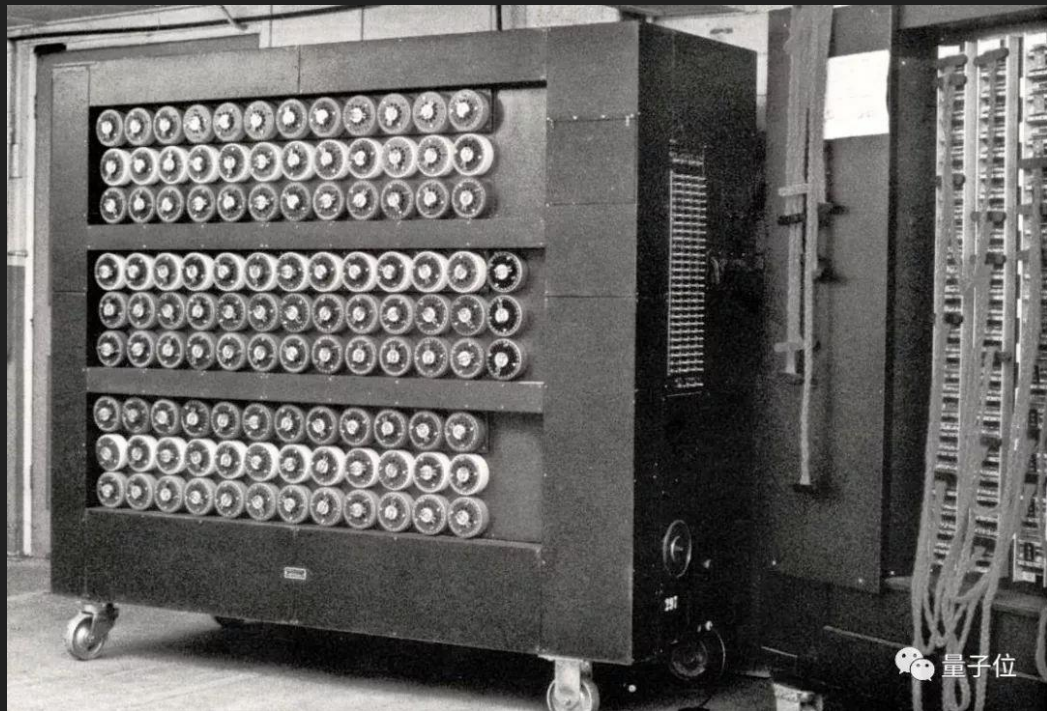
后期德军对又对恩尼格玛的加密进行了强化，强化内容如下

- 将转子从3个增加到5个
- 转子外侧的字母圈相对转心改为可以旋转
- 插线板从6根增加到10根
- 次密钥只输入一次

英军的绝地反击 - 图灵机的诞生

图灵接受破译工作后，他一直希望找到一种更通用的方法破解恩尼格玛，而不是利用德军使用条例的漏洞，最终，他决定制造一种通用的机器破解恩尼格玛。

用魔法来打败魔法！



英军的绝地反击 - 寻找Crib

要破解恩尼格玛，图灵需要一种称为Crib的东西来帮助图灵机进行破译工作。

所谓Crib是猜测出的一些明密文对应关系。最终他找到了德国人最常用的句子，
Heil Hitler（希特勒万岁）

明文位置1	H	E	I	L	H	I	T	L	E	R		
明文位置2		H	E	I	L	H	I	T	L	E	R	
明文位置3			H	E	I	L	H	I	T	L	E	R
密文	X	E	L	P	T	O	H	H	P	I	A	D

英军的绝地反击 - 寻找Crib

根据恩尼格玛反射器的特性，可以排除掉位置明文位置1和明文位置2。这样我们可以找到一个Crib，即明文位置2与密文的对应。

明文位置1	H	E	I	L	H	I	T	L	E	R		
明文位置2		H	E	I	L	H	I	T	L	E	R	
明文位置3			H	E	I	L	H	I	T	L	E	R
密文	X	E	L	P	T	O	H	H	P	I	A	D

英军的绝地反击 - 寻找Crib

根据恩尼格玛反射器的特性，可以排除掉位置明文位置1和明文位置2。这样我们可以找到一个Crib，即明文位置2与密文的对应。

明文	H	E	I	L	H	I	T	L	E	R
密文	E	L	P	T	O	H	H	P	I	A

英军的绝地反击 - 破解恩尼格玛

根据对照表，我们可以找到一组字母链：

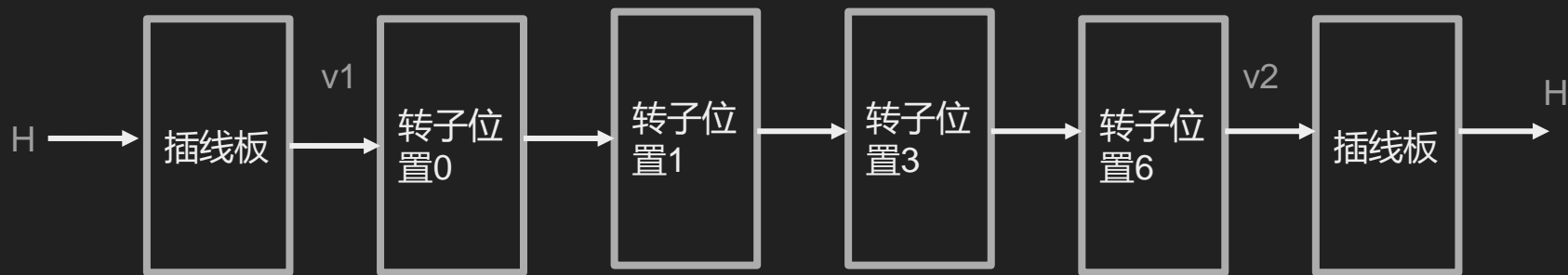
H (转子0) -> E (转子1) -> L (转子3) -> T (转子6) -> H

明文	H	E	I	L	H	I	T	L	E	R
密文	E	L	P	T	O	H	H	P	I	A

英军的绝地反击 - 破解恩尼格玛

根据对照表，我们可以找到一组字母链：

H (转子0) -> E (转子1) -> L (转子3) -> T (转子6) -> H



暴力搜索： $v1=v2$

英军的绝地反击 - 破解恩尼格玛

图灵制造的这台机器，代号“炸弹”，操作员把准备好的Crib输入机器，通过暴力破解，遇到可能的解机器就会停止运行。终于完全破解了恩尼格玛。

图灵通过“炸弹”破解恩尼格玛，据历史学家分析，他的之一贡献拯救了至少1400万人的性命，使二战至少提前2年结束。



Q&A