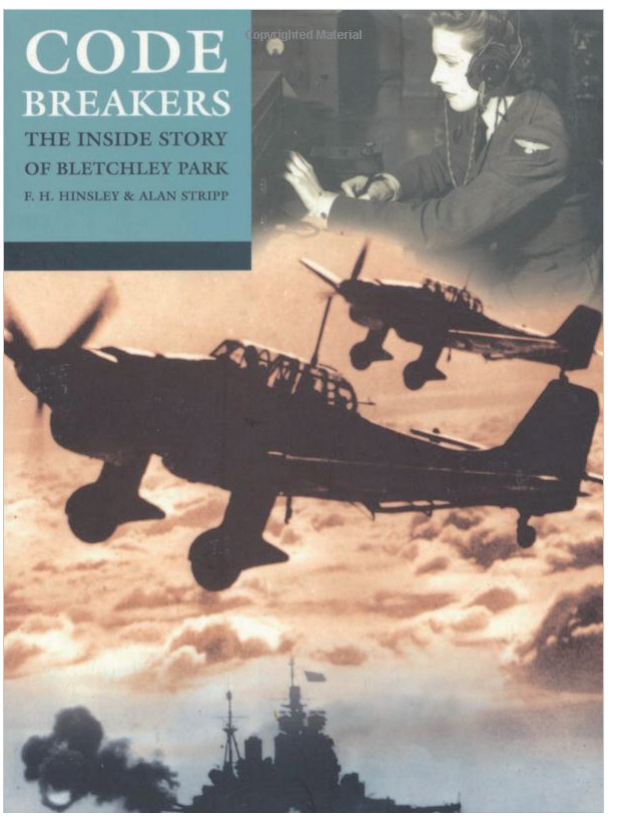
FISH 密码和我[1]

William Thomas Tutte / 文　　李明明　韩广国　许丽卿 / 译

1 引言



Codebreakers（Francis Harry Hinsley & Alan Stripp，牛津大学出版社，2001）

今天，很荣幸地被邀请来这里做演讲，讲述四十年代在布莱切利庄园我曾从事的密码工作。我主要参与研究德军机器密码，即在布莱切利庄园众所周知的“ FISH”密码。这个系统的网络衍生出了很多变种，并且每个变种都以一种鱼来命名。我记得第一个被截获的链接叫做“金枪鱼”，紧接着有“鳊鱼”，“鲱鱼”和“马鲛鱼”。

这次演讲所涉及的读物是由 F. H. Hinsley 和 Alan Stripp 编著的 *Codebreakers*，它的副标题是“布莱切利庄园内的故事”，本书的第三部分讲述了“FISH”密码的故事。据说，第一个 FISH 密码通信是在 1941 年中期，当德军用无线电台在雅典和维也纳之间传递信息时被截获的。这台截获设备可以提供德军消息的精确副本（很少字母被篡改，且每个字母无论篡改与否，都在正确的位置），它的设计者和操作员曾因此受到了高度赞扬。

[1] David Joyner（Editor）, Coding Theory and Cryptography: From Enigma and Geheimschreiber to Quantum Theory, Springer, 1999.11, Pages9-17.

我们的通信采用的是国际电传打字机代码。它的两个基本符号，在布莱切利庄园里称作“•”和“×”,等同于现代二进制编码里的“0”和“1”。如果有电子开关的概念，那么也称之为“开”和“关”。每个字符都是五个基本符号串，因此，总共有 32 个字符。表 1 列出了这一国际代码。

在表 1 中，一个字符的五个基本符被写成一行，不过在布莱切利庄园更习惯把它们写成一列。因此，在电传打字机代码里，一条信息的开头可能如表 2 中出现的那样，其中,“9”代表空格。当一条信息或其它字符序列写成这样时,我们称这五行为五个“脉冲”，而这五个“脉冲”为“•”和“×”组成的五个数据流。

记得我是 1941 年 5 月开始在布莱切利庄园工作，几个月后，我去破译金枪鱼密码。

• • • • •	空白
• • • • X	T
• • • X •	回车
• • • X X	O
• • X • •	空格
• • X • X	H
• • X X •	N
• • X X X	M
• X • • •	换行
• X • • X	L
• X • X •	R
• X • X X	G
• X X • •	I
• X X • X	P
• X X X•	C
• X X X X	V
X • • • •	E
X • • • X	Z
X • • X •	D
X • • X X	B
X • X • •	S
X • X • X	Y
X • X X •	F
X • X X X	X
X X • • •	A
X X • • X	W
X X • X •	J
X X • X X	数字移位
X X X • •	U
X X X •X	Q
X X X X•	K
X X X XX	字母移位

表 1. 电传打字机代码

9	S	P	R	U	C	H	N	U	M	M	E	R	9
•	X	•	•	X	•	•	•	X	•	•	X	•	•
•	•	X	X	X	X	•	•	X	•	•	•	X	•
X	X	X	•	X	X	X	X	X	X	X	•	•	X
•	•	•	X	•	X	•	X	•	X	X	•	X	•
•	•	X	•	•	•	•	•	•	X	X	•	•	•

表 2.

2 关于加法密码

在加法密码中，我们将明文消息 (C) 逐字加上密钥流序列 (K) 转换为密文消息 (Z)。有一种加密方法是按照字母表顺序，将字母依次赋值为 1~26，然后对这些数字做模 26 加法。因此，有（见表 3）

$$J + S = 10 + 19 = 29 \equiv 3 = C.$$

在电传打字机代码中，一个简便的方法是将字母的加法写成 5 维向量模 2 加法。因此

$$J + S = \begin{matrix} X & X & \bullet \\ X & \bullet & X \\ \bullet & + & X \\ X & \bullet & X \\ \bullet & \bullet & \bullet \end{matrix} = \begin{matrix} X \\ X \\ = X \\ X \\ \bullet \end{matrix} = C$$

我们假设密钥是由密码机产生的字符串，因此我们可以将加密过程用代数式表示

$$C + K = Z.$$

A 1	N 14
B 2	O 15
C 3	P 16
D 4	Q 17
E 5	R 18
F 6	S 19
G 7	T 20
H 8	U 21
I 9	V 22
J 10	W 23
K 11	X 24
L 12	Y 25
M13	Z 26

表 3

加法密码有个众所周知的缺陷，假设不小心将两条不同的信息用同一密钥进行加密，即

$$C_1 + K = Z_1,$$
$$C_2 + K = Z_2.$$

因此，有

$$C_1 - C_2 = Z_1 - Z_2.$$

我们称这一对为“一个深度对”。如果敌方密码专家怀疑这一深度对，他会用已知的 Z_1 减去 Z_2，由此得到 。再加上足够的运气，便能分离出明文 C_1 和 C_2，这样就破译出了两条明文。此外，用 Z_1 减去 C_1 便可以找到密钥 K。这个过程是在 C_1 连续的位置，先尝试一个可能的单词，比如说 LONDON，计算 C_2 中相应的六个字母，直到找到一个位置使得这六个字母对应可能的明文。或许明文是 IMPENE, 然后猜测接下来的明文，得到“IMPENETRABILITY”，如下所示：

C_1 L O N D O N T H O U A R T T H (E)
I M P E N E T R A B I L I T Y T

紧接着他就宣布 C_1 的开头为“London thou art the flour of cities all”，而 C_2 的开头为“Impenetrability, thats what I say”。

3 HQIBPEXEZMUG

在“金枪鱼”变种中，德国人习惯将每条信息的电报报头写为 12 个字母的序列。在布莱切利庄园，人们把这个序列叫作“指示符”，并猜测它给定了密码机中 12 个转轮的设置。有时候两条密文信息会用相同的指示符。密码专家可能会说“同样的设置，因此会用同样的密钥，用一个深度对试试”。使用上文中我提到的模 2 加法运算，将金枪鱼密码等同于加法密码，获得了巨大的成功。

有一天截获了两条长密文，每条大约 4000 字，并且具有相同的指示符“HQIBPEXEZMUG”。利用这一深度对成功地将其破译出来。这被证明是同一信息的两次尝试，一条信息间距较多，而另一条标点较多。很明显，这对深度破译具有极大的帮助。Col. J. Tiltman 破译了这个深度并且推断出了大约 4000 字的密钥。接下来的问题：假定机器产生这一密钥，决定该机器的结构。用当时当地的语言来说，密码专家致力于“破译金枪鱼密码的密钥”。

所有这些在我接触“金枪鱼”密码之前都已经完成了。

大约三个月后，密钥方面依然没有突破。研究部门的 G. W. Morgan 少校给了我一份密钥复本，对我说“对此密码，看看你能做些什么”。

进入布莱切利庄园之前，在伦敦的密码学校学习时，我已经得知，以周期的形式写出密文并寻找重复规律，有时可得到预期结果。我决定用密钥的一个或多个脉冲来试验。但周期是多少呢？我已经从指示符的字母中获取了一些信息，前 11 个字母似乎有 25 种可能性，但最后 1 个字母仅有 23 种可能。也许我该尝试以 23 或 25 为周期。或者为何不直接写出一个周期为 23*25 ＝ 575 的脉冲来试试呢？确切地说，我对这个过程没有太大的信心，不过我总觉得看起来杂乱无章是最好的。因此我写出了第一个 7 行的脉冲，每行的长度为 575 个字符，并且来寻找“点”和“叉”的简短模式的重复，逐行寻找竖直重复。

如我所料，并没有多少显著的重复。但是我发现在对角线上有很多重复。看来我以 574 为周期能得到更好的结果。因此我以此为周期又写了一次这一脉冲，惊喜地发现很多长度为 5 或 6 的“点 - 叉”模式的重复。

然后我尝试了以 41 为周期，由于它是 574 的一个素因子，也因此得到了更好的结果。结果显示密钥的第一个脉冲是两个“点 - 叉”组成的序列的和，我称这两个序列分别为 χ_1 和 Ψ_1。χ_1 是以 41 为周期的周期序列，Ψ_1 基本上也是周期的，周期为 43。但是当 χ_1 每个字母移一位时，Ψ_1 有时候移动一位，有时候不移位。

在这一阶段，整个研究室的人都参与进来，将其余的每个脉冲分解为 χ- 转轮和 Ψ- 转轮形式。在 *Codebreakers* 中有记载，χ- 转轮从第一个到第五个脉冲，周期依次为 41，31，29，26，23。而 Ψ- 转轮的周期分别为 43，47，51，53 和 59。一个重大发现就是所有的 χ- 转轮都是同步运行的，它们或者都移动一位或者都静止不移位。当第 11 个转轮出现一个“叉”（周期为 37）时，它们移动位置。当第 12 个转轮（周期为 61）出现一个“叉”时，第 11 个转轮移动一位，并且对于每一个字母，第 12 个转轮都会移动一位。这样，第 11、12 个转轮合称为“驱动转轮”。

在 *Codebreakers* 中，将所有的这些工作说成都是我自己完成的，这样说有些夸张。