

## Analysis to discover the cause of three (apparent) errors in the received inaugural Enigma M4 message from ZL1ANY

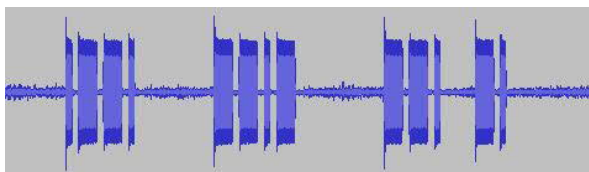
Band conditions on 80 m just after midday were typical for the daylight path across the Tararua Range between Masterton and Waitarere. Propagation, determined by both stations using ~ 10 m high horizontal half-wave dipoles, could only have been NVIS. This day, the mode had attendant moderate QSB and occasional S3 QRN; the report to ZL1ANY was RSN 421. QSB caused random loss of whole letters, probably typical of conditions experienced by *Funkers* managing Enigma traffic via QRP wireless from an *Unterseeboot* during WW2, and several repeats, were needed. Despite repeats and returns, two errors still crept in typical of those made when there is no context to enable incomplete or scrambled common words to be guessed.

### CRYPT TEXT ALLEGEDLY SENT

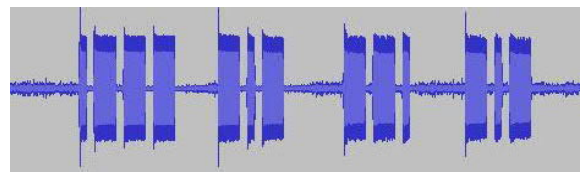
GYXY TXRS HUIQ MCJM PQGN CIWD IXRU JLDU XHFD  
UYZA JUJZ LYBI YK GK IYJW IWGC GZLI EBNT RGYX  
YTXR SXXX GYXY TXRS

### CRYPT TEXT RECEIVED

GYXY TXRS HUIQ MCJM PQGD CIWD IXRU JLDU XHFD  
UYZA JUJZ LYBI JK GK IYJW IWGC GZLI EBNT RGYX  
YTXR SXXX GYXY TXRS



Proof that the D instead of N was a receiving error



Proof that the J instead of Y was a sending error

Then we have the scrambled letters right at the end of the PLAIN TEXT ...  
SEVEN THREES **BSO**

In the third group from the end of the CRYPTTEXT, we see SXXX, showing that three filler letters, all Xs needed to be added to the message text to make complete four letter groups.

Instead of being appended to the PLAIN TEXT, however, they were inadvertently appended to the CRYPT TEXT, which is a protocol violation, and thus, when the CRYPT TEXT was transmitted the Xs revealed where the message text really ended, giving a crib to the enemy. The **RED** letters **BSO** at the end of the PLAIN TEXT, are the three Xs in the CRYPT TEXT which have effectively been encrypted by the decryption process. Had they been appended correctly, they would have decrypted to XXX in the recovered PLAIN TEXT and able to be ignored by the reader.

If there is one lesson is to be learned from this, it is the truth of the old adage:

### **‘The need for Accuracy supersedes any need for Speed’**

For reliable Enigma traffic handling regardless of machine type, especially in less-than-ideal conditions and when operators are unfamiliar with protocols and have no contextual indicators, 15 wpm or lower is recommended to provide more easily distinguishable letters and give time to think as well.