Decrypted Secrets:
Methods and Maxims of Cryptology
(Second Edition)

网络与信息安全技术丛书

只有密码分析者
才能评判密码体制的安全性

密码编码和密码分析

原理与方法

(德) F. L. Bauer 著
吴世忠 等译

机械工业出版社
China Machine Press
Springer

网络与信息安全技术丛书

密码编码和密码分析
原理与方法

（德） F.L. Bauer 著
吴世忠 宋晓龙 李守鹏 译

机械工业出版社
China Machine Press

本书介绍密码编码学和密码分析方法，对破译密码的方法提出了许多建议。本书从密码学的历史中摘录了大量史料，内容丰富，叙述生动，不仅适合密码学研究人员和网络安全技术人员参考，也适合想了解密码学的普通读者阅读。

本书版权登记号：图字：01-2000-1572

图书在版编目（CIP）数据

密码编码和密码分析：原理与方法/（德）保尔（Bauer, F. L.）著；吴世忠等译. -北京：机械工业出版社，2001.9

（网络与信息安全技术丛书）

书名原文：Decrypted Secrets: Methods and Maxims of Cryptology, Second Edition

ISBN 7-111-09084-5

Ⅰ.密… Ⅱ.①保… ②吴… Ⅲ.密码-基本知识 Ⅳ.TN918.1

中国版本图书馆CIP数据核字（2001）第045572号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：李援南 张鸿斌

北京忠信诚胶印厂印刷·新华书店北京发行所发行

2001年9月第1版第1次印刷

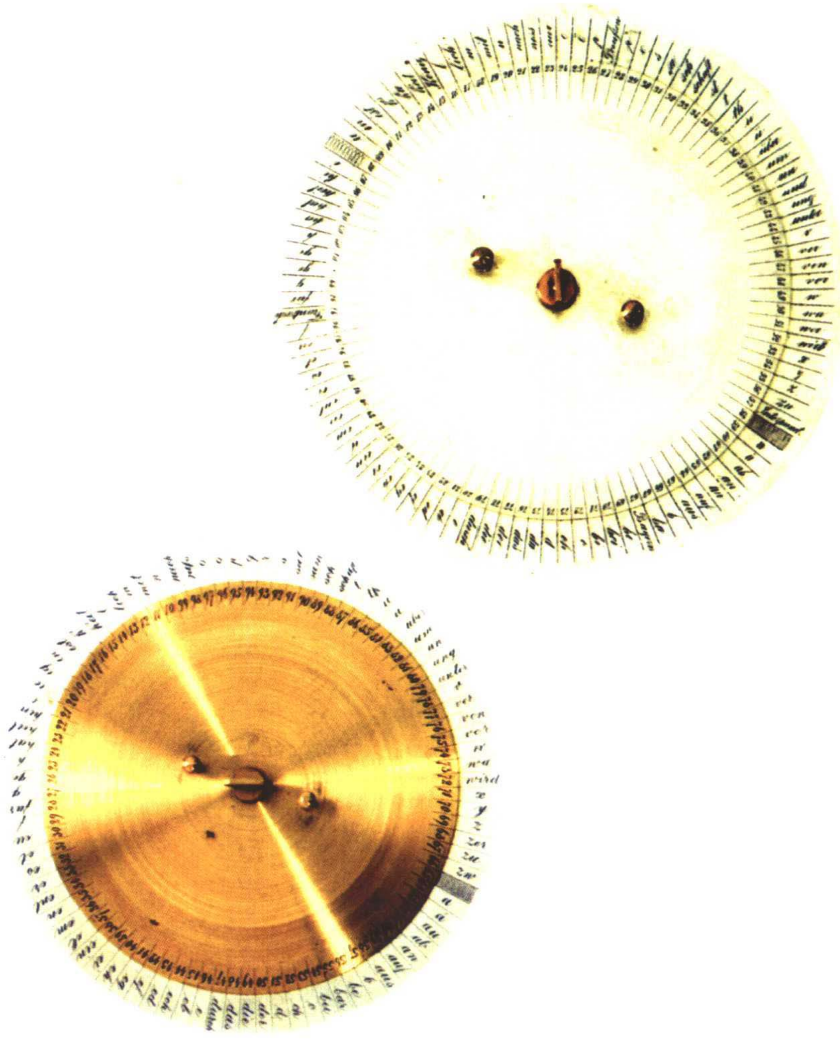
787mm×1092mm 1/16·25印张

印数：0 001-5 000册

定价：49.00元

插图A

Phaistos圆盘，一种直径约为160mm的Cretan-Minoan粘土圆盘，始于公元前17世纪。表面有明显字间空格的字母，至今还没有破解。“如果没有进一步的线索，短的报文段不会提示其含义的”（J.Friedrichs）。



插图B

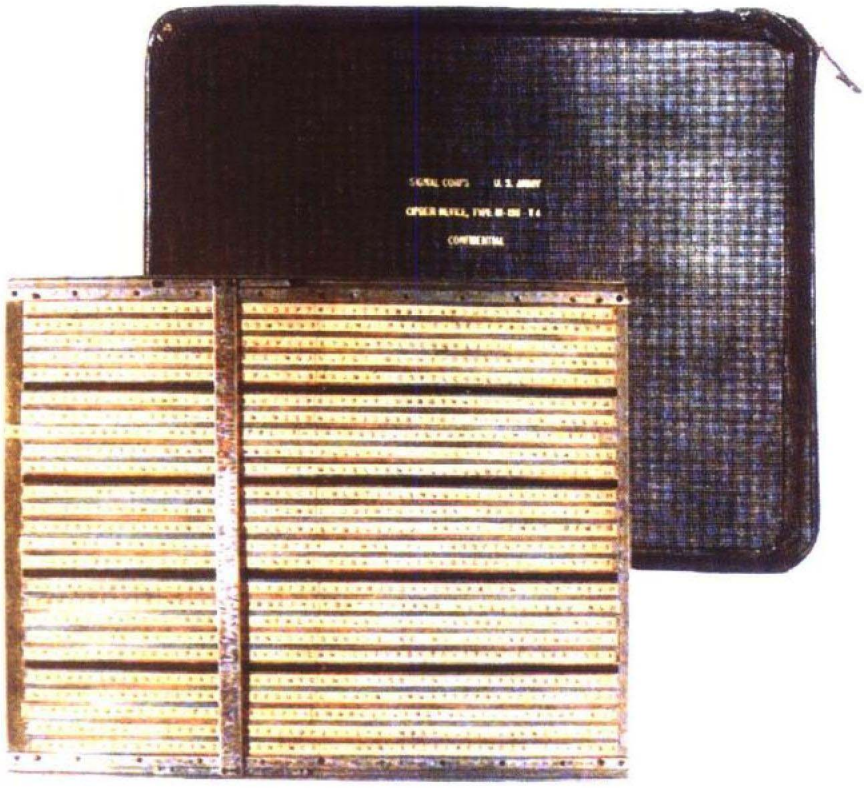
双密码盘，估计始于18或19世纪。外层圆盘上有类似词汇表的明文，明文中有字母、元音字母和常用单词，密文是由两位的十进制数组成。

插图C

惠斯通（Wheatstone）“密码”，一种钟表形式的设备，首次露面是在1867年巴黎世纪展览会上。这是一个单表加密密码设备，顺时针旋转的指针每次指向下一个明文字母，圆盘也随着混合的密文字母旋转。

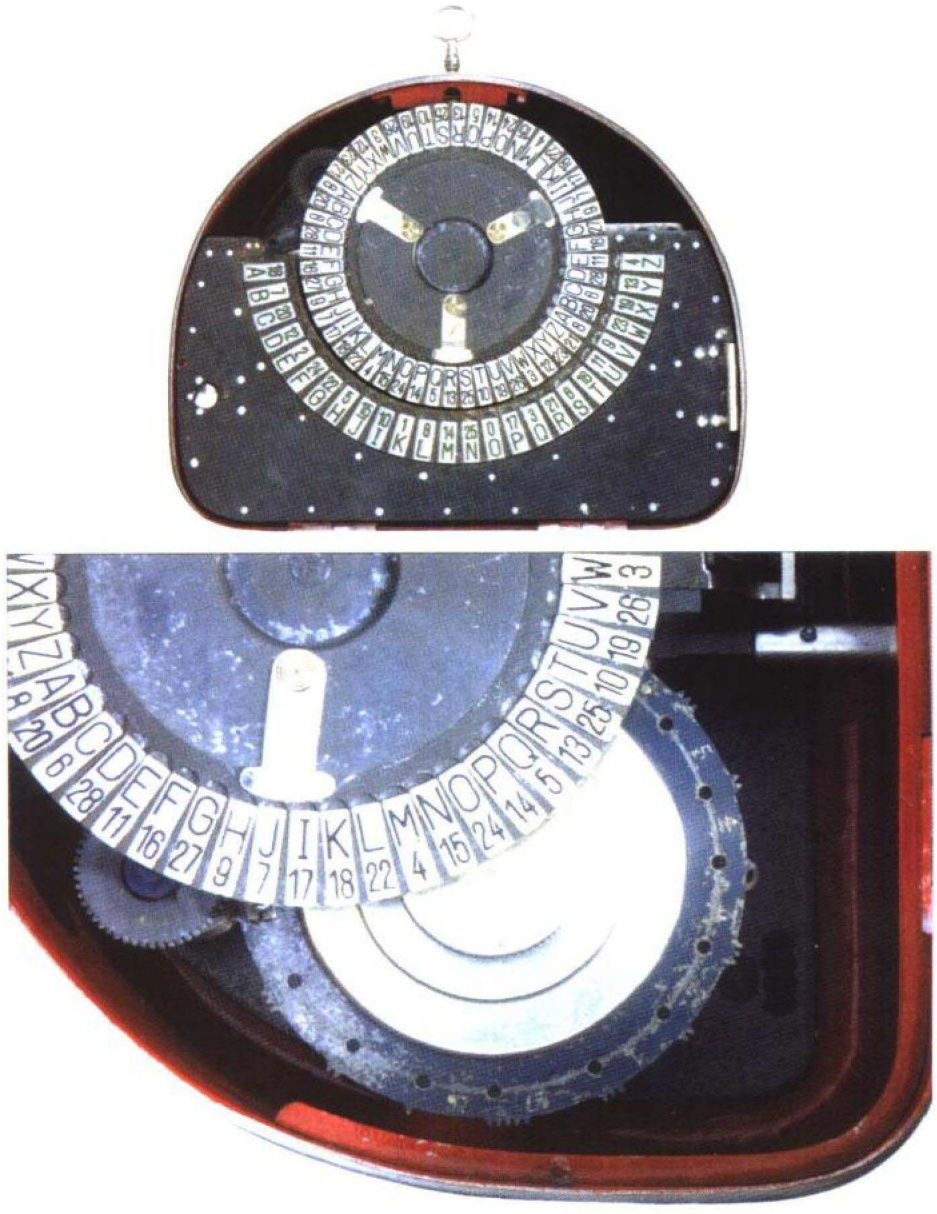
插图D

美国陆军圆柱形密码设备M-94，共有25个直径35mm的铝盘，外缘上刻有字母，它的设计思想可追溯到Jefferson（杰斐逊）和Bazeries（巴泽里埃斯）。它于1922年在W.F Friedman（威廉·弗里德曼）的建议下投入使用，主要针对低级的军事通信，1942年以前被广泛使用。



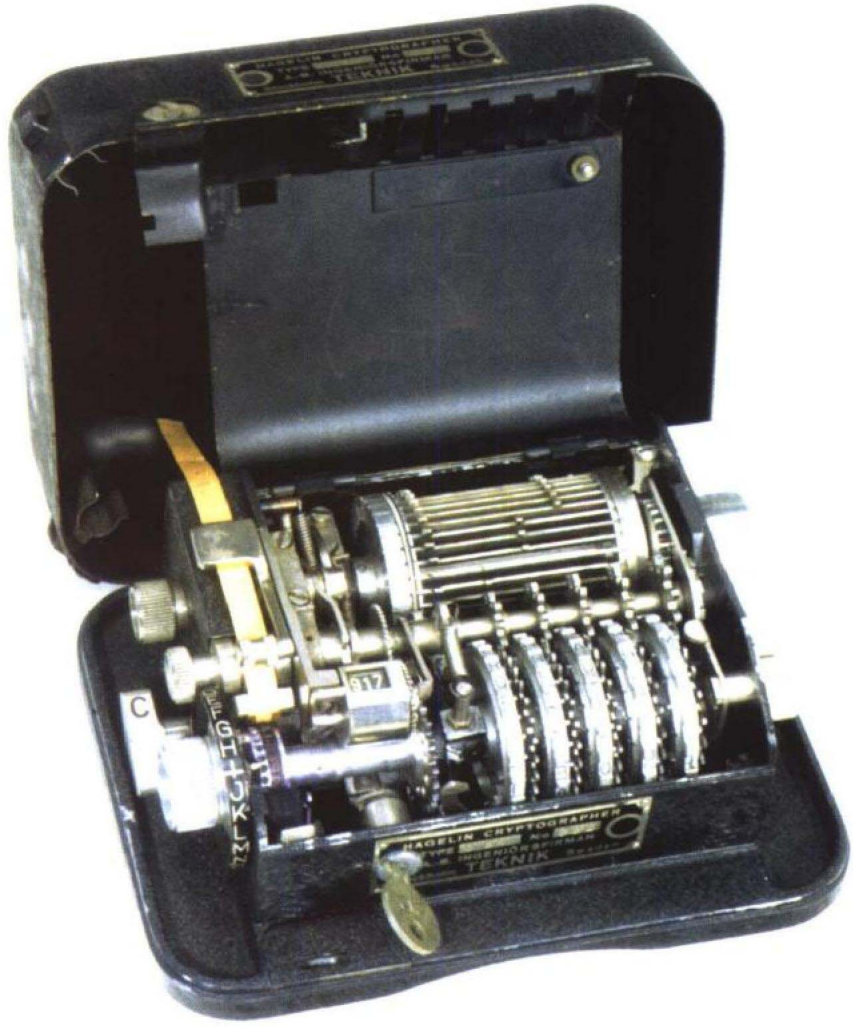
插图E

二战中美国陆军和海军使用的条形密码设备M-138-T4，根据1914年Parker Hitt的提议而设计。25个可选取的纸条按预先编排的顺序编号和使用，加密的强度相当于M-94。



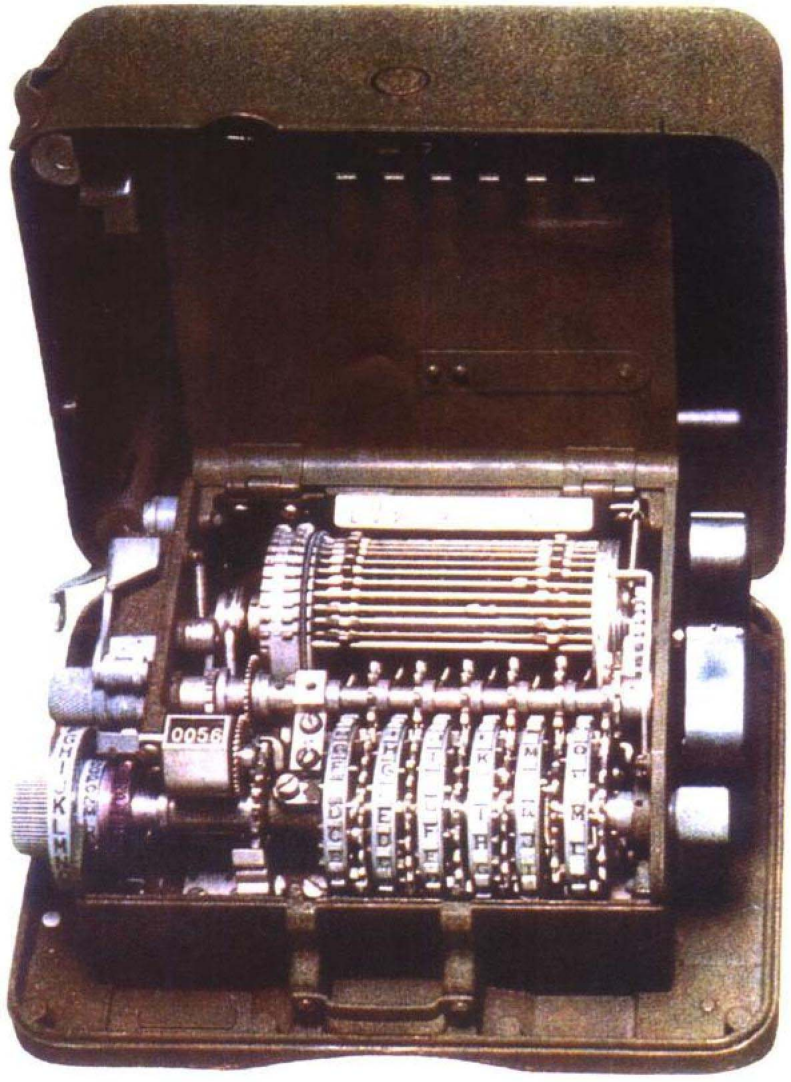
插图F

Kryha密码机大约在1926年由Alexander von Kryha发明。这是一个多表加密设备，密钥长度为442，周期固定。一个有数量不等的齿的轮子引导密文轮不规则地运动。尽管它有弱点，但这台乘法密码机在许多国家很抢手。



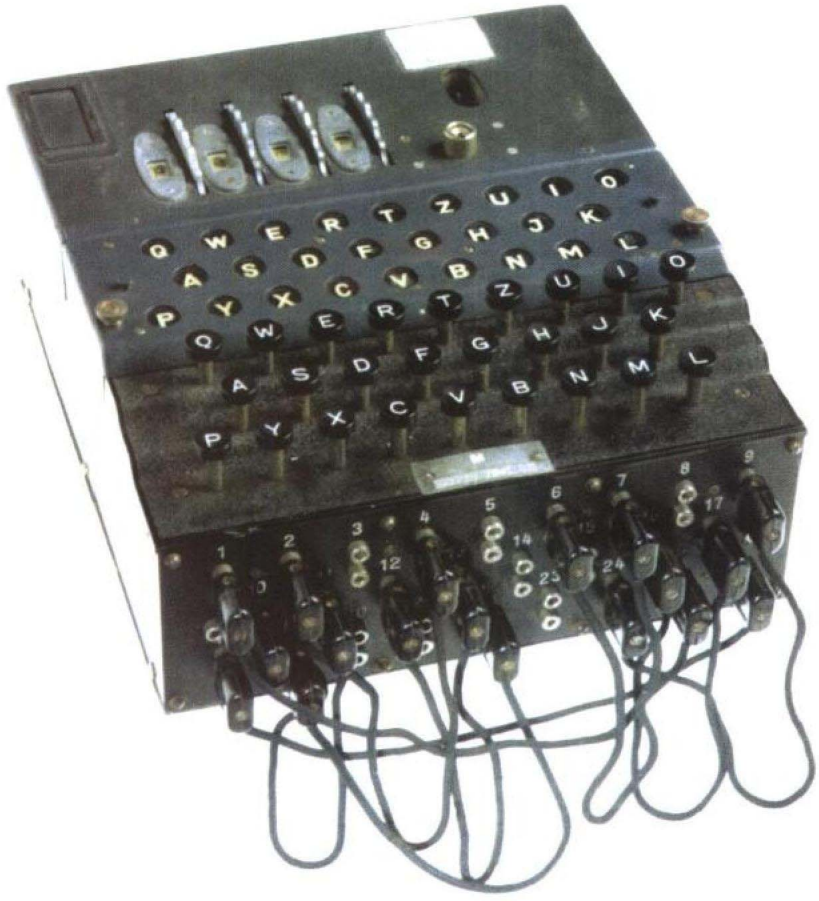
插图G

哈格林（Hagelin）密码机C-36，由Aktiebolaget Cryptoteknid Stockholm于1936年制造，通过BEAUFORT（博福特）加密步完成自反加密，是哈格林的一个发明。密钥的不同长度，即17，19，21，23，25个齿，导致产生不规则运动，密钥周期的长度为3 900 225。对于纯机械的密码机来说，这已是非常不简单了。



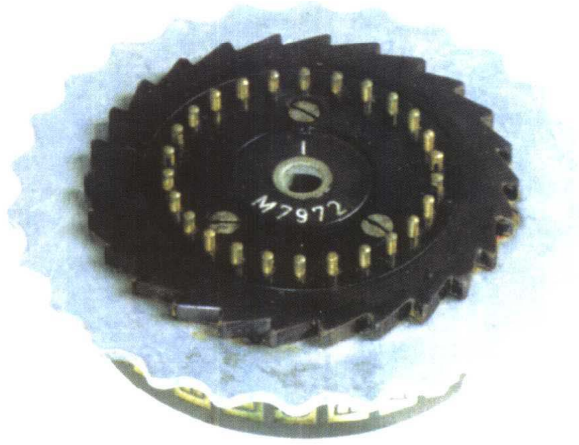
插图H

M-209是哈格林对C-36改进后的产品，根据哈格林的许可，由Smith-Corna负责为美国陆军生产。它增加了一个有26个齿的密钥轮，从而使密钥周期达到了101 405 950。手柄转动时，字母轮带动拨针和凸片，使鼓状筒上的横杆移位；这些横杆的作用象齿轮上的齿那样，使轮子转动，将密文字母打印到把手后面的卷纸上。



插图I

转轮密码机ENIGMA，由Arthur Scherbius（阿图尔·舍尔比乌斯）于1919年发明，面板前有灯泡和插接板；4轮ENIGMA在1944年装备德国海军。它用3（最多为8）个正规轮和1（至多为2）个反射轮（Griechenualzen β，γ），这使得英国从1942年2月到12月都没能解读德国潜艇的信号。



插图J

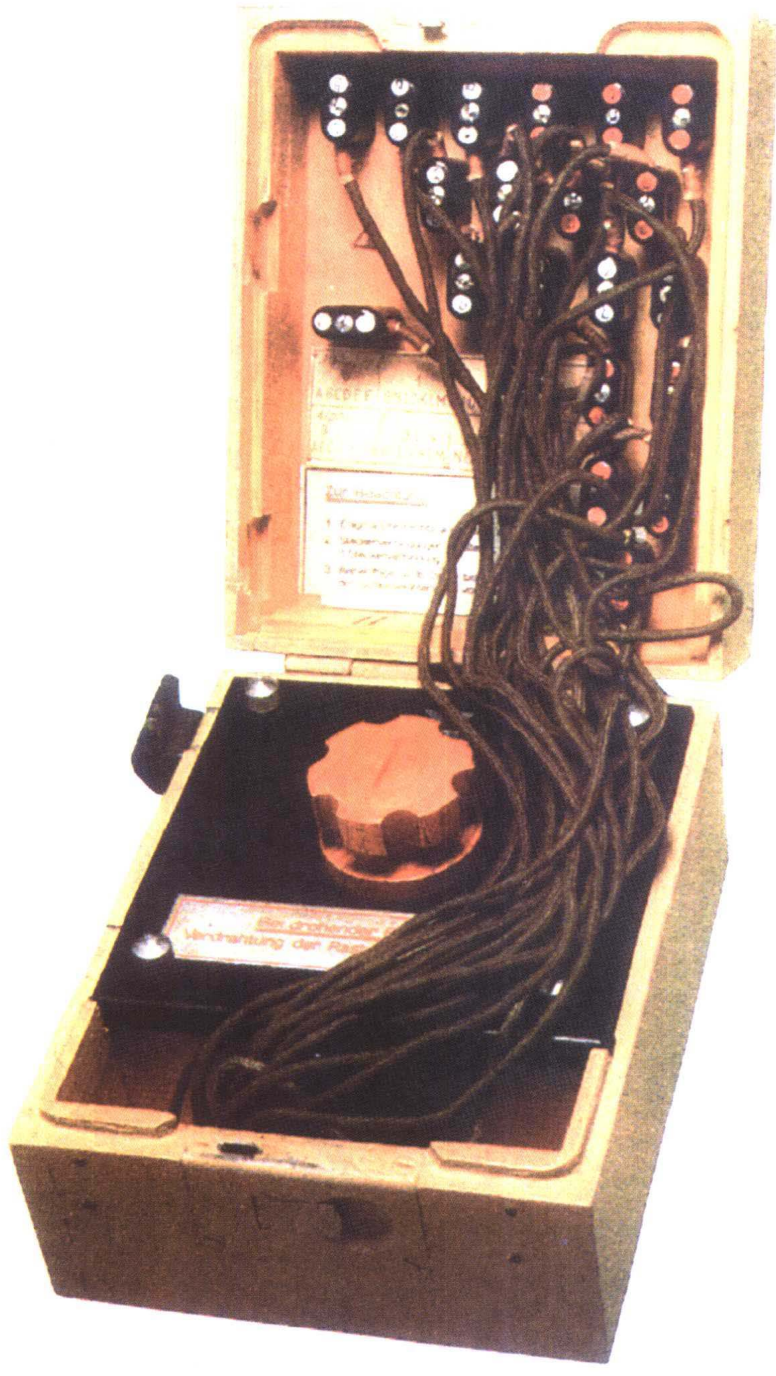
ENIGMA转轮：内部线路有26个电路连接。

上图：I轮，可以看见设置轮。

下图：Ⅷ轮，有2个缺口。

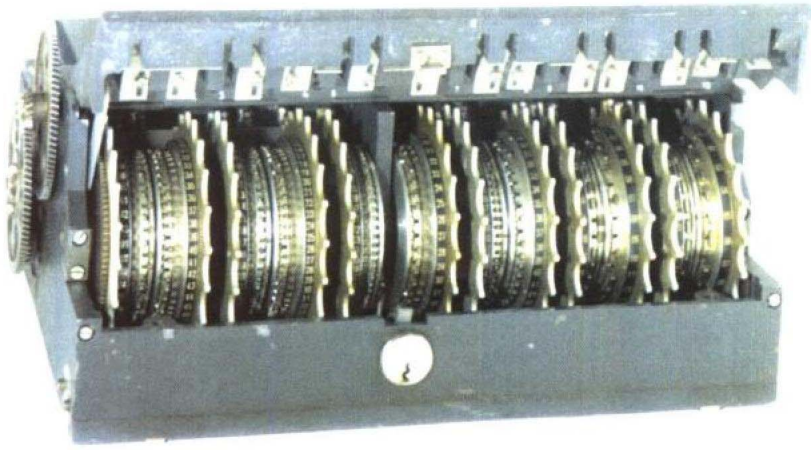
插图K

英国的TYPEX打字密码机，是德国3轮ENIGMA的改进型密码机。它增加了两个轮（操作中不动）使得破译更加困难。它在英国通信中使用广泛，且在破译密钥后帮助破解德国信号。面板上显示TYPEX为Ⅲ型，序列号为NO.376。



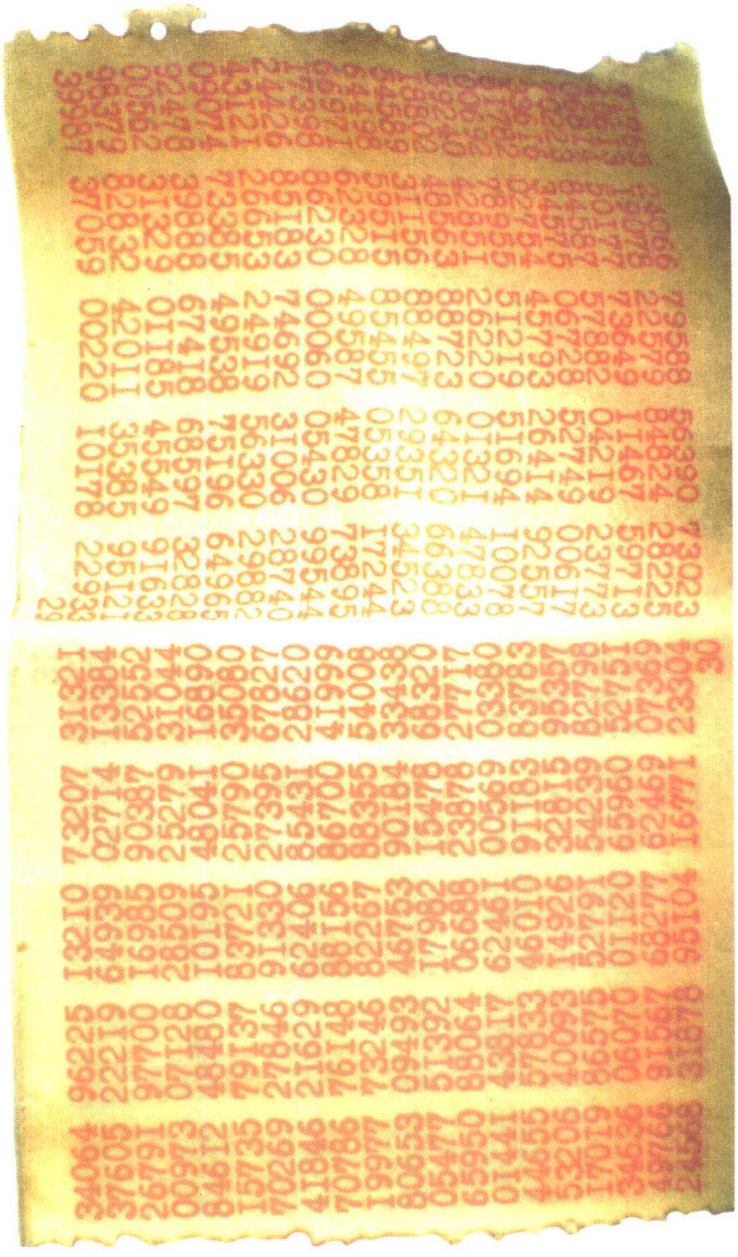
插图L

Uhr盒用来替换德国防军ENIGMA机插接板的机器，用非互反代替，可以选择40个不同位置转动把手，轻易改变代替。尽管其安全性有所增强，但没有广泛应用。



插图M

在线密码电传机Lorentz SZ 42，大约在1943年由Lorenz A.G制造。一种用于Baudot信号的密码机，英国人称为“tunny”，用于战略级陆军司令部。12个密钥轮有不同的齿，（从左到右）是43，47，51，53，59，37，61，41，31，29，26，23，这些密钥轮和不规则间距的销产生较大的密钥周期。五对轮子控制5比特代码的5个VERNAM代替，另两个轮仅用于控制不规则运动。SZ 40/SZ 42加密因为德国人的加密错误而被英国人破译，此后英国人一直使用电子COLOSSUS机器解读德国信号。



插图N

起源于俄罗斯的一次乱数本，差不多只有手掌那么大小。数字的排列具有俄国特色。