FISH and I

W. T. Tutte*
University of Waterloo

1 Introduction

I have been asked to speak today about some cryptographic work I was engaged in at Bletchley Park, during the Forties. I was concerned mainly with a German machine-cipher known in Bletchley as "FISH". The network using this system grew to have many links and each link was given the name of a kind of fish. Thus the first link to be intercepted was called "Tunny" and I recall such names as "Bream", "Herring" and "Mackerel" for later links.

The text-book for this lecture is "Code Breakers", edited by F.H. Hinsley and Alan Stripp. It is subtitled "The Inside Story of Bletchley Park," (Oxford University Press, 1993). Part 3 of this book tells the story of "FISH". It tells that the first FISH traffic to be intercepted was on a German Army radio link between Athens and Vienna from the middle of 1941. Much praise is due to the designers and operators of the intercepting equipment for producing accurate copies of the German messages, with few garbled letters and every letter, garbled or not, in its proper place.

The letters used were those of the International Teleprinter Code. There were two basic symbols, called at Bletchley "Dot" and "Cross". They would equally well have been called "Zero" and "One". Or, with electrical switches in mind, "On" and "Off". Each letter was a sequence of 5 basic symbols, so there were 32 letters in all. Table 1 sets out this International Code.

In Table 1 the five symbols of a letter are written in a row. It was more usual at Bletchley to write them in a column. Thus the beginning of a message in teleprinter code might appear as in Table 2. Here "9" stands for "Word Space". When a message or other sequence of letters

*Professor Tutte, FRS, is a Distinguished Professor Emeritus and an Adjunct Professor in the C&O department at the University of Waterloo. He worked from 1941 to 1945 in the British cryptanalytic headquarters at Bletchley Park, the most successful intelligence agency in world history. His work, which combined elements of statistics and combinatorics, was instrumental in the breaking of FISH, a series of codes that were used by the German command for encrypting communications between the highest authorities. Subsequent cryptanalytic work on FISH included the development of Colossus, the world's first electronic computer. This paper is a transcript of Professor Tutte's lecture on June 19 1998 at the opening ceremony of the Centre for Applied Cryptographic Research (CACR) at the University of Waterloo.

•	•	•	•	•	All space (7)
•	•	•	•	X	T
•	•	•	X	•	Carriage Return (4)
•	•	•	X	X	O
•	•	X	•	•	Word Space (6)
•	•	X	•	X	H
•	•	X	X	•	N
•	•	X	X	X	M
•	X	•	•	•	Line feed (5)
•	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	Figures (3)
X	X	X	•	•	U
X	X	X	•	X	Q
X	X	X	X	•	K
X	X	X	X	X	Letters (2)

Table 1: Teleprinter Code

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	X	•	•	•

Table 2:

was written like this we referred to the five rows as the five "impulses", five streams of dots and crosses.

I started work at Bletchley Park in (I think) May 1941. It was several months later that I encountered Tunny.

2 On additive ciphers

In an additive cipher we convert the clear message ($\mathcal{C}$) into the cipher message ($\mathcal{Z}$) by adding to it, letter by letter, a sequence of letters called the key ($\mathcal{K}$). The addition has to be defined. One method is to number the letters of the alphabet, in order, from 1 to 26 and then add those numbers mod 26. Thus (see Table 3),

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

In the case of the teleprinter code an obvious method is to add the letters as 5-vectors mod 2. Thus

$$J + S = \begin{array}{c} \mathrm{X} \\ \mathrm{X} \\ \bullet \\ \mathrm{X} \\ \bullet \end{array} + \begin{array}{c} \mathrm{X} \\ \bullet \\ \mathrm{X} \\ \bullet \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \mathrm{X} \\ \mathrm{X} \\ \mathrm{X} \\ \bullet \end{array} = C$$

The key we may suppose is a string of letters produced by the cipher machine. We can write the process of encipherment as an algebraic equation

$$\mathcal{C} + \mathcal{K} = \mathcal{Z}.$$

Additive ciphers have a well-known weakness. Suppose two messages are carelessly sent on the same key. Then

$$\begin{aligned} \mathcal{C}_1 + \mathcal{K} &= \mathcal{Z}_1 \\ \mathcal{C}_2 + \mathcal{K} &= \mathcal{Z}_2. \end{aligned}$$

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
M	13	Z	26

Table 3:

Therefore

$$\mathcal{C}_1 - \mathcal{C}_2 = \mathcal{Z}_1 - \mathcal{Z}_2.$$

We called such a pair a "depth of two". If the enemy cryptanalyst has reason to suspect such a depth he subtracts $\mathcal{Z}_2$ from $\mathcal{Z}_1$ and knows that he probably has $\mathcal{C}_1 - \mathcal{C}_2$. This, with reasonable luck, he can separate into the two clear messages $\mathcal{C}_1$ and $\mathcal{C}_2$. He reads them both. Moreover by subtracting $\mathcal{C}_1$ from $\mathcal{Z}_1$ he can find $\mathcal{K}$. The procedure is to try a likely word, perhaps like LONDON, in successive positions in $\mathcal{C}_1$ calculating the corresponding six letters of $\mathcal{C}_2$ until one finds a position in which those six letters are plausible as plain text. Perhaps they are then IMPENE. Guessing that this continues as "IMPENETRABILITY" he writes as follows

$\mathcal{C}_1$	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

Soon he is announcing $\mathcal{C}_1$ as beginning "London thou art the flour[1] of cities all" and $\mathcal{C}_2$ "Impenetrability, thats what I say".

3 HQIBPEXEZMUG

It was the German custom on the TUNNY link to give in the preamble of each message a sequence of 12 letters. At Bletchley people called this sequence the "indicator" and guessed that it gave the settings for 12 wheels in a cipher machine. Occasionally two cipher messages would come with the same indicator. The cryptanalyst would say "Same settings, therefore same key.

[1] old spelling

Try it as a depth of two". There was enough success to identify Tunny as an additive cipher using the mod 2 addition I have already mentioned.

One day there came two long cipher messages, each about 4000 letters long, with the same indicator HQIBPEXEZMUG. This depth of two was successfully read. It proved to be two attempts at the same message, one having more word-spacing and other punctuation than the other. This obviously was a great help in the depth-reading. Col. J. Tiltman read this depth and deduced some 4000 letters of key. Next problem: given that the machine produced this key, determine the structure of the machine. In the language of the time and place cryptanalysts sought to "break the Tunny key".

All this was done before I had any dealings with "Tunny".

Some three months later, the key still unbroken, Major G.W. Morgan, head of the Research Section, gave a copy of the key to me and said "See what you can do with this".

Now at my pre-Bletchley cryptographic school in London I had learned that you can sometimes get results by writing out a cipher text on a period and looking for repeats. I resolved to do this with one or more impulses of the key. But on what period? I had been given some information about the letters of the indicator. There seemed to be 25 possibilities for 11 of these but only 23 for the last. Perhaps I should try periods of 23 or 25. Or why not try both at once by writing the impulse on a period of $23 \times 25 = 575$? I can't say that I had much faith in this procedure but I thought it best to seem busy. So I wrote out the first impulse in 7 rows of length 575 and looked for repeats of short patterns of dots and crosses, vertical repeats from row to row.[2]

As expected there were not significantly many. But then I noticed a lot of repeats on a diagonal. It seemed that I would have got better results on a period of 574. So I wrote out the impulse again on that period and found pleasingly many repeats of dot-cross patterns of length 5 or 6.

Then I tried a period of 41, this being a prime factor of 574, with even better results. The upshot was that the first impulse of the key was a sum of two sequences that I named χ_1 and Ψ_1, of dots and crosses. χ_1 was periodic with period 41. Ψ_1 was basically periodic too, with period 43. But whereas χ_1 moved on one place for each letter, Ψ_1 sometimes moved on one place and sometimes stayed still.

At this stage the whole Research Section joined in to analyse each other impulse into a χ-wheel and a Ψ-wheel. In "Code Breakers" it is recorded that the χ-wheels, in order from the first impulse to the 5th, had periods 41, 31, 29, 26 and 23, while the Ψ-wheels had periods 43, 47, 51, 53 and 59. A major discovery was that the χ-wheels moved in step. Either all moved on one place or all stayed still. They moved whenever an 11th wheel showed a cross. (Period 37.) This 11th wheel moved on one place when a 12th wheel, of period 61, showed a cross, and the 12th wheel moved on one place for each letter. The 11th and 12th wheels were called the "motor wheels".

[2] I hope noone is going to ask why I didn't use a computer.

In "Code Breakers" I am said to have worked out the whole of this by myself, but that is an exaggeration. Note that the fifth χ-wheel had period 23 and the clue from the indicator letter of 23 possibilities was a valid one.

Presumably if I had not noticed the diagonal repeats I would have tried the method again on the 2nd, 3rd, 4th, and 5th impulses. And on the fifth it would have worked, the fifth χ-wheel having period 23. I suppose I would have been said to have broken the key by pure analytic reasoning. As it was I was thought to have a stroke of undeserved good luck. There must be a moral in this.

A cryptographer might criticize the German χ-patterns which contained too many sequences of 3 or more dots or 3 or more crosses. In the resulting χ-key most of these sequences were stretched out to greater lengths. Hence in a key impulse sequences of five basic symbols were significantly often the corresponding part of the χ-wheel, or the reverse thereof. The critic must point out two grave errors, first the poor Ψ-patterns and second the sending of a long depth of two. Either error without the other the Germans would I think have got away with. But the two together gave away the structure of the machine.

With our knowledge of the machine we could work on some keys from shorter depths. We discovered that in the past there had been a change of wheel-patterns once a month.

It was early in 1942 that we got an opportunity to attack current traffic. Then a vulnerable depth came in. It was read and yielded about 1000 letters of key. I have a vague memory of a depth of 3 at this time, and this may have been it.

4 Attacks on current traffic

The 1000 letters of new key proved a disappointment. We discovered later that the Germans had corrected their Ψ-error. So the method that had been so successful with HQIBPEXEZMUG did not work.

Then we received a near-depth, two messages whose indicators agreed in all but one letter, that letter corresponding to a χ-wheel. I advocated an attempt to read this even though the reading would have to be from 4 impulses only. However the difference between the two keys would be periodic; after sufficient initial success the messages could be so corrected as to be read as a true depth. It was a very difficult task requiring skilled linguists. Such people existed at BP and some of them tackled the near depth. They read it and got the key, with extra information about the off-set χ-wheel. That was 30 or so possibilities for its pattern only a few being plausible. With that extra information it was possible to analyse the key.

It was Alan Turing who not long afterwards solved the problem of analysing a length of key obtained from an ordinary depth. He would assume the first two symbols in the χ_1 pattern to be •X, or perhaps ••. The possibilities X• and XX are not genuine other choices since the reversal of all χ and Ψ patterns leaves the key unaltered. Suppose he assumed •X. Then at each repetition of that part of the χ_1 pattern one can deduce Ψ_1 as either •X, X•, XX or ••. If one of the last two he provisionally assumed Ψ_1 had not moved. He then got the corresponding doublet (2 possibilities) in the other χ-wheels and repeated it through the key according to the χ-periods. And so on, making as few corrections as were necessary for consistency. It is a method requiring great artistry. I never used it successfully myself. But there were others with whom it worked well enough.

We were reading only those messages that the German operators were careless enough to send in depth or near-depth. That was too few to satisfy Bletchley's customers. We learned however to use known wheel-patterns to break messages not in depth. Basically a commonly occurring "crib" like SPRUCHNUMMER or OBERKOMMANDO9WEHRMACHT would be "dragged", that is tried in one position after another until a plausible stretch of key was obtained. It was plausible if some positions of the χ-wheels gave plausible Ψ patterns, i.e., not too many occurrences of •X• or X • X. In practice at least one χ-wheel had to have a known setting, that is have the same indicator letter as in some message already read. So the more messages that were read, the easier it became to read others.

It was even found possible to break the wheel-patterns for a month from indicators alone, exploiting stereotyped beginnings and information from indicators as to which wheels in which messages had the same setting. I remember trying this method myself, getting some initial success but soon losing control. Then Capt. J.M. Wyllie tried. In civil life he edited the Oxford Latin Dictionary. "This is just the job for a lexicographer" quoth he. And he broke the wheel-patterns for a past month, hitherto untouched.

The method was used. But since it required so many messages it was unlikely to succeed until late in the month. It might be cut short by the breaking of a depth and then its partial information would help in the reading of other messages.

In the second half of 1942, with all this progress we thought we were doing well. And so we went on through 1943.

It could not last. Eventually the Germans, noticing that the indicators were giving away information that need not be given away, abolished 12-letter indicators. Instead they gave a simple number. Presumably the operator looked up the number in a book and found his twelve letters against it.

We could still recognize depths, messages with the same number and, with luck, get wheel-patterns from them. But how to set those wheel-patterns on other messages?

5 The statistical method

The question now was as follows. Given a cipher message $\mathcal{Z}$, and given the corresponding wheel-patterns, how were we to set those wheels so as to decipher the message?

In the ith impulse we have

$$\mathcal{Z}_i = \chi_i + \Psi_i + \mathcal{C}_i. \tag{1}$$

For some purposes it is desirable to replace $\mathcal{Z}_i$ by $\Delta\mathcal{Z}_i$. The nth symbol of $\Delta\mathcal{Z}_i$ is the sum of the nth and $(n+1)$th symbols of $\mathcal{Z}_i$. We could call $\Delta\mathcal{Z}_i$ a difference. Addition and subtraction are the same in this arithmetic. Similarly for χ_i, Ψ_i and $\mathcal{C}_i$. We note that $\Delta\chi_i$ has the period of χ_i. Also $\Delta\Psi_i$ is zero whenever Ψ stays still.

Let us write (1) with $i=1$ and then with $i=2$ and let us add the two equations

$$(\Delta\mathcal{Z}_1+\Delta\mathcal{Z}_2)=(\Delta\chi_1+\Delta\chi_2)+(\Delta\Psi_1+\Delta\Psi_2)+(\Delta\mathcal{C}_1+\Delta\mathcal{C}_2). \quad (2)$$

I derived this equation because I suspected that $\Delta\Psi_1+\Delta\Psi_2$ would be mostly dot. It is always so when Ψ stays still and sometimes so when χ does not. I calculated that it would be about 70% dot. Note that $(\Delta\chi_1+\Delta\chi_2)$ has period $41\times 31=1271$. $\Delta\mathcal{C}_1+\Delta\mathcal{C}_2$, constructed from a military German message, was expected to be 60% dot or a little more. I concluded that $\Delta\mathcal{Z}_1+\Delta\mathcal{Z}_2$ agreed more often that not with $\Delta\chi_1+\Delta\chi_2$. In favourable cases there might be as much as 55% agreement. It seemed that to set χ_1 and χ_2 we should try $\Delta\chi_1+\Delta\chi_2$ against $\Delta\mathcal{Z}_1+\Delta\mathcal{Z}_2$ in all the 1271 possible relative positions and pick the one with best agreement.

Extensions of the method would set the other χ-wheels.

I remember explaining the method to Gerry Morgan and Max Newman. There were rapid developments. Post Office engineers in consultation with applied mathematicians mechanized the process using first electrical relays and then vacuum tubes. This was the way to Bletchley's pioneering electronic computer "Colossus". In those days telephones and the associated engineering problems were the responsibility of the Post Office.

Soon χ-wheels were being set on current messages and Bletchleyites spoke of the process of "dechiing".

After dechiing there remained the sum $\mathcal{C}+\Psi$. Since $\mathcal{C}$ and Ψ each had its peculiarities this could be broken somewhat in the manner of a depth. Or you could say it was the old process of "dragging", simplified by all the χ wheels having been set. The process was called "depsiing". Or, when unsuccessful "deep sighing". This process was carried out by hand, mostly by members of the W.R.N.S.

It occurred to me that with a sufficiently long message this statistical method might be strengthened so as to find the unknown wheel-patterns. One day, having received a message 15,000 letters long I tried out the idea. It worked. I remember reporting to Major Tester, head of the appropriate Section (known as the Testery) with the news of "the first machine to be broken on a depth of one".

Statisticians at BP, notably Jack Good greatly strengthened the method and the famous Colossus computers were programmed to apply it. Now depsiing became a more tricky process being done with initially unknown psi patterns, which had to be determined in the process. For this work would normally be done in the absence of any helpful depth.

Meanwhile the Germans began to change the wheel-patterns every day and to make the Ψ movement depend partially on the χ-wheels, or even on the past plain text. But production at Bletchley continued up to the end of the European War.

It appears from the work at Bletchley that the main weakness of the Tunny machine was that the five Ψ-wheels kept in step. They either all moved on one place or they all stayed still. Turing's method and the statistical method all depended on this, and so did dragging in the days of indicators. The mere fact that the cipher was additive was also a weakness since depths could be read however subtle the machine. I suppose there was a switch allowing an effortless return to the initial position. With such as switch it would have been hard to avoid sending an occasional depth, especially in times of emergency, strain and overwork.

There was another teleprinter cipher machine that we called "Sturgeon", used by the Luftwaffe. It mixed the five impulses more thoroughly than did Tunny. There was a permutation of the five impulses in the course of key construction.

"Code Breakers" explains why the authorities decided to concentrate on Army Tunny rather than Air Force Sturgeon. One reason: resources were limited and it seemed better to make a full scale attack on one cipher system than to make half-hearted attacks on both. Another reason: Enigma was supplying much information about the German Navy and Air Force but little about the Army.

To which I might add that though we found out how Sturgeon worked we failed to think of a way to apply that knowledge to the reading of messages.