战争之“谜”

曾经世界危在旦夕的“谜机”

毛昕渝 2021/11/07

Enigma机，战争与计算机

Enigma机是什么？

- 一种密码机：有加密消息、解密消息的功能。
- Enigma 在拉丁语中的意思是“riddle, 谜”。
- 由德国工程师 Arthur Scherbius 发明
- 在二战中被纳粹德军广泛使用，用于军事通信。

特点：用一台机器实现了加密、解密功能，并且加密、解密的操作完全相同。

Example.

```
Input:  HELLO WORLD
Output: JXQXJ RFYUM
```

```
Input:  JXQXJ RFYUM
Output: HELLO WORLD
```

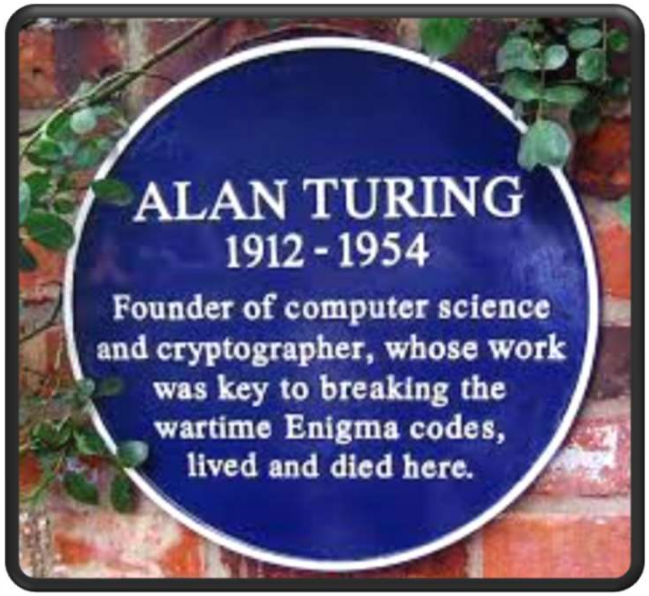
破解Enigma机有多难?

Enigma 的可能状态数:

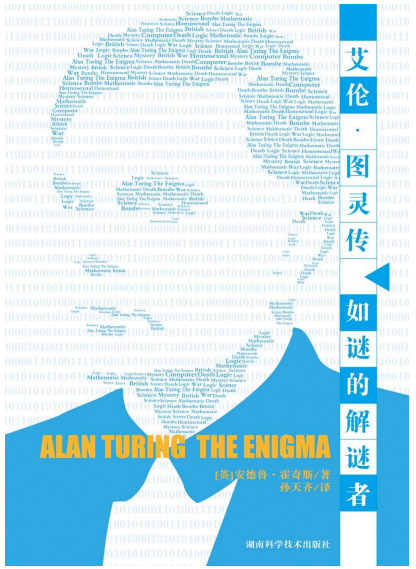
$$107{,}458{,}687{,}327{,}250{,}619{,}360{,}000 \approx 1.07 \times 10^{23}$$

- 1927 Enigma机 诞生。
- 1928 德国军方首次大规模采购Enigma机。
- 1940 Enigma机被成功破解。
- 整整十三载!
- 后来德军多次改进Enigma机，使其可能状态数更多。

图灵：如谜的解谜者

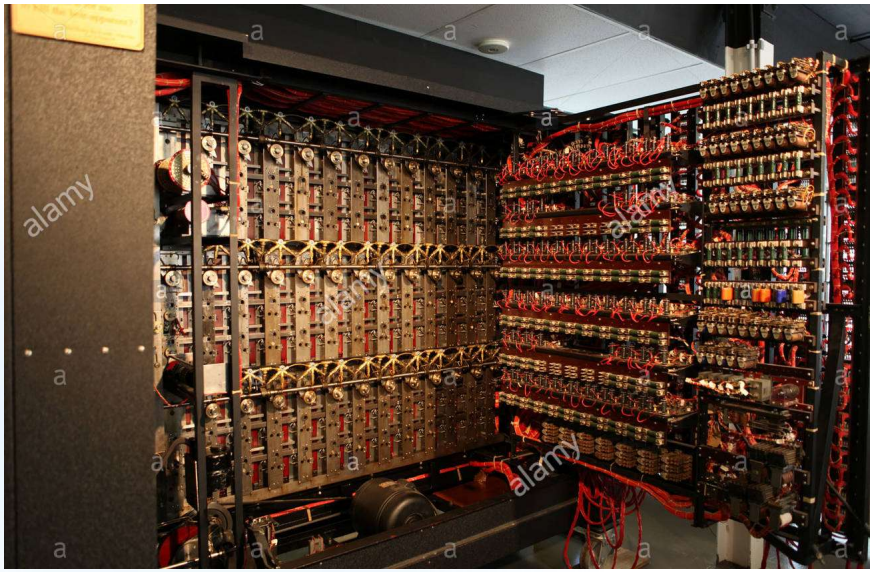


计算机科学的奠基人，
密码分析家，
他的工作是战时破解Enigma密码的关键。

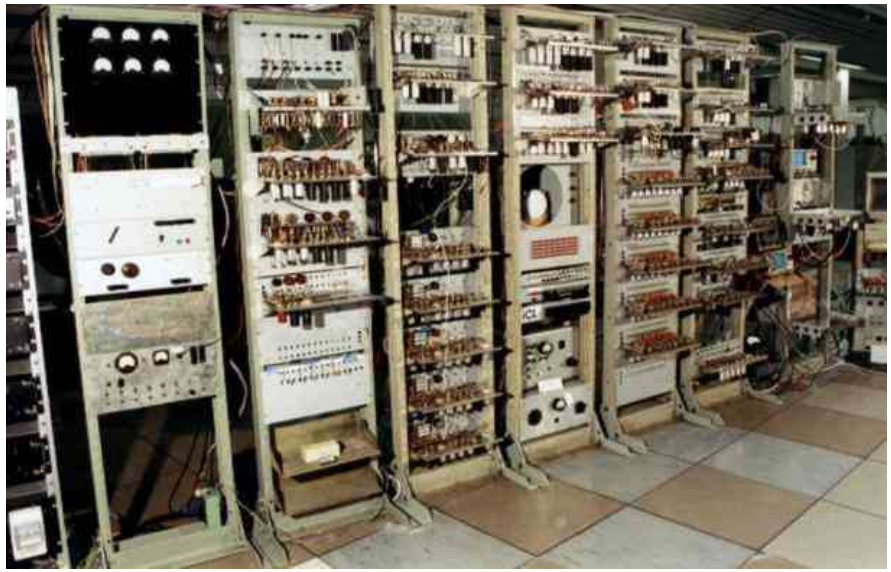


Alan Turing: The Enigma
By Andrew Hodges
中文版：
《图灵传：如谜的解谜者》

从“炸弹”机到计算机



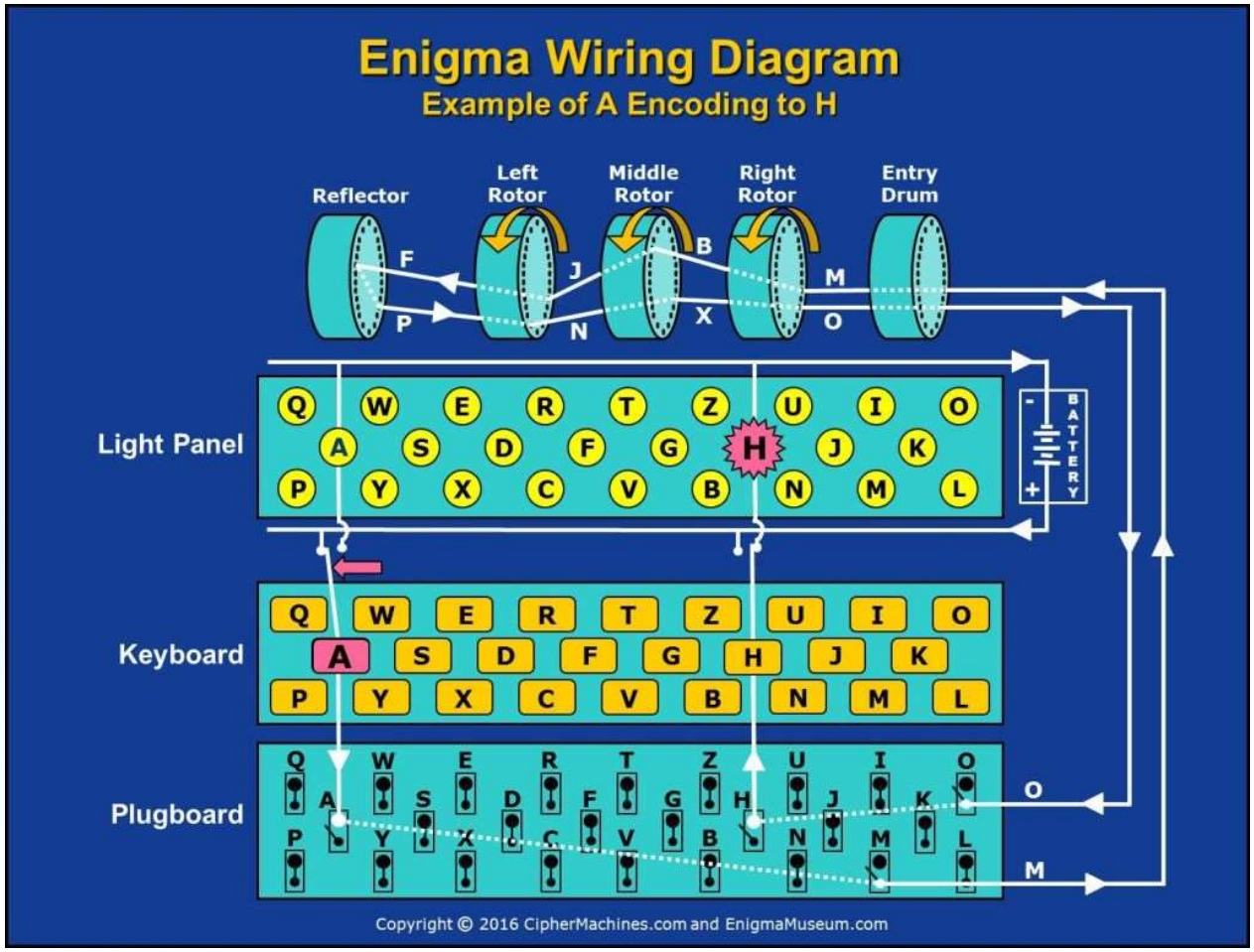
1940 Bombe
图灵等人为破解Enigma机建造的“炸弹”机



1944 Manchester Mark I
最早的可编程计算机之一

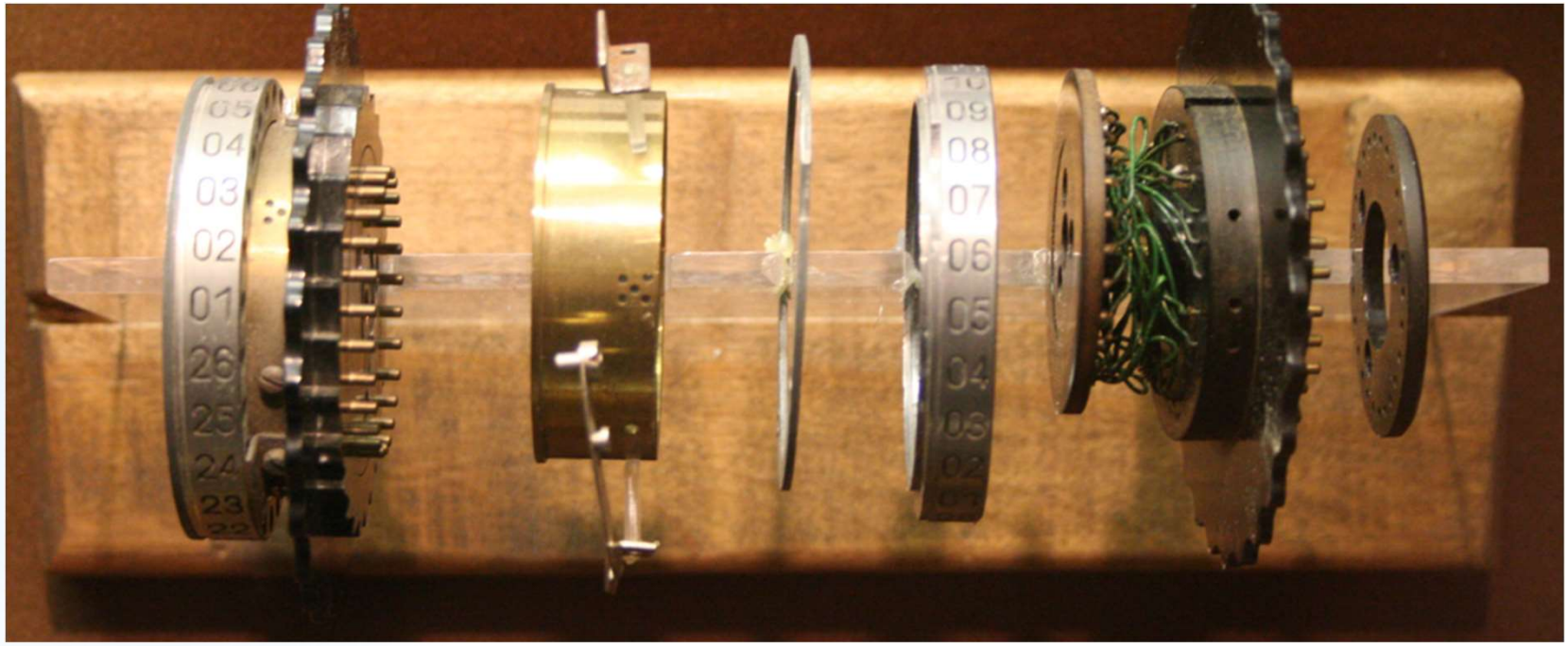
理解Enigma机

Enigma的加密原理



- 反射板是13组两两对换。
- 每次输入后最右边的齿轮旋转一次。
- 最右边的齿轮转动一圈将带动右数第二个齿轮转动一次。

齿轮的内部结构



置换（Permutation）

置换

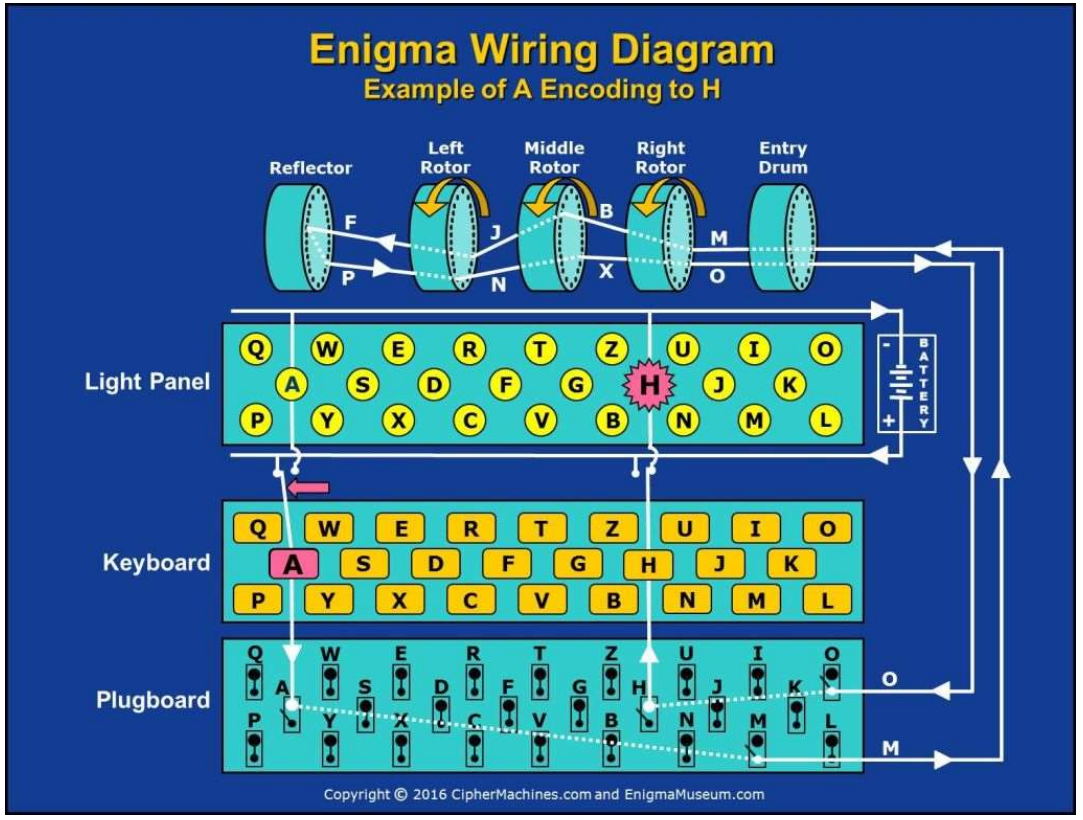
从有限集合 X 到其自身的双射称为 X 上的置换。

- 与集合的元素具体是什么无关，不妨设集合$X = [n] = \{1,2,\dots,n\}$.
- $S_n :=$ $[n]$上的置换组成的集合.
- 恒等映射记为 e.
- 置换的乘法（合成）:$(\sigma\tau)(i) = \sigma\big(\tau(i)\big)$.
- $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$.

用置换来描述Enigma的加密过程

$$P^{-1}R^{-1}M^{-1}L^{-1}FLMRP$$

- P（plugboard）：连接板
- L, M, R：三个转子
- F：反射板
- 右边的转子旋转一次?
- $P^{-1}(\sigma R^{-1}\sigma^{-1})M^{-1}L^{-1}FLM(\sigma R\sigma^{-1})P$
- $\sigma = (abcdefghijklmnopqrstuvwxyz)$



置换的一些性质

循环

对于置换 $\sigma \in S_n$, 如果存在$i_1, \dots, i_k$ 满足如下条件，则称之为k −循环:

- $\sigma(i_t) = i_{t+1}, \forall t \in [k-1]$;
- $\sigma(i_k) = i_1$;
- $\sigma(i) = i, \forall\, i \in [n] \setminus \{i_1, \dots, i_k\}$

$$i_1 \xrightarrow{\sigma} i_2 \xrightarrow{\sigma} \cdots \xrightarrow{\sigma} i_k \xrightarrow{\sigma} i_1$$

置换的循环分解

置换的循环分解：置换可以分解为若干不相交循环的乘积。如果不考虑次序的话，分解是唯一的。

共轭置换

置换的共轭

设$\sigma \in S_n, \tau \in S_n$, 我们称 σ和τ 共轭（记作$\sigma \sim \tau$）当且仅当 $\exists \delta \in S_n$ 使得 $\sigma = \delta^{-1}\tau\delta$.

共轭置换的循环分解

设$\sigma \in S_n, \tau \in S_n$, 而且$\sigma, \tau\sigma\tau^{-1}$的循环分解为：

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_n, \tau\sigma\tau^{-1} = \pi_1 \cdots \pi_m.$$

适当调整次序可以得到：

$$m = n \text{ 并且 } |\pi_i| = |\sigma_i|, \forall i \in [n].$$

- 上述定理的逆命题也成立
- 有关共轭的置换方程：已知τ, σ, 求δ 使得 $\delta\sigma\delta^{-1} = \tau$.

Enigma对应的置换

- $E = P^{-1}R^{-1}M^{-1}L^{-1}FLMRP$

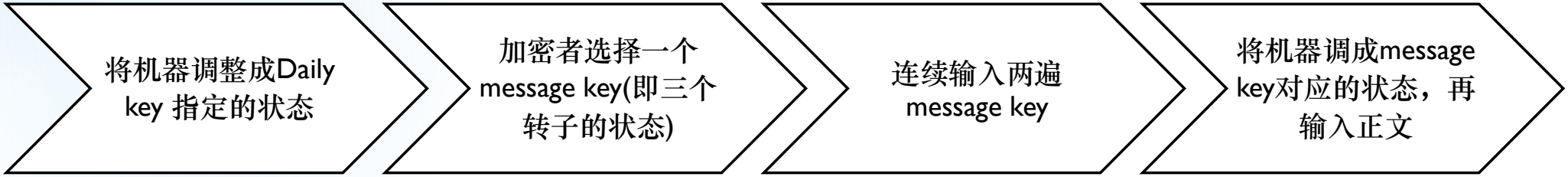
- F是由13个不相交的对换组成的
- E也是由13个不相交的对换组成的
- $E^2 = e$

破解Enigma：解谜接力赛

德军如何使用Enigma进行加密


```
Daily key (shared secret):
  Wheel Order   : II   I   III
  Reflector     : A
  Plugboard     : A-M, F-I, N-V, P-S, T-U, W-Z
  Grundstellung: FOL

  Operator chosen message key : ABL
  Enciphered starting with FOL: PKPJXI
```



密码研究领域的“波兰三杰”

马里安·亚当·雷耶夫斯基
（Marian Adam Rejewski，
1905年8月16日－1980年2月13日）

雷耶夫斯基与波兰数学家杰尔兹·罗佐基和亨里克·佐加尔斯基并称为密码研究领域的“波兰三杰”。

Rejewski's 的例子

DMQ VBN
VON PUY
PUC FMQ
.....

假设Enigma机处于 Daily key 设置时，对前6个字母的加密对应置换 $\sigma_i, i = 1,2,3,4,5,6.$

$\sigma_4\sigma_1 = (dvpfkxgzyo)(eijmunqlht)(bc)(rw)(a)(s)$

$\sigma_5\sigma_2 = (blfqveoum)(hjpswizrn)(axt)(cgy)(d)(k)$

$\sigma_6\sigma_3 = (abviktjgfcqny)(duzrehlxwpsmo)$

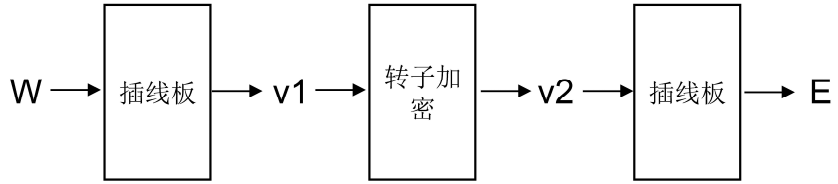
这些循环节的特征只由转盘的状态决定，与反射板无关。因此循环节的特征被破译者们称为Characteristic of the day.

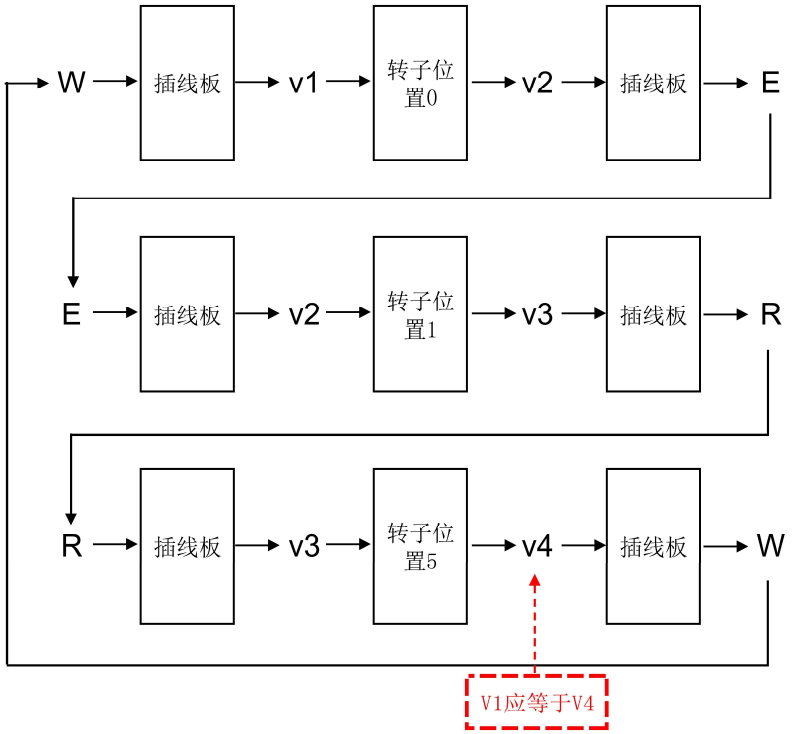
昙花一现的曙光

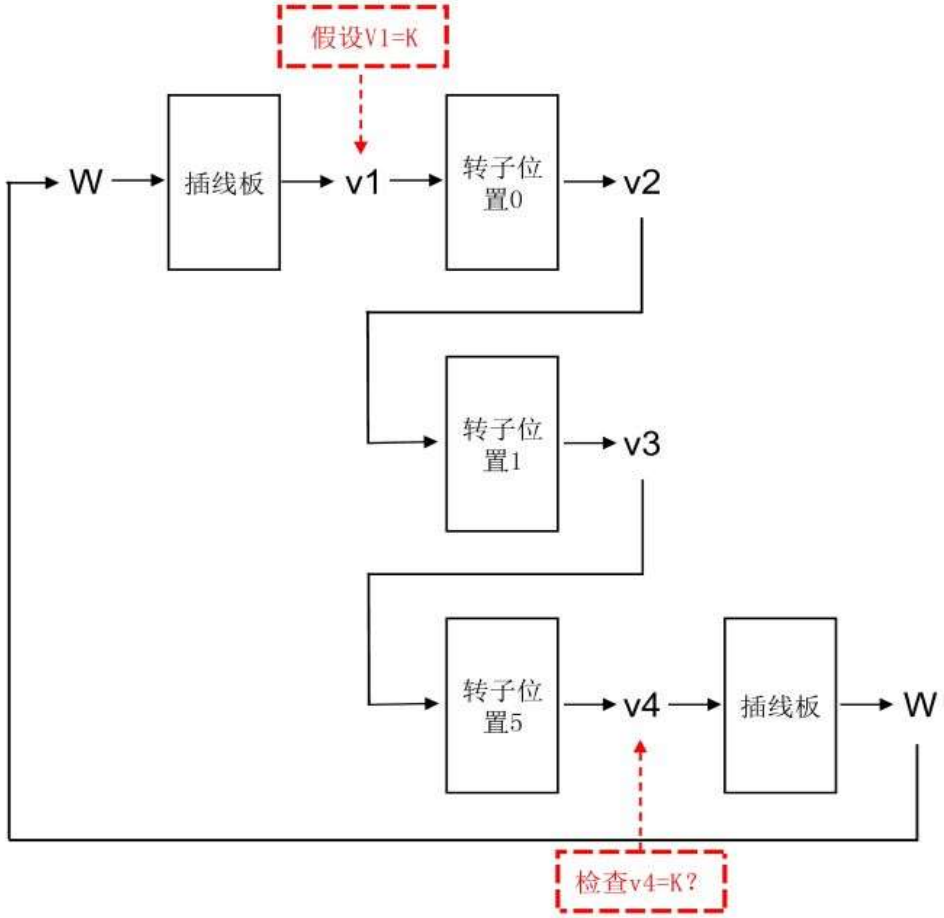
- 通过更加精细的分析，可以通过$\sigma_1\sigma_4, \sigma_2\sigma_5, \sigma_3\sigma_6$解出$\sigma_i$,进而解出最左侧转子对应的置换$R$。
- 通过“特征”给转子的设置情况分类，人力枚举所有可能。
- 插线板的设置可以通过猜 + 试 + 情报。
- 1938年12月15日，德军把转子的数量从三个增加到了五个，安装的时候从五个里面随机选三个。
- 1939年1月1日，德军把插线板上交换字母的最大数量从6对增加到了10对。
- 1940年5月1日，德军规定每条信息的信息密钥发送一遍即可，无需重复两次。

图灵：用机器战胜机器

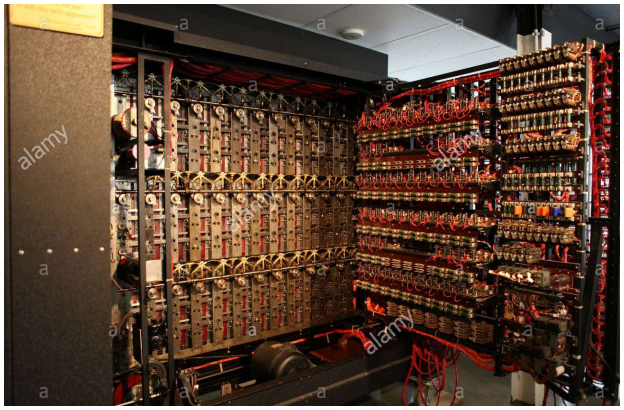
明文 W E T T E R
密文 E R K M G W







- 图中虽然有三台Enigma机，但它们转子之间的差距是确定的，因此总的可能只有$60 \times 26^3 = 1054560$种。
- 剩下的交给机器。



反思Enigma：怎样才算“安全”？

- 密钥空间大 ≠ 安全
- 计算机的计算能力有多强？局限在哪里？
- 计算机能解决/不能解决什么问题？
- 怎样定义安全？
- 安全的密码系统可能吗？如何实现？
- ……

Thanks for listening. ☺