Breaking M4: How would Bombes do it?

Geoff Sullivan

The M4 Project http://www.bytereef.org has now produced two breaks into original German U-Boat messages from the North Atlantic from messages intercepted in November 1942.
Examination of these two messages has revealed some interesting information. In the first message, broken on 20th February 2006, about one third into the message we find:

MARQUANTONJOTANEUNNACHTSEYHSDREI

And in the second message, broken on 7th March, also about one third into the message we find:

MARQUANTONJOTADREINEUNNEUNFUENF

These are two positions in the naval grid system used by the German navy (AJ9863 and AJ3995). Major grid AJ is located south of Greenland. These two stretches of text are rather interesting, giving in the first instance the position of enemy ships and in the second the position of the U-Boat. Each message originated from different U-Boats, composed by its commander, but have identical formats, which is quite amazing and illustrates how cribs come about. We can perhaps assume that the third message, soon to be broken, will have a very similar stretch of text....
The German navy grid system was used to avoid giving latitude and longitude information in its radio transmissions. Each letter pair grid was 480 nautical miles on a side, further divided into 91 smaller squares each of 54 miles across – the first two numbers in the reference. Each of these numbered squares was further sub-divided into 9 smaller squares. A position could therefore be given to within 6 nautical miles.

We will attempt to use the second position message as a crib in a reconstruction of a Bombe run to find the Enigma key. The second message is 200 letters long. If we take the middle third of the message, we have 67 characters of interest. It is a property of the Enigma that no letter can be enciphered to itself. We can therefore find positions where the chosen crib is a possible decryption of the cipher text and positions where it cannot be. Aligning the crib at first position, the 66th letter, we find the 10th position in the crib has an identical letter (a crash). So this cannot possibly be the correct position of the crib in the message:

```
MARQUANTONYOTADREINEUNNEUNFUENF
ANWXGTKTHNRLVHKZPGMNMVSECVCKHOI
```

We find that the first position in the middle third of text where there is no crash is at letter position 72:

```
MARQUANTONYOTADREINEUNNEUNFUENF
TKTHNRLVHKZPGMNMVSECVCKHOINPLHH
```

Of the 35 alignments of crib in the middle third of the message, 20 have a letter crash and can be excluded, 15 are possible candidates for the correct position of the crib.

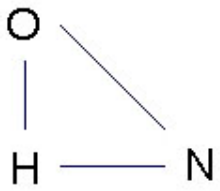
For an example of the Bombe run, the alignment at the correct position will be used to run on the Bombe simulator software

MARQUANTONYOTADREINEUNNEUNFUENF
CKHOINPLHHPVPXKMBHOKCCPDPEVXVVH

The main idea in creating a menu, a wired configuration for the sets of wheels in the Bombe, from a crib is to produce a chain of letter pairs from the two aligned texts paying particular attention to forming the chain into one or more closed loops wherever possible. A useful explanation of this can be found in [1] or [2].

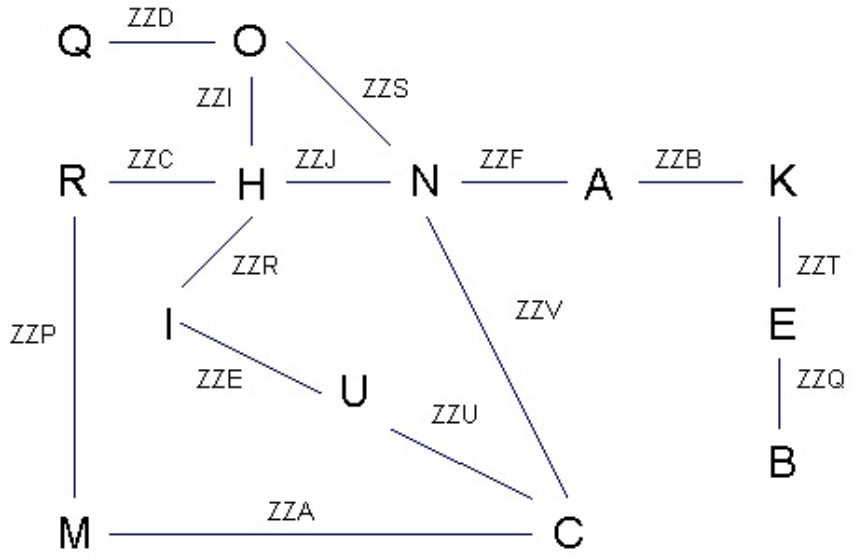
For example the first loop, or closure, can be formed easily by looking for high frequency letters. We have at positions I, j and s the chain
O > H > N > O

```
Position:  abcdefghijklmnopqrstuvwxyzabcde
crib:      MARQUANTONYOTADREINEUNNEUNFUENF
cipher:    CKHOINPLHHPVPXKMBHOKCCPDPEVXVVH
```



Another desirable feature is to group the linked letters close together or to choose letters from several close neighbouring groups with gaps between them. The reason for this is we do not know whether a middle wheel turn-over will take place. By forming the menu thus it reduces the number of Bombe re-runs if the first run should fail. A subsequent run will need to have an assumed turn-over inserted somewhere into the menu. The fewer places where a turn can be placed gives less Bombe re-runs. Working through the menu, we arrive at the sequence shown below. Trailing links have also been added, for example O-Q and N-A-K-E-B. These have been added where they are near to the other closed letters, to avoid the increased possibility of testing for middle wheel turns. These letters have the effect of strengthening the menu slightly, but the main strength comes from the closed loops. By strength we mean a menu configuration that will produce few false stops. Ideally it should contain several closed loops.

```
Abcdefghijklmnopqrstuvwxyzabcde
MARQUANTONYOTADREINEUNNEUNFUENF
CKHOINPLHHPVPXKMBHOKCCPDPEVXVVH
```



Each link has been labelled with 3 letters, for the three moveable wheels. These are the relative offsets that each set of wheels is set to after connecting up the 26-way Bombe cable. Bletchley used ZZZ as the zero position, hence the first candidate decryption is C > M at wheel position ZZA (the wheels step before encoding a letter).

The Bombe result file, after a complete 336 wheel order run, runtime around 30 minutes (P4 1.5GHz) has produced just two stops:

```
1  ZZA M C
2  ZZB A K
3  ZZC R H
4  ZZD Q O
5  ZZE U I
6  ZZF A N
7  ZZI O H
8  ZZJ N H
9  ZZP R M
10 ZZQ E B
11 ZZR I H
12 ZZS O N
13 ZZT E K
14 ZZU U C
15 ZZV N C

menu letters:    ABCEHIKMNOQRU
input at N

BB156 QRXZ  Steckers: V/O Q/I U/U J/H Z/R F/B T/E X/K A/A D/N P/C L/M

BB241 MWOA  Steckers: B/B P/E Q/K O/I T/A J/N L/C U/M D/H X/R

153543936   positions considered
```

We have two Bombe stops for wheel order BB156 and BB241. The second stop looks like the correct Stecker, but the wheel positions don't seem to make any sense. Why are there two stops, would we expect a unique solution for this message? If we attempt to decrypt the message we will find that all letters in the menu decrypt, but at any intermediate positions we may get other letters. For example the expected P > N decrypt at position g in the crib may be some other letter in an false stop. The Bombe did not test this position. We can therefore reject any stops that don't give the correct decrypt for every letter in the message crib, although we need to watch out for Steckers, if any that are not known. For example the Stecker F/G is not in the stop list, since it is not in the menu and not Stecker-paired to any menu letter.

The wheel positions given by the Bombe are not at the start of the message but are at the position where the crib was placed. This goes some way to explaining why they look wrong. Furthermore the dials on the Bombe drums are marked A-Z in reverse order and in conjunction with the the start position being Z rather than A, the conversion from Bombe to Enigma positions is:

```
Bombe dial:      ZABCDEFGHIJKLMNOPQRSTUVWXY
Wire position:   ZYXWVUTSRQPONMLKJIHGFEDCBA
```

There is yet one more complication of the drum markings. The wheel wiring for the first 3 wheels was recovered mathematically by Marian Rejewski between December 1931 and January 1932. The wiring for wheels 4 and 5 was recovered by him at a slightly later date and these have rotation offsets of 1 and 2 respectively compared to the actual wheels. Hence the conversion table for these two wheels is:

```
Bombe dial:    ZABCDEFGHIJKLMNOPQRSTUVWXY
Wheel 4:       YXWVUTSRQPONMLKJIHGFEDCBAZ
Wheel 5:       XWVUTSRQPONMLKJIHGFEDCBAZY
```

Using these conversions the stop position MWOA becomes MCJY (for wheel order 241). This is the position of the wire core at the start of the crib. Moving the wheels back by 92 positions will get to the wire core position of the message key for the second break which is MCFK. Note that the Bombe does not give any ring positions other than any that are set into the crib. This explains why the hill-climb key is different at MCSF with Ringstellung AANV. Since there was no slow wheel turn, the hill climb could not determine the middle ring. Both breaks have identical wire core positions.

This Bombe run was quite lucky, since although the crib spans 22 letters there was no mid wheel turn-over. If no stops were verified as correct then it is possible that there is a turn-over within the crib. The first position to insert a turn-over is at position k, since this eliminates five positions k-o with one run. If this failed a turn would be next placed at position g. If still no break then the run would need to be placed at each other position in turn. Hence there may be up to 14 full runs needed to exclude the possibility of a middle wheel turn on this menu. The turn-over is set by moving the middle drum forward by one position for each node after the turn, for example the R-M connection would be set to ZAP for the second run. If all these runs failed, then one of the other 15 possible crib positions would need to be run. If there was some uncertainty of the small grid square in the crib then MARQUANTONJOTADREINEUN may be used. In this case there would be 48 alignments in the middle third of the message with 26 possible fits and 18 crashes.

The US Bombe machines, manufactured by NCR, on which most of this 4-wheel work was done were fitted with 16 sets of wheels, so the above menu could be run on these machines. Using only the first 19 letters of the crib, the 15 non-crashing alignments of crib and cipher produces the following links. These have not been checked for possible closures but it seems likely that a useable menu could be formed from most positions for this crib.

Posn.	Links
71	ADEGKLMNRTUV HOPQ IS YZ
77	ACDHIPRVY EGKLMNOQST UZ
78	ACDEGHIMNOTV KR PU QZ SY
80	AEIKMNUZ COPRSTVY DH GQ
81	AGHIMPQRZ CDENOUVY KST
82	ACEGHKMNOPQRSTUVY DIL
83	ACDEGHILMNOPQRSTUV KY
85	ACEHIKMNOPRTUVY DL QS
90	ACDHILMNOPRTUVXY EKQ
92	ACDHIKLMNOPQRTUVXY BE
93	ABDEHIKLMNOPQRTUX VY
95	ABCDEHIKMNOPQRTV LU XY
96	ACDEHIKMNOPRUXY BTV LQ
97	ABHIOPQTUX CELR DKMNVY
100	ABCHKMNOTXY DEIPRU QV

This report has shown how a Bombe run might works against a crib. Whether such a crib or range of cribs could be obtained is open to question. Direction finding (HF-DF) results were somewhat erratic [4, 232], but improvements by applying corrections obtained from decrypts was possible. The 4-wheel Bombes did not enter service until mid 1943 [5]. Even then a full 336 wheel order run would take many days. The usual way into naval Enigma was by breaking weather code messages enciphered on 3-wheel machines and obtaining the M4 fast wheel identity from “Banburism”. Running this crib, with so many wheel orders and several menus, would not be practical without this additional help.

Geoff Sullivan March 2006

References

1. Welchman, Gordon.1997. *The Hut Six Story*. Kidderminster UK: M & M Baldwin.

2. http://www.ellsbury.com/bombe1.htm

3. *6812th Signal Security Detachment (PROV)*, dated 15 June 1945. NARA Record Group 457, File #2943, 7.

4. Hinsley, F. H. with R. C. Knight, E. E. Thomas, C. F. G. Ransom. 1985 *British Intelligence in the Second World War.* Volume 2. London HMSO.

5. Erskine, R. *Breaking Naval Enigma (Dolphin and Shark)*