

En i gma密码的原理与破译

于红波

2024-3-6



提纲

- Enigma密码机的设计原理
- Enigma密码机的破解
 - 波兰人方法
 - 图灵的方法



古典密码

- 置换密码：交换字母的位置

- 代换密码

 - 单表代换：频率分析

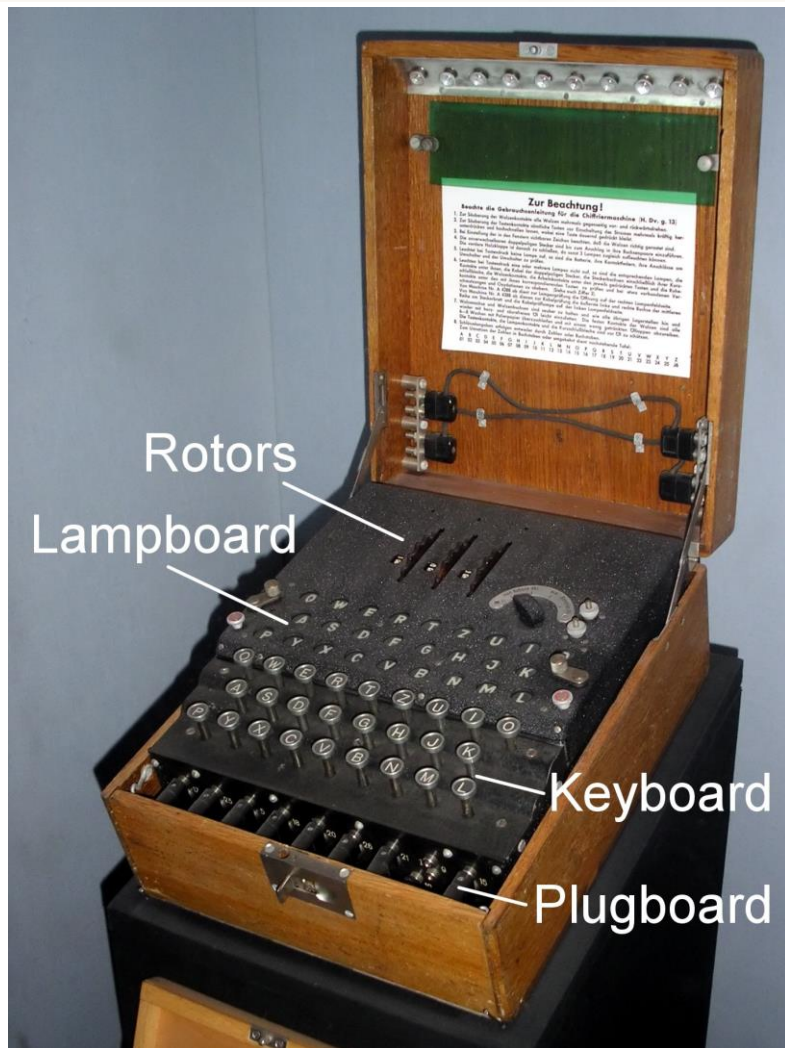
 - 多表代换：重合指数法+频率分析

每加密一个字母就更换一次密码表并且永不重复

- 一次一密



Enigma密码机的原理



键盘 (keyboard) : 输入字母
灯盘 (Lampboard) : 在键盘上
输入一个字母后, 等盘上会有一个
字母亮起, 代表加密后的字母
转轮 (Roter) : 加密部件
插线板 (Plugboard) : 加密部件

优点:

1. 安全性高
2. 使用方便



Enigma密码机原理

模拟器：

<https://www.101computing.net/enigma-machine-emulator/>

视频

<https://www.bilibili.com/video/av21919076/>

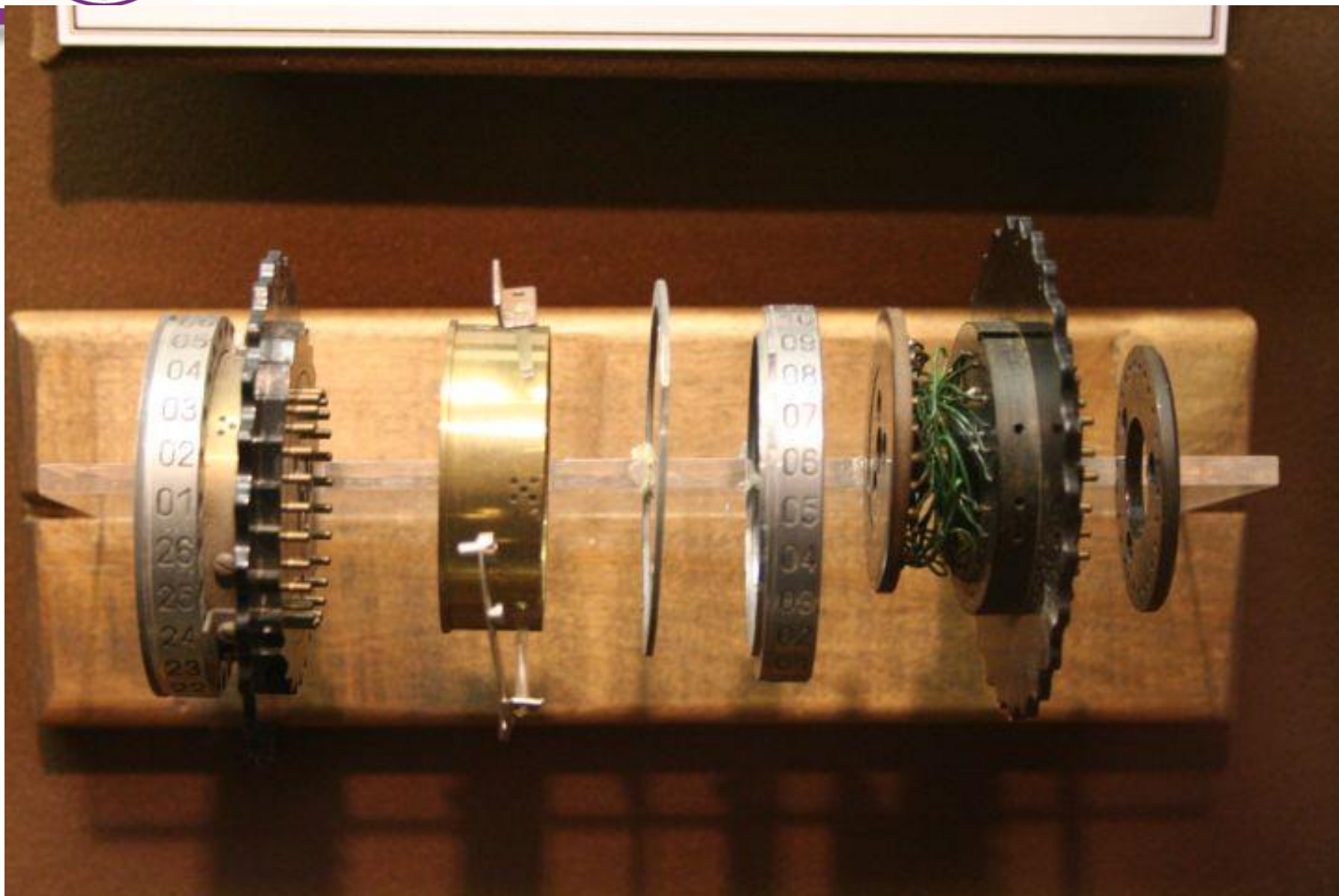
<https://www.bilibili.com/video/av21919076/?p=2>

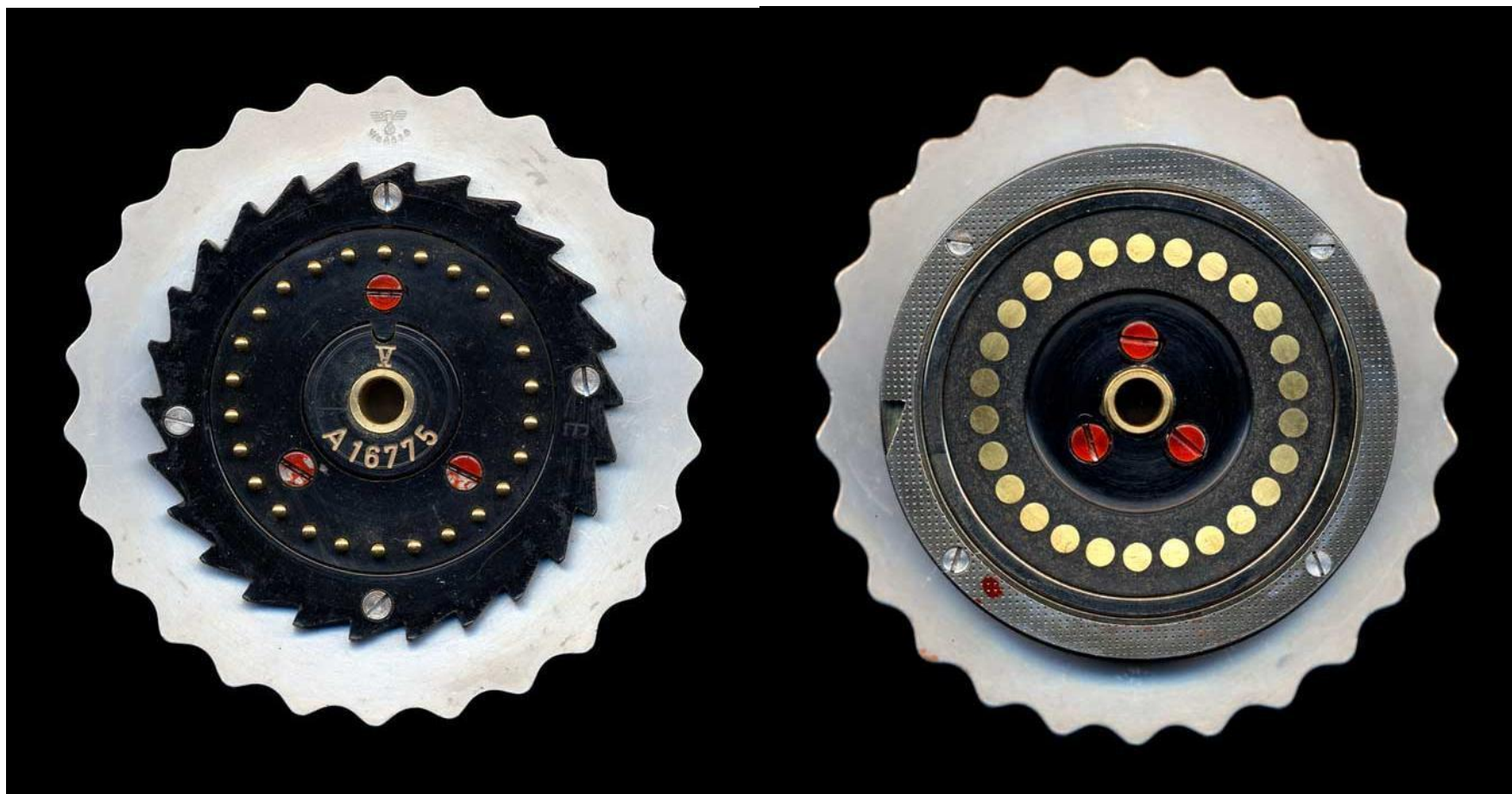
思考：

1. Enigma密码机各个部件的组成和作用？
2. Enigma密码机的密钥空间有多大？



转轮

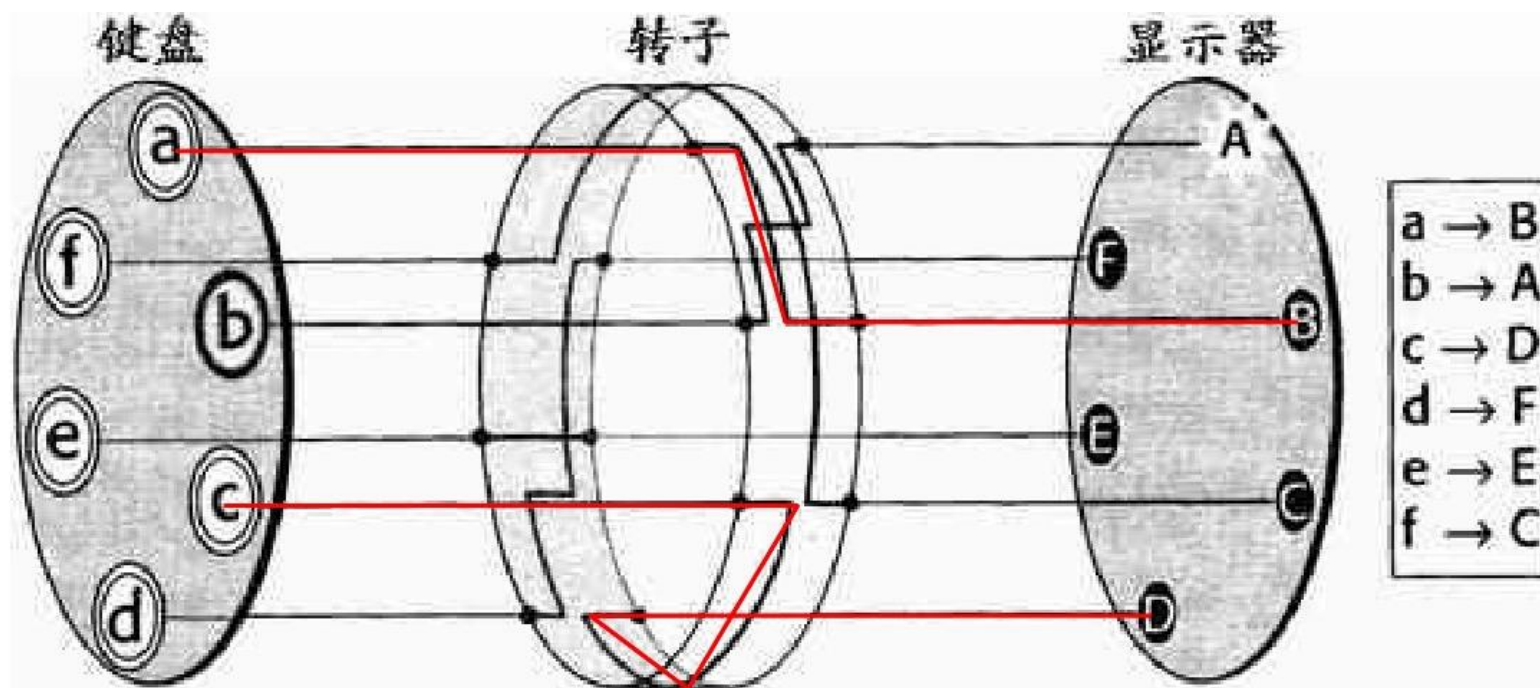


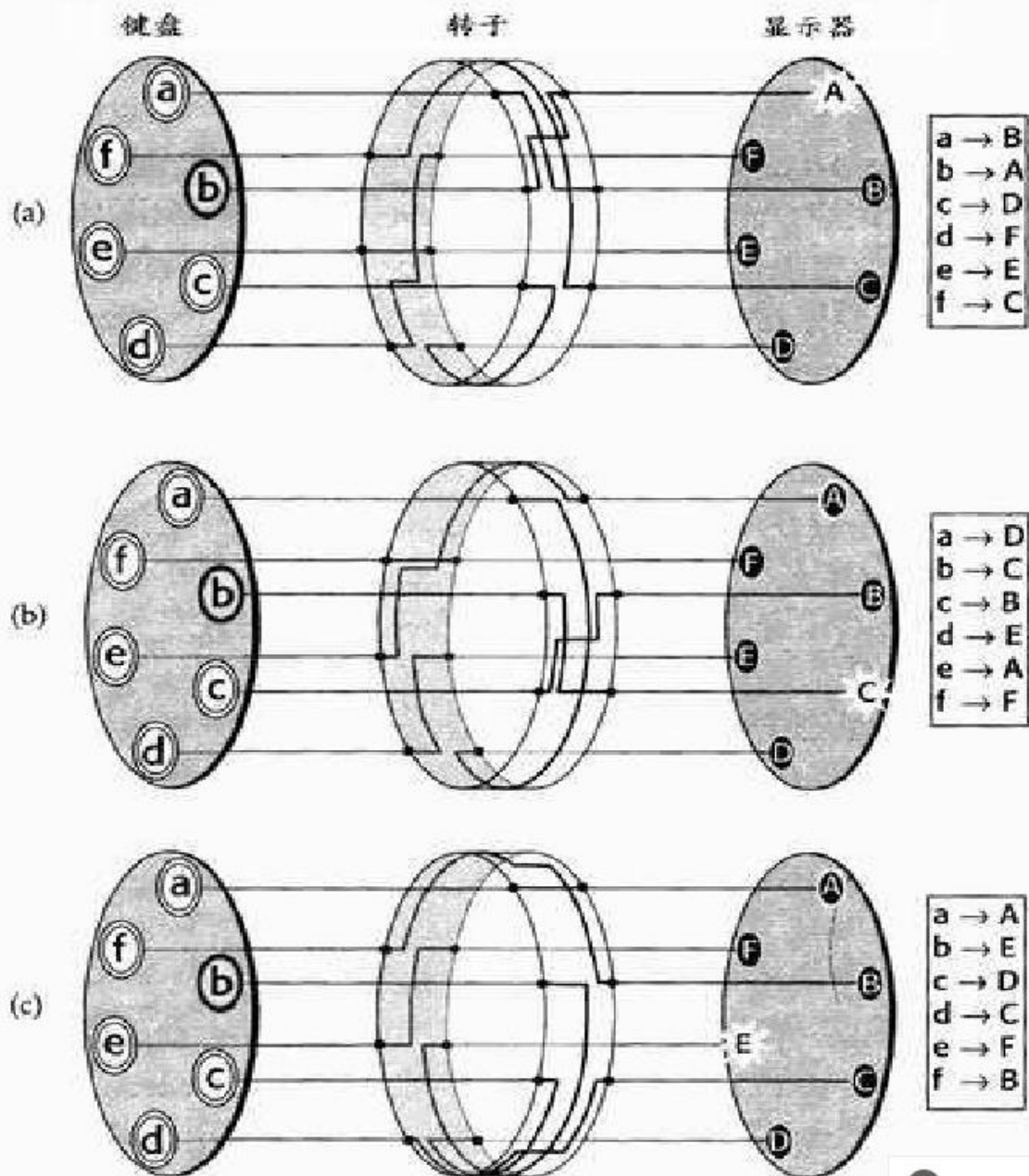




每输入一个字母以后，第一个转子都会自动转动一格，当第一个转子转动一圈后，会带动第二个转子转动一格。同理，第二个转子转动一圈后，第三个转子转动一格。

每加密一个字母就更换一次密码表





1,5,1,2,0,3

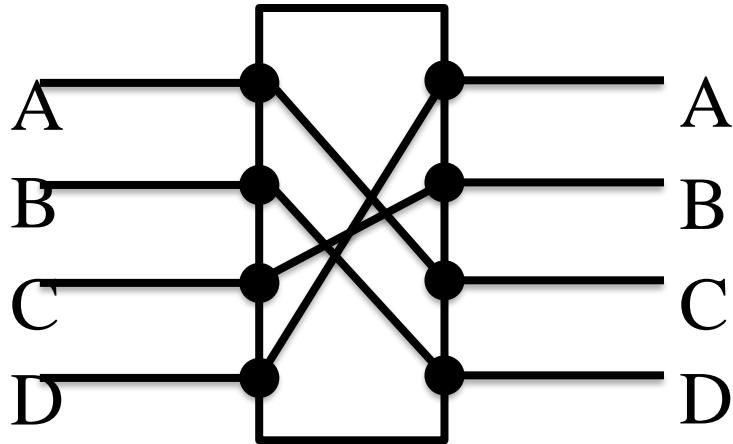
3,1,5,1,2,0

0, 3,1,5,1,2

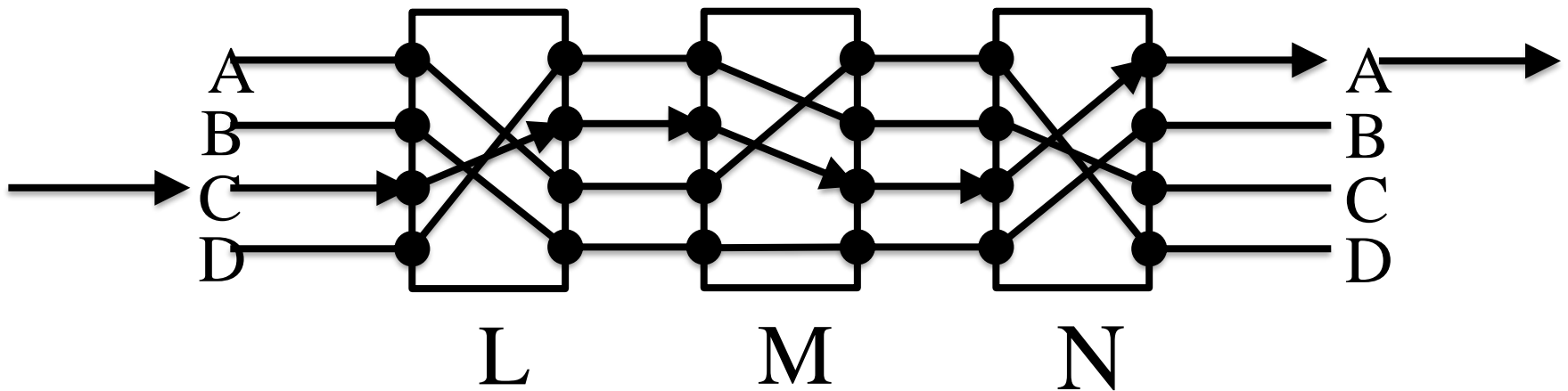
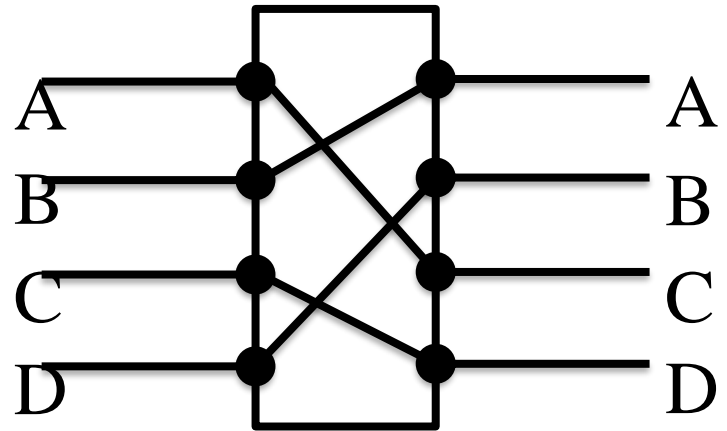


二战中的Enigma密码

转轮初态: (2,2,3,1)



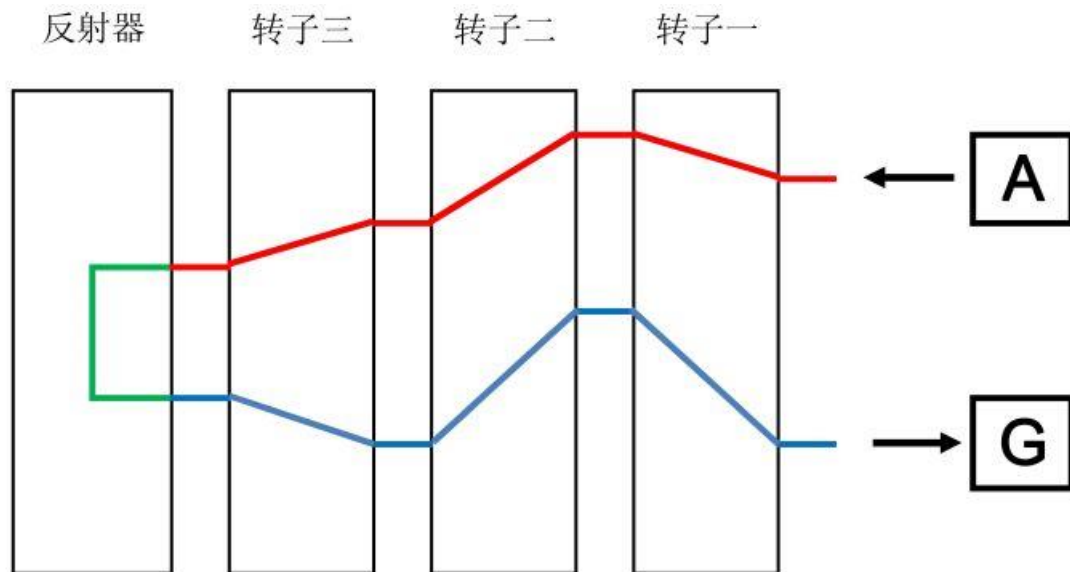
转轮驱动一次: (2,3,1,2)





反射器

□ 13对字母两两交换

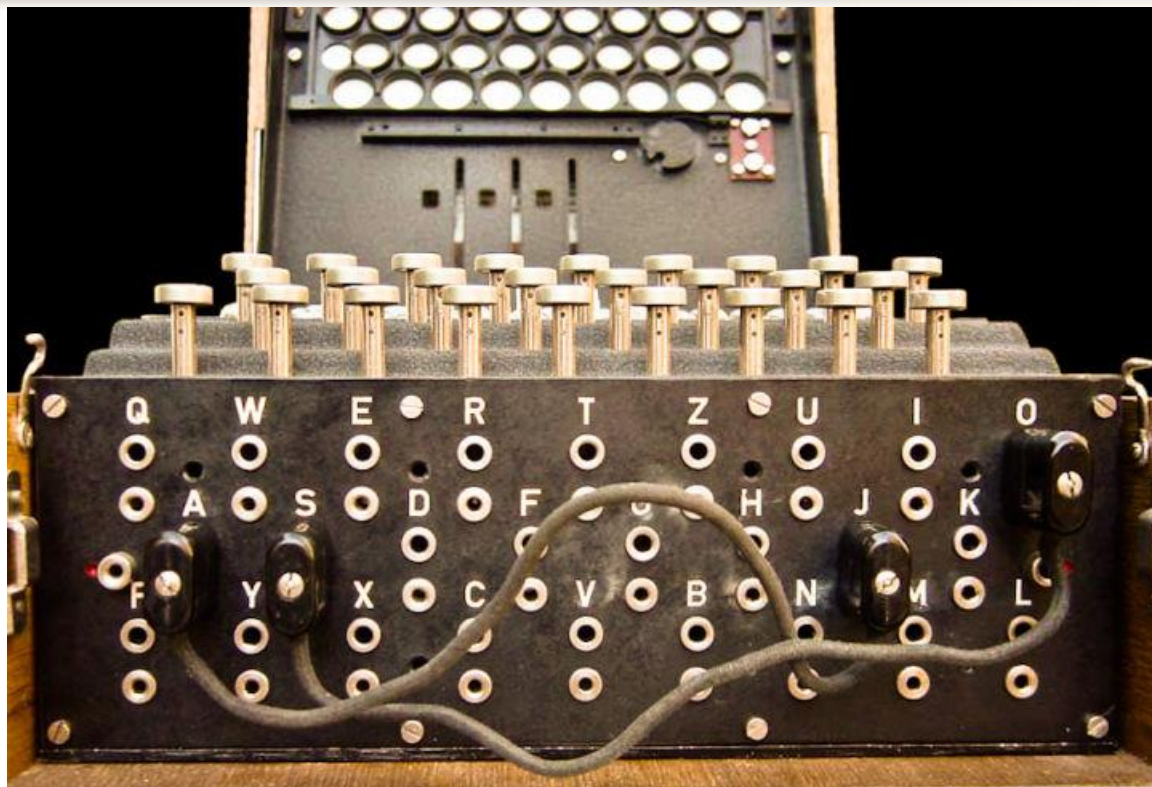


□ 反射器作用：

- 加密过程是自反的
- 一个字母加密后输出的结果绝对不会是他自身



插线板



早期Enigma：任意
交换6对，有1000亿
种组合

后期：交换10对



Enigma密码机的使用

1. 3个转子的顺序：（例，从左向右标号2-3-1）
 2. 三个转子的位置（三个转子分别转动到Q-V-W）
 3. 插线板的设置：对哪些字母进行交换
- 问题：密钥空间多大？

Enigma 模拟器：

<http://enigmaco.de/enigma/enigma.html>



日密钥和信息密钥

- 日密钥：加密信息密钥 （主密钥）
- 信息密钥：加密一条信息 （会话密钥）

随机选取TGS作为信息密钥， 用日密钥加密的密文BMXYUI

每天信息的前6个字母是信息密钥的密文



Enigma破解

□ 第一阶段

- Schmidt出卖Enigma文件给法国
- 1932年，三个波兰的数学家，雷臼斯基(Rejewski)，破解了三个扰频器的Enigma

□ 第二阶段

- 1938年，德国将三个扰频器增加到5个，连线板由6根信号线变为10根，雷臼斯基技术破解受限制
- 1939年，波兰将破解技术提供给法国和英国图灵破解Enigma



Enigma密码破解（波兰）

□需要三部分信息：

- Enigma的设计原理和内部结构：转子的内部连接，反射器的连接
- 德军对Enigma机的操作守则
- 每日Enigma机的初始设置（日密钥）

□XYZ 加密成HGABLE

H-B的关系：

$X(A0)=H, Y(A1)=G, Z(A2)=A,$

$X(A3)=B, Y(A4)=L, Z(A5)=E$

$\Rightarrow H(A0)(A3)=B$



Enigma密码破解

第一个字母: 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

第四个字母: F Q H P L W O G B M V R X U Y C Z I T N J E A S D K

观察:

A→F→W→A

3个字母的循环圈

B→Q→Z→K→V→E→L→R→I→B

9个字母的循环圈

C→H→G→O→Y→D→P→C

7个字母的循环圈

J→M→X→S→T→N→U→J

7个字母的循环圈

如果没有插线板,遍历A0, 可以破解。

有接线板呢?

1. 假设原来线路链接是将S和G互换。更改一下设置, 将S和G之间导线移除, 字母链就变为?
2. 将T和K进行链接, 字母链变为?



第一个字母: 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

第四个字母: F Q H P L W O G B M V R X U Y C Z I T N J E A S D K

将S和G之间导线移除

第一个字母: 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

第四个字母: F Q H P L W T S B M V R X U Y C Z I O N J E A G D K

将T和K进行链接

第一个字母: 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

第四个字母: F Q H P L W K S B M N R X U Y C Z I O V J E A G D T

循环圈就变成了:

A→F→W→A

B→Q→Z→T→V→E→L→R→I→B

C→H→S→O→Y→D→P→C

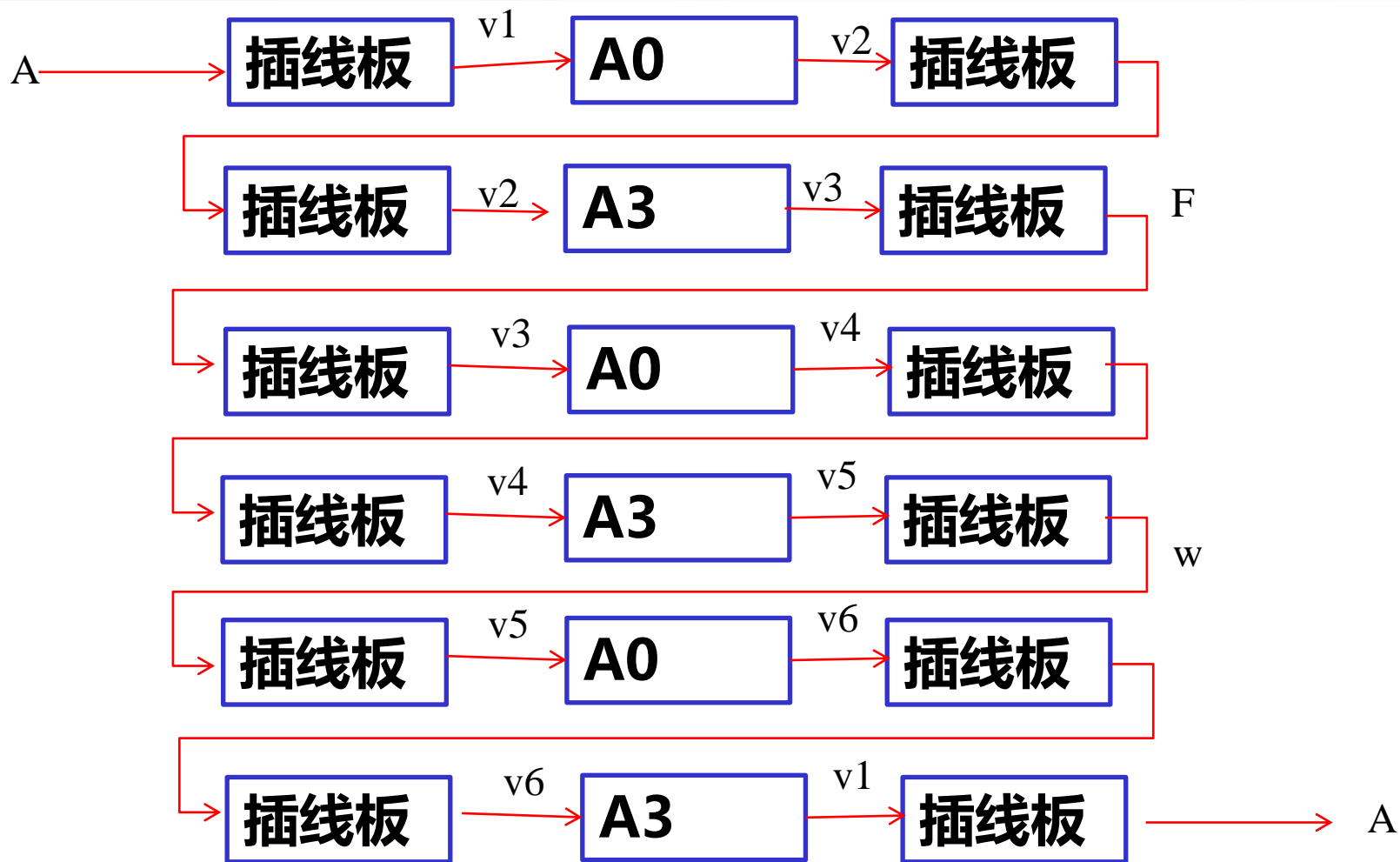
J→M→X→G→K→N→U→J

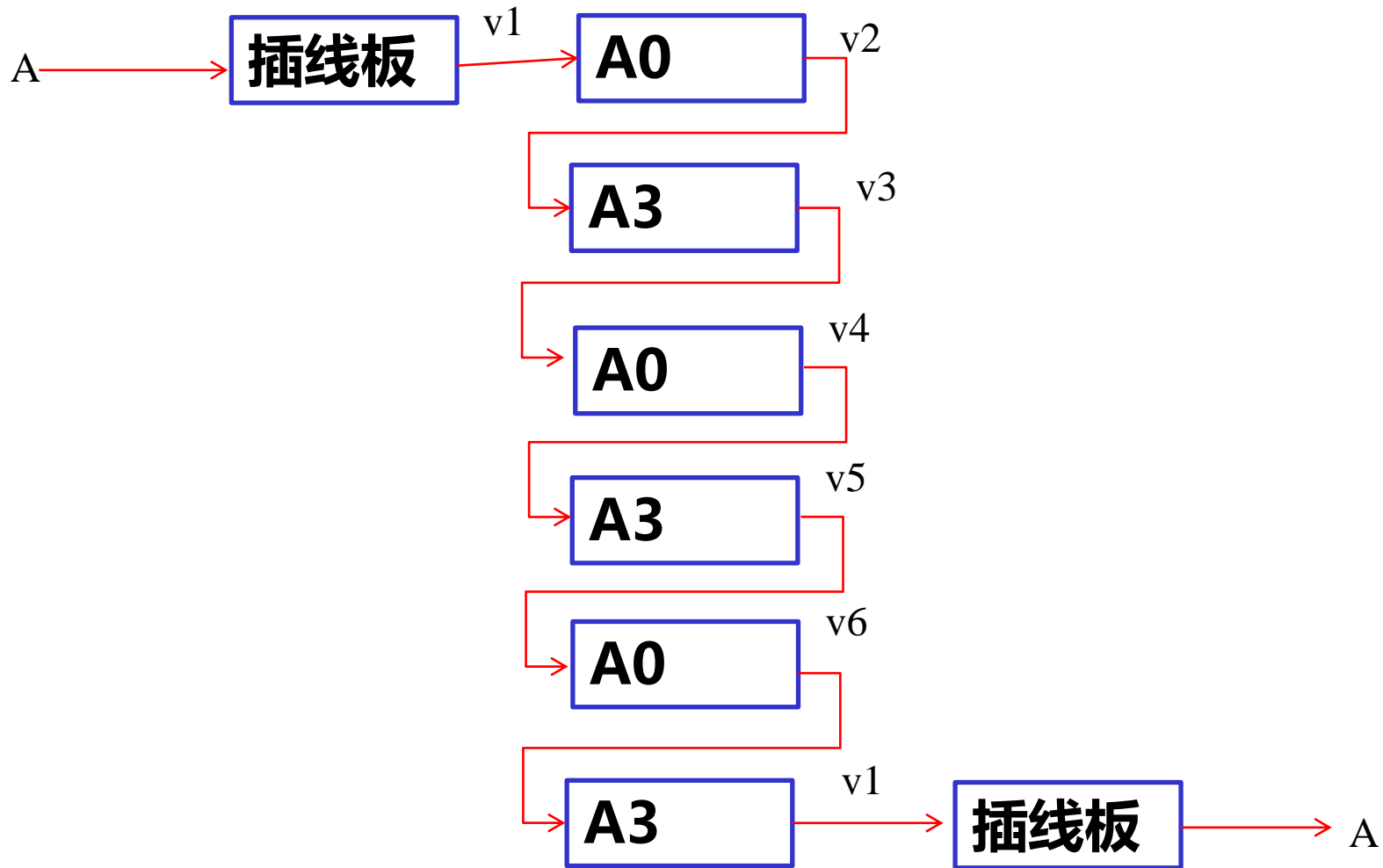
3个字母的循环圈

9个字母的循环圈

7个字母的循环圈

7个字母的循环圈







Enigma密码破解

重要发现：字母链的数目和长度不变！

字母链数目3,9,7,7，四条字母链，由字母1和4推得。

字母链数目2,3,9,12，四条字母链，由字母2和5推得。

字母链数目5,5,5,3,8 五条字母链，由字母3和6推得。



Enigma密码破解（波兰）

预计算过程：

对10万个转子位置（密钥）进行遍历。每一个密钥产生字母表的链条数和链长，产生分类目录（一年时间）

破解步骤：

1. 根据当日截获的每一封电报的前6个字母推导出字母链条的数量和长度
2. 在分类目录中找到可能的转子设置
3. 针对所有可能的转子设置进行暴力破解



Enigma密码机的破解

问题： 转子位置确定后，如何确定接线板的设置？

将密文输入复制的Enigma机，移除所有的导线，得到不可辨认的乱码。可是仍然会有模糊可辨的词组或短语。如alliveinbelrin, 可能是arrive in berlin. 推断L和R交换, A, I, V, E, B, N 没有导线。



Enigma密码的破解

□ 二战爆发前后，Enigma密码的安全性加强

- a) 1938年9月15日开始，德军干脆连日密钥中的转子位置也让操作员自己选择。这样一来，就连每条信息的前六个字母也变成是用不同密钥加密的了。
- b) 1938年12月15日，德军把转子的数量从三个增加到了五个，安装的时候从五个里面随机选三个安装在恩格玛机上，将可能的转子组合增加了10倍。更重要的是，有了多出来的转子，波兰人做的分类目录就失效了。
- c) 1939年1月1日，德军把插线板上交换字母的最大数量从6对增加到了10对。
- d) 1940年5月1日，德军规定每条信息的信息密钥发送一遍即可，无需重复两次。



二战中的Enigma密码

德军的日密钥内容就变成了以下三个部分：

- 1) 从五个转子中选择三个特定的转子，并按一定顺序排列；
- 2) 每个转子外侧的字母圈相对于转子芯的位置；
- 3) 插线板所交换的10对字母；

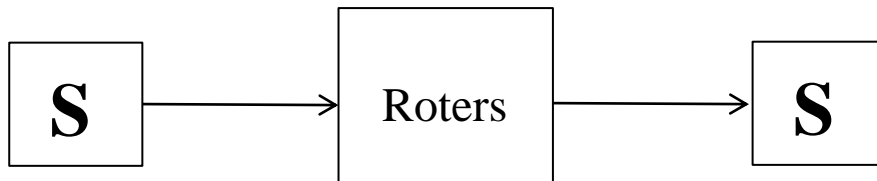


Enigma密码破解（图灵）

已知明文攻击：

Wetterbericht (weather report)

j x a t q b g g y w c r y b g ...
w e t t e r b e r i c h t



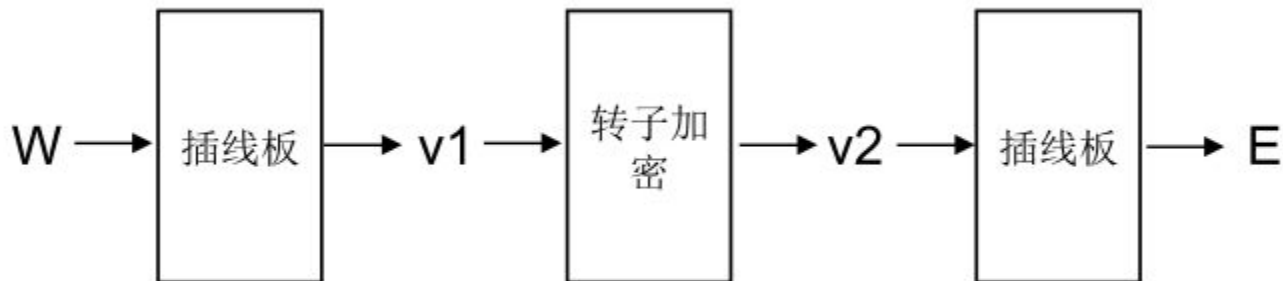


Enigma破译（图灵）

- Enigma加密算法：

$$y = S^{-1}N^{-1}M^{-1}L^{-1}RLMNS(x) = (LMNS)^{-1}RLMNS(x)$$

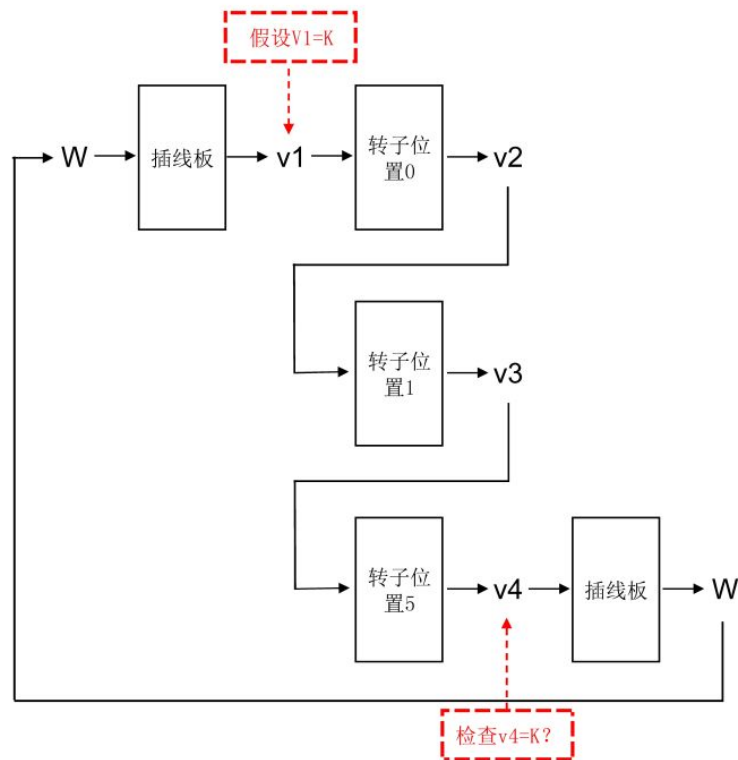
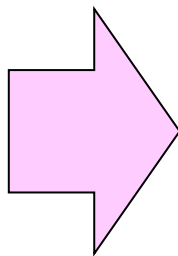
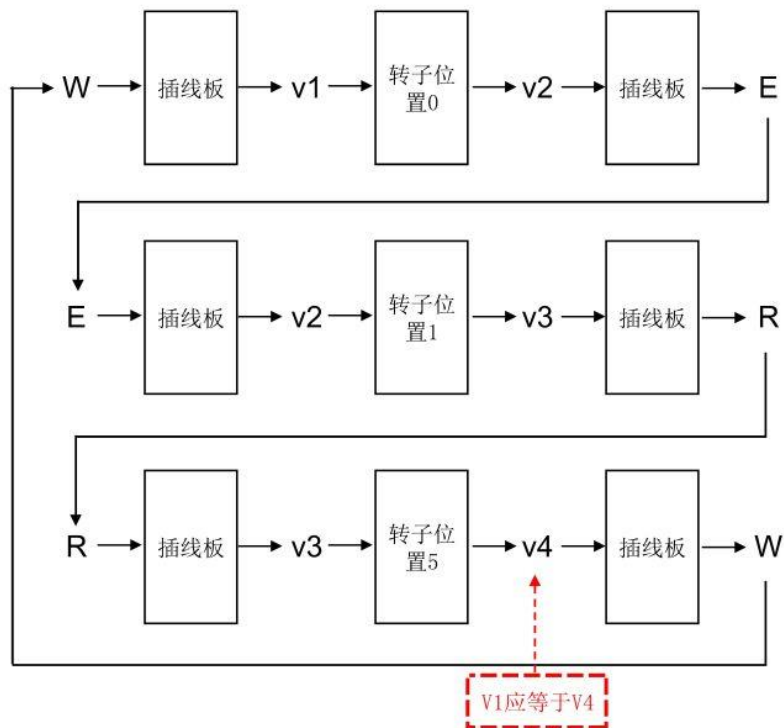
已知明文攻击：





Enigma破译（图灵）

明文 W E T T E R
密文 E R K M G W



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

□ $P_i = N^{-1}M^{-1}L^{-1}RLMN$ 则 $P_i S(x) = S(y)$

例： $P_8 S(A) = S(M)$; $P_6 S(M) = S(E)$; $P_{13} S(E) = S(A)$

则 $S(E) = P_6 P_8 P_{13} S(E)$

密钥恢复过程：

猜测转轮初始值，则 P_i 确定。

猜测 $S(E)$ 的值： $G = P_6 P_8 P_{13}(G)$

□ 如果对26个猜测值都不成立，排除掉一个密钥；

□ 如果对26个猜测值有一个成立，猜测的转轮初值是否正确？（不能确定）



攻击过程：

□找第二个圈：

$$S(E)=P_3S(R); S(W)=P_{14}S(R); S(W)=P_7S(M);$$
$$S(E)=P_6S(M)$$

$$\text{则 } S(E)=P_3P_{14}^{-1}P_7P_6^{-1}S(E)$$

猜测 $S(E)=G$ ；则满足两个圈的概率为 $(1/26)^2$ 。

5个转轮的Enigma密钥空间由 2^{30} 缩减为
 $2^{30}/26=2^{25.3}$ 。

如果找到 n 个圈，则密钥空间缩减为 $2^{30}/(26)^n$



Enigma Attack(猜测转轮的初始设置)

//Given: Cycles C_0 and C_1 for $S(\mathbf{E})$

//(L_0, L_1, \dots, L_{25}) = ($\mathbf{A}, \mathbf{B}, \dots, \mathbf{Z}$)

for each rotor setting

Computing required permutations to test C_0 and C_1
for $j = 0$ to 25

$S(\mathbf{E}) = L_j$

if C_0 and C_1 hold then

save putative rotor settings and $S(\mathbf{E})$

value L_j

end if

next j

next rotor setting



Bombe Machine





问题：

□ 如何恢复接线板的设置？

假设使用上面的攻击方法恢复了转轮的初始位置，而且 $S(E)$ 已恢复，如何恢复其他的接线板设置？



谢谢！