

纪念一次破解Enigma密码的经历

Yeenyeong
THUCST

51 人赞同了该文章

Enigma密码简介

Enigma密码机是一种用于加密信息的设备，在第二次世界大战中被德军广泛地在各级军队中使用。据说盟军破解Enigma密码使得二战得以提前两年结束。

下面是一张德国军用Enigma密码机的图片



军用Enigma密码机(图源维基百科)

上图中我们可以看到Enigma密码机的大致组成结构，这个密码机把盖子打开，暴露除了内部的结构。下图是正常使用的Enigma密码机的状态

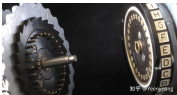


装在木质箱子里的Enigma密码机(图源维基百科)

可以看到，Enigma密码机有3个转子(Rotors)，每个转子都可以手工拨动，转到需要的位置。密码机下方被木板稍稍盖住的是插线板(Plugboard)，在插线板上有26处标有A-Z的插线孔，可以用若干线路将若干个插线孔两两连接起来。转子的转动和插线板的接线，都可以改变密码机内部的线路，从而获得不同的加密线路。从密码学的角度看，这些加密线路属于密钥(读作“mì yuè”，虽然不重要，但是还要说)。

除了转子和插线板，可以影响密码机内部线路的还有反射器(Reflector)和转子的字母环和转子芯的相对位置(Ring setting)。德军用的M3型号的Enigma密码机使用的反射器只有Type-B型一种，是已知的，不需要破解。

至于字母环和转子的相对位置，我们可以从第一张Enigma密码机的图看到带有齿轮的转子，上面标有00-25的数字，对应A-Z 26个字母，也可以直接标上字母，称为字母环，如下图



字母环和转子芯(图源维基百科)

可以看到，在字母环下面的转子内部，称为转子芯，有26个圆形的触点，原本字母环上A对应的触点产生的信号就是A，但后来德国人做了升级，可以转动外部的字母环，和转子芯产生一个偏移。字母环上A对应的触点产生的信号可能是D，这样的话，B对应的触点就产生信号E，Z对应的触点产生信号C，以此类推。因此，即使两个密码机的转子转到同样的数字(或字母)，插线板的连线完全相同，但如果转子的字母环和转子芯的偏移不一样，也不能得到相同的加密线路。

现在我们还未有深入了解Enigma密码机的加密原理，但使用者不需要明白这些。在使用Enigma密码机加密信息之前，使用者只需要将转子拨动到所需位置，将需要连接的插线孔连接起来，就可以在键盘(Keyboard)上输入信息。在键盘上按下下一个字母(明文)，灯板(Lampboard)上就会亮起一个字母，这就是加密后的字母(密文)。

解密的过程和加密的过程完全一致，当使用者拿到一封密文时，只需要将转子和插线板设置成和加密时一致(这些设置是提前约定好的)，再将密文输入，就可以得到对应的明文。这种优雅的对称，得益于一个装置，就是之前提到的反射器，反射器将加密和解密变得一致，想要理解这一点，就要了解一些Enigma密码机的工作原理了。

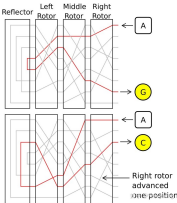
当使用者在键盘上按下下一个字母，比如A，电信号首先到达插线板，下图是插线板



Enigma密码机插线板(图源维基百科)

图中插线板A和J连在一起，因此字母A发出的信号经过插线板后，就变成了字母J的信号(如果没有连线，信号经过插线板保持不变)。信号穿过插线板，就到达了转子。

3个转子，按位置分别称为左、中、右转子。信号穿越插线板，先到达右转子，然后到达中转子，再穿过左转子，到达反射器，再沿着左右转子的顺序回到插线板，然后到达灯板点亮一个字母。



转子反射器线路示意图(图源维基百科)

上面简单地显示转子和反射器的工作线路，以图中的例子来说，字母A的电信号经过右转子，根据转子内部的结构，会被转换为其他字母，比如B的信号，再经过中转子和左转子，被转换了两次，又在反射器内部转换一次，然后穿过3个转子，得到字母G的信号。可以看到，字母A和G之间有一条经过3个转子和反射器的电路，此时如果输入G，那么电信号就从G的一端通过转子和反射器，再回到A，因此加密和解密的过程是一致的。

从图中我们还可以看到，因为反射器的存在，一个字母永远不会被加密为自身，一个字母被加密成自身，好像等于没有加密，因此一个字母保证不会被加密成自身，应该是一个优点，二战时德国人也是这么认为的。但“保证不会”也是一种确定性，这种确定性被盟军利用，成为破解Enigma密码的突破口。

破解的事情我们稍后再说，现在回到Enigma密码机的加密原理。目前为止，我们还没有提到Enigma密码的厉害之处，即使我们上加密线路经过更多的插线板、转子、反射器，所得的密码本质上还是的代换密码，多次代换可以合并成一次代换，比如A->D->J，有两次代换，完全可以合并成一次A->J。也就是说，目前为止，Enigma密码机这些花里胡哨的装置，我们完全可以用一张朴实无华的字母代换表代替。显然，Enigma密码机不可能这么菜。

Enigma密码机的核心，在于转子的自动转动，当使用者加密一个字母后，右边的转子会自动转动一格，每当它转移26格，会带动中间的转子转动一格，当中间的转子转动够26格，又会带动左边的转子转动一格。这意味着，这张字母代换表，每被使用一次，就会做出改变！并且，德国人每天都会更换转子和插线板的设置(德军提前准备了一整年的设置表格)，因此破译时效也只有一天。

下面我们计算一下这张字母表有多少种不同的状态。对于德军M3型号的Enigma密码机，有5个不同型号的备选转子，随机选出3个，随机排列在密码机上的3个位置，这样有 $C_5^3 \cdot 3!$ 种可能。3个转

子, 每个转子有26种可能的状态, 因此3个转子的状态一共有 $26^3=17576$ 种。考虑插线板, 德军会连接10对插线孔, 也就是要选择20处插线孔(≤ 20), 再将这20处插线孔分成10组($10 \times 17 \times \dots \times 3 \times 1$), 相乘结果得 $10! \times 17! \times 17! \times 20!$ 种可能。再乘上转子的可能, 一共有 $10! \times 17! \times 17! \times 20! \times 17576$ 种, 达到了 10^{16} 的数量级, 就这还没有算上字母串的偏移, 也没有考虑10根线可能没有完全插上插线板的情况。即使按照现在的大个计算机每秒运算 10^7 次来估算, 也需要至少 10^{10} 量级的秒数, 才能暴力破解Enigma。一天有 86400 秒, 因此至少需要 10^3 天! 现代的计算机尚且如此, 更不要说第二次世界大战的时候, 所以德国人认为他们的密码是绝对安全的。

波兰人的破解过程

早在1932年, 德国人的Enigma机还只有3个转子, 并不是5个转子的時候, 波兰当局就利用德军发报的习惯破解了Enigma, 德军当日的信息, 主要有两层密码进行加密, 分别是日密码和信息密码。日密码就是提前约定好的的密钥, 德国人为了避免同一天的大量电报用同一个密码加密(大量使用同一个密码不利于保密), 决定为每一封电报随机选取一个信息密码(3个字母, 对应转子的设置, 其余设置和日密码相同), 并用日密码加密这个信息密码, 重复两次避免漏机的输入错误), 置于电报开头, 因此每封电报的前6个字母就是信息密码的密文, 之后就是用信息密码加密的电报密文。但重复是密码的大忌! 德军将信息密码重复两次的操作被波兰数学家与密码学家富耶夫斯基利用, 通过一天大量电报的前6个字母, 破译了Enigma密码!

富耶夫斯基的破解方法如下:

每一封电报的信息密码, 设为 $a_1a_2 \dots a_3$ (由A-Z任意组成的3个字母)。假设截获了一封电报, 前6个字母为 $a_1a_2a_3a_4a_5a_6$, 这6个字母就是--被连续加密两次的密文。我们知道, Enigma密码机每加密一个字母就会改变一个状态, 我们把初始状态称为 s_0 , 下一个状态称为 s_1 , 以此类推, 则我们可以知道, a_1 通过 s_0 被加密成了 B , a_2 通过 s_1 被加密成了 B , 记为 $B=s_0(a_1), B=s_0(a_2)$ 。这一步之前的线索是显然的, 再往下走, 我们要记得, Enigma密码加密和解密过程是一致的, 所以 $B=s_0(a_1)$, 必然有 $a_1=s_0(B)$, 可惜 s_0 未知(不然破译盲盒, 直接解密就好了), 不过事情并没有很糟糕, 用 $s_1(B)$ 代换 s_0 , 可以得到 $B=s_1(s_0(B))$, 简单记为 $B=s_2(a_1)$ 。这是一封电报的前6个字母, 得到了第1个字母和第4个字母之间的关系, 一天有大量电报, 每一封电报都记录第1个字母和第4个字母, 可以得到一张表, 例如

161 | 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
48 | P Q R S T U V W X Y Z 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

通过观察上面的表格, 我们可以发现: 当 a 作为第1个字母时, 第4个字母是 r ; 当 e 作为第1个字母时, 第4个字母是 w ; 当 w 作为第1个字母时, 第4个字母又变成了 a ! 这是一个循环, 记为 $a \rightarrow P \rightarrow W \rightarrow A$, 可形象地称之为环。类似地, 这张表里还有这些环:

$B \rightarrow Q \rightarrow R \rightarrow K \rightarrow V \rightarrow E \rightarrow L \rightarrow B$
 $C \rightarrow M \rightarrow D \rightarrow A \rightarrow B \rightarrow C$
 $J \rightarrow M \rightarrow X \rightarrow H \rightarrow T \rightarrow N \rightarrow J$

现在假设没有插线板, 我们猜测 s_0 对应的转子状态(是 s_0 的转子转动3倍), 然后验证这个猜测能不能得出这些环, 如果可以, 则猜测正确。如果不行则猜测错误。波兰当局花了一年的时间, 遍历了所有转子的状态, 每一种状态都得出了一系列的环, 并据此制作了一份检索表, 可以通过环的特征(比如所含字母顺序、长度)来找到可能的转子设置。这样一来, 每天截获电报, 取得第1个和第4个字母, 得到类似上面的表格, 进而得到环的信息, 然后就可以通过检索表查询可能的转子设置, 当然这些可能性的数量已经是可以接受的了, 因此能直接暴力破解(波兰的破解设备叫“炸弹”, Bomba)。

注意到上面假设了没有插线板, 但是仍然不影响这个破解方法的效果, 这是为什么呢? 富耶夫斯基发现, 插线板设置虽然会改变某几个环上的某几个字母, 但是每个环的长度和环的总数不变! 这其实也很好理解, 我们知道, 之所以会出现这些字母串, 是因为每加密一次转子就会转动(之前提到过, 如果转子不转动, Enigma机等价于一张字母代换表, 是不会出现环的), 转子状态的周期变化才是这些环出现的原因, 插线板的设置是不会周期变化的, 同时, 在Enigma机里, 信号首先经过插线板进入转子, 最后也是从转子出来后, 才经过插线板输出, 因此插线板的设置仅能影响进入转子的信号和转子输出的信号, 而不能影响转子的周期变化, 因此就体现为字母串的部分字母改变, 但每个环的长度和环的总数不变。当然, 这只是理解, 而严格证明就不在此展开了。

到此, 我们知道了即使加上插线板, 字母环的主要特征也能最大限度保留, 因此检索表还是很有效的。至此我们可以通过检索表得到正确的转子设置, 那么如何恢复插线板的设置呢? 其实办法很简单, 先不插任何导线, 然后将截获的密文输入Enigma机, 虽然会得到辨识度极低的乱码, 但仍然会有模糊可辨的单词或短语, 比如alliveinberlin, 就可以合理推测这是arriveinberlin, 然后 a 和 s_0 之间有导线, 而 A,I,V,E,R,N 不插导线。这样的例子足够多之后, 就可以恢复插线板的设置。

通过检索表, 波兰人在1933年就可以对德国的电报进行破译!

阿兰·图灵的破解过程

上面讲了波兰人的努力获得了成效, 不过一劳永逸是不现实的, 德国人虽然爱搞强操作, 但显然也不是傻子, 二战爆发前后, 他们用一套组合拳, 把波兰人一锅打回解放前:

- 转子数量从3个增加到5个, 转子的排列可能性就增加了10倍, 更重要的是, 多出来的转子让波兰人的检索表失效了
- 插线板的最多导线数目从6根变成10根(可能性增加了一万多倍)
- 信息密码只发送1次

Enigma密码的安全性得到加强, 原本Bomba只需要运转6台Enigma机, 但破解加强版的Enigma需要同时运转60台! 波兰的算力达到了极限, 因此在被德国占领之前, 波兰将被破译技术交给了英法, 年轻的阿兰·图灵加入了破译Enigma密码的工作。

之前被波兰利用的弱点, 德国人都改进了, 但是Enigma机还有一个致命的弱点, 那就是一个字母加密后不可能是它本身! 德国人认为这是一个优点, 必经一个字母加密成自身等于没有加密。但是这个特点, 被盟军狠狠利用了。

德国人发报都会有固定的格式, 比如在开头的某个位置会有“天气预报”(德语 wetterbericht)的字样。我们可以用这一段已知的明文来做出攻击, 密码学上称为“已知明文攻击”。再次强调, 在Enigma密码里, 一个字母不会被加密为自身, 如果能确定明文出现的大概位置, 完全可以用明文在电文的某个区间逐个比较明文和密文的字母, 找到一个位置, 满足“明文的所有字母不被加密为自身”, 如果明文足够长, 这样的位置是容易确定的, 因此可以认为找到了这段明文对应的密文。

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

比对明文(下和密文上), 图源清华大学现代密码学课程

如图, 这个明文的位置就不可以往左偏一格, 因为这样第3个t就和密文中的t匹配了, 而t不能被加密成t。

当得到一对足够长的明文和密文时, 就能得到一张表

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

明文和密文, 图源清华大学现代密码学课程

这样的表是不是有点眼熟? 没错, 其实这和波兰人得到的第1个和第4个字母的对应表有异曲同工之妙, 我们同样可以在上面找环, 更妙的是由于Enigma机加密和解密的对称性, 环的方向不仅可以从明文字母指向密文字母, 也可以反过来, 从密文字母指向明文字母! 相比之下, 波兰人的环只能从第1个字母指向第4个字母, 只有一个方向。

例如, 这张图里的环可以是 $E=s_0(a_0), E=s_1(a_0)$, 也可以是 $E=s_0(a_1), s_0(a_1)=E$, 这里上标-1表示从密文到明文的意思, 但注意到加密解密的对称性, 实际上 $s_1^{-1}=s_0$, 因此第2个环也可以写作 $E=s_0(a_0), s_0(a_0)=E$, 我们还可以找到更多的环, 当找到足够多的环后, 我们就可以枚举转子状态, 然后用这些环来验证。验证方法如下:

首先选一个转子的初始状态 s_0 , 之所以不是 s_1 , 是因为上述的明文出现的位置不一定在电报的开头, 但我们仍然可以令 $s_0=s_1$, 而这样做的代价就是, 对于某个环, 比如 $a \rightarrow s_0(a_0), a_0$ (上面是 $a=s_0(a_0)=a$), 既然环不一定满足这个环了, 我们需要枚举26个字母, 如果有一个字母可以满足这个环, 那么此时的转子设置就有可能是正确的, 然后再用第2个环验证, 如果在用某个环验证时, 发现26个字母都不能满足这个环, 就说明此时的转子设置是错误的, 然后验证下一个转子设置。一般来说, 只有一个转子设置能经过30个环的筛选, 这个设置就是正确的。

恢复转子设置后, 插线板的设置就可以用之前提到的模糊文本辨认的方法恢复了。

发布于 2021-04-09 00:38

密码学


图灵 (Alan Turing)

写下你的评论...

5 条评论

默认

最新



树无藤
精品无人系列



Lin On Work
好文章啊。我准备给校队的学弟出一道，破解enigma密文（没有描线板）
2022-07-27



一生只爱朱茵
🤔

密码milyao
2022-03-03



Yeenyong



作者
我也怀疑过，但听老师念过，去查了，还真念yue
2022-04-10



树无藤
Yeenyong
好像两种读音都有的，但在密码学里念yao
2022-05-16

文章被以下专栏收录

计算机学习笔记
记录学习计算机有趣的、有价值的经历

推荐阅读

把密码存在 GitHub 里面，你家里是有矿嘛？
虽然每个人都知道不要将密码、密钥等信息放到仓库代码里面，但是密码泄露的事情其实一直在发生，而直接是吃不起亏，曾经年少无知的我就犯过这样的错误，以前调用 GitHub 的相关接口用到 To...
非著名程序... 发表于GitHub...

输入密码
PyQt5系列教程（12）：构建我们自己的密码输入框
我想飞

CHANGE USER
PASSWORD
新手教程：Ubuntu 下如何修改用户密码
Linux... 发表于Linux...

密码安全
NIST出台密码安全新标准：不再强制用户定期修改密码...
密码Roa... 发表于密码Roa...



登录即可查看 超5亿 专业优质内容
超 5 千万创作者的优质提问、专业回答、深度文章和精彩视频尽在知乎。
立即登录/注册

赞同 51 5 条评论 分享 喜欢 收藏 申请转载 ...