Some thoughts on the Playfair cypher

John Beasley, March 2017

The recent receipt of some books about Bletchley Park has cause me to reread *Have His Carcase* by Dorothy Sayers, and to study the decryption by Wimsey and Harriet of the Playfair-encyphered letter in Chapter 26. It is not claimed that anything which follows is new.

The Playfair cypher requires a keyword of reasonable length, no letter in it being repeated. This is filled in at the start of a 5 x 5 square, and the rest of the alphabet is put in the rest of the square in its normal order, I and J being treated as one. So if the key word is SQUANDER, the square is filled as follows:

```
S Q U A N
D E R B C
F G H I K
L M O P T
V W X Y Z
```

The message to be encyphered is divided into pairs of letters, and each pair is encyphered separately. If the letters are in different rows and columns, they form the corners of a rectangle, and they are replaced by the letters at the other two corners, each letter being replaced by the other corner letter in the same row (so IN becomes KA). If they are in the same row, each is replaced by the letter immediately to its right, wrapping round from right to left if necessary (so AN becomes NS). If they are in the same column, each is replaced by the letter immediately below it, wrapping from bottom to top if necessary. And if they are the same? We can't cope with that, so when pairing off the message to be encyphered "we shove in Q or X or something which won't confuse the reader" (1932 Penguin edition, page 275). So to encypher the traditional message

```
FLY AT ONCE ALL IS DISCOVERED
```

we pair its letters off as

```
FL YA TO NC EA LQ LI SD IS CO VE RE DQ
```

and it will be noted that we have had to insert a dummy Q between the two letters L of ALL and to add another at the end to give us a final pair. We then encypher these pairs, giving a string of letters

```
LV AB LP CK BQ MS PF DF FA RT WD BR ES
```

which can be broken up and punctuated as we wish. The decyphering is done in the same way, except that if the two letters are in the same row we replace each by the letter to its left, and if they are in the same column we replace each by the letter immediately above it.

The beauty of this is that a letter in the plain text is not always represented by the same letter in the encyphered message, and so simple frequency-count methods of decyphering won't work. Nevertheless, the cypher can be cracked, and perhaps surprisingly easily.

The encyphered letter in *Have His Carcase* can be found in full at the start of Chapter 26 (page 273 in the Penguin edition), but for present purposes all we shall need are its first two lines:

```
XNATNX
    RBEXMG
```

Wimsey conjectured that these might represent town and date, the date being in line 2. The hypothesis that this date was written entirely in numerals, using a code such as 1 = A, 2 = B etc, proved to be untenable, and for brevity's sake the calculations were omitted. Next to be tried was June, the murder having taken place on June 18 and the letter having presumably been sent shortly beforehand. Something-June or June-something? Wimsey thought something-June was more likely, so they tried this first. It gave a lead-in, but progress then became desultory until Harriet came up with a brainwave. The letter was supposed to have come from Central Europe, from a six-letter town whose last two letters were its first two letters reversed; what about Warsaw? This proved to be a major advance, and the keyword was gradually teased out and the message read.

When I was rereading this recently, it occurred to me to wonder what would have happened if Harriet had had her brainwave first. It gives WA = XN and RS = AT, and in each case all four letters are different. If two letters, say XY, are in the same row or column and adjacent to each other, XY will encypher to Y-something, and the four letters will not be all different. This hasn't happened, so either WA are in the same row or column but not adjacent to each other, in which case XN will be further letters in the same row or column, or WA are in different rows and columns, in which case XN will be the other corners of the rectangle defined by WA. The latter case is four times as likely as the former (allowing for adjacency by wrap-round, 50 of the 300 possible pairs of positions within a 5 x 5 square are adjacent to each other, 50 are non-adjacent but in the same row or column, and 200 are in different rows and columns), so let us try it first. It gives us, provisionally,

```
 W | X       R | A
---+---     ---+---
 N | A       T | S
```

where we see that WX are in the same row, as are NA, RA, and TS, and that WN are in the same column, as are XA, RT, and AS.

Now if WX are in the same row, either both are in the keyword or both are in their normal alphabetical place. Not many potential keywords contain both X and W, so the latter is much the more likely, and this place can only be in the bottom row. Furthermore, if WX are in their normal alphabetical order in the bottom row, W will be immediately to the left of X, so N will be immediately to the left of A in some higher row. This means that N certainly, and A very probably, will be in the keyword.

Similar arguments can be applied to RS = AT. The inference that ST are in their normal alphabetical place is less secure, since it is quite possible that both are in the keyword, but it is at least worth a try. Since in this case S will be immediately to the left of T, A will be immediately to the left of R.

All this gives us WX somewhere in the bottom row, ST somewhere in the next row up, and NAR together somewhere in the keyword. Ah, but we must have ASX all in the same column; is this possible? Yes, if none of S...X is in the keyword then S will be followed by TUVWX, and X will come neatly under S.

This is as much as WARSAW = XNATNX can tell us. Now let us look at IUNE = EXMG.

There are no repeated letters in IU = EX nor in NE = MG, so let us try, provisionally,

```
 I | E       N | M
---+---     ---+---
 X | U       G | E
```

We have already provisionally placed X in the bottom row, so U must be there also, but it is alphabetically next to T, so it will have to be at the extreme left-hand end of this row with ST at the right-hand end of the row above. This gives UVWX– as the bottom row, so Y or Z must be in the keyword. It also gives NAR in positions 3-5 of their row, since A comes directly above X. Moreover, EU are in the same column, as are ME, so ME must be in column 1 with U, and since MN are in the same row, this row (which is part of the keyword) must be M–NAR.

There is more. IE and GE are in the same row, and if we look at their columns we see that this row must be E–GI–. It is very tempting to make it the third row, with F between E and G, and H somewhere in the keyword. This leaves only O and Y for the missing letter of M–NAR, which is surely a vowel, and O is much the more likely. Can MONAR be the second row of the keyword? If it is, the first row must contain BCDH and Y or Z, which is surely impossible. So it forms the first row, and we can look up possible words in the dictionary; or, like Wimsey, we can spot MONARCH at once, swiftly correcting it to MONARCHY to accommodate Y.

As Wimsey says, all done by kindness.

The speedy finding of this keyword can be attributed to three things: (a) the cypher which had been used was known, or at least correctly guessed; (b) a piece of the plain text which had been encyphered was known, or at least correctly guessed; (c) we had good luck. To deal with the last first, we made several placements not on a basis of cast-iron proof but merely on the principle of trying the most likely possibility first, and all these placements came up trumps. Normally, at least one would have led down a blind alley, and we would have had to backtrack and try something else. This would almost certainly not have prevented the finding of the keyword, but the process would have taken longer.

As regards knowing or guessing the cypher used, (a) a count of the frequencies of the various letters in the complete message showed that it wasn't a simple letter-for-letter substitution cypher, (b) examination of a dictionary in the preceding chapter had disclosed a number of underlined words, each of at least seven letters with no repeating letter, suggesting that they had been earmarked for use in a cypher which required keywords of this kind, and (c) Wimsey had had previous experience of the Playfair cypher and knew it to be one such. Yes, it was a lucky guess, but such things do happen.

There remains the knowing or guessing of a piece of the plain text. As Wimsey says, nobody but an amateur would start an encyphered letter with two isolated lines which could be interpreted as town and date, but military messages in particular tend to contain stereotyped terms and phrases which can be looked for. Any sycophantic Nazi who ended all his messages with a dutiful "Heil Hitler" will have been a godsend to Bletchley Park. Even an apparently innocuous phrase such as

```
NOTHING TO REPORT
```

can give away a keyword.

Indeed, what has impressed me most about this exercise is how little correctly guessed plain text may be needed to crack a cypher wide open. Wimsey remarks that the Playfair cypher was used during the First World War, and that he had used it himself. One can only hope that no important message fell into enemy hands.