Breaking M4: Was it a lucky break?

Firstly we must congratulate Stefan Krah and his team on breaking an original Naval Enigma message which has confounded amateur cryptography circles for a few years. We hope they continue to succeed.

But was the break lucky, easy or hard? As veterans of breaking a few hundred Wehrmacht Enigma messages we thought we would analyse this break and also try out our Ebreaker software on this message.

First the cipher text, repeated in newspapers all over the world:

```
NCZW VUSX PNYM INHZ XMQX SFWX WLKJ AHSH NMCO CCAK UQPM KCSM
HKSE INJU SBLK IOSX CKUB HMLL XCSJ USRR DVKO HULX WCCB GVLI
YXEO AHXR HKKF VDRE WEZL XOBA FGYU JQUK GRTV UKAM EURB VEKS
UHHV OYHA BCJW MAKL FKLM YFVN RIZR VVRT KOFD ANJM OLBG FFLE
OPRG TFLV RHOW OPBE KVWM UQFM PWPA RMFH AGKX IIBG
```

And a frequency count of these letters may be of interest. It is nowhere near flat, but that's often the case with Enigma messages:

```
K  M  H  V  U  R  L  X  O  F  S  C  A
17 13 13 12 12 12 12 11 11 11 10 10 10

W  B  E  N  I  G  P  J  Y  Z  Q  T  D
9  9  8  7  7  7  6  6  5  4  4  3  3
```

Here is the break:

```
UKW: B
W/0: B241
Stecker: AT BL DF GJ HM NW OP QY RZ VX
Self Steckers: C E I K S U
Rings: AAAV
Message key: VJNA
```

```
vonvonjlooksjhfffttteinseinsdreizwoyyqnnsneuninhaltxx
beiangriffunterwassergedruecktywabosxletztergegnerst
andnulachtdreinuluhrmarquantonjotaneunachtseyhsdreiy
zwozwonulgradyachtsmystossenachxeknsviermbfaelltynnn
nnnooovierysichteinsnull
```

The first thing we note is that the self-Steckered letters includes K which has a unusually high frequency in the cipher text (17) and E and S which are two of the most common letters in plain (23 and 17 respectively in the decrypt). This offers a very good starting position for a successful hill climb.

The next thing we note is the frequent occurrence of numbers within the message. These have high n-gram frequencies and are of considerable help to hill climbs:

```
vonvonjlooksjhfffttteinseinsdreizwoyyqnnsneuninhaltxx
beiangriffunterwassergedruecktywabosxletztergegnerst
andnulachtdreinuluhrmarquantonjotaneunachtseyhsdreiy
zwozwonulgradyachtsmystossenachxeknsviermbfaelltynnn
nnnoooviersichteinsnull
```

The third thing in favour of attacking this message is the length, 232 letters of cipher which helps a lot, as long as there is no slow wheel turn complication.

There are only few garbles in the numbers, *eins* (twice) and *sechs* are slightly garbled. Numbers are very important and are probably the main reason why some short Enigma messages can be successfully hill climbed. It is interesting to note that *acht* is not abbreviated to *aqt* as it is universally in army messages and also *nul* often has one l. In army messages *null* is more common. Fine tuning of n-gram databases may be important and this message contains some very valuable information. One interesting point is the phonetic alphabet letters *anton yot* which specifies one of the German navy's grid squares allocated to the world's oceans. The addition of this alphabet to the statistics would be very useful, it may be that many messages will have a position report and either *anton* or *berta* will occur in most north Atlantic signals. We encountered phonetic letters in the army messages but they tended to be always the same, for example *einsberta* for the military unit 1B. Naval grids will probably use the full alphabet. The use of Y and J for punctuation is also noted, as is the reduced usage of X which is more common in army messages.

Running this message on our Ebreaker system it hill climbed very readily. In fact we got high scoring breaks with the fast ring in the correct position and also when offset by +1, +2, -2, +4, -4 and +9 ring positions. Once the wheel settings had been reached the only thing likely to defeat a hill climb on this message would be a slow wheel turn, but that would depend on where it occurred. Luckily it did break and has provided very useful information for attacking the other messages in the series. The actual wheel order, 241, was lucky. Wheels VI, VII and VIII have two notches each and unless these were accounted for when in the two fast positions, it would make failure more likely. The probability of one of these wheels being in either of the two fast positions, assuming they are randomly selected, is 0.64. However it is wise to try the easier options first. And it worked!