HAVE YOU TRIED THE "CHAOCIPHER"?

In 1953, Farrar, Strauss and Young published *"Silent Years, An Autobiography with Memoirs of James Joyce and Our Ireland"*, by John F Byrne. The book was reprinted by Octagon Books in 1975. Most of the book follows the title, but Chapter 21 goes wildly out of character with a highly detailed account of Mr Byrne's efforts from about 1922 to 1942 to interest the American government in his cipher machine. He made a model of it in a cigar box, and sent it to the likes of Friedman and (later) to Campbell of AT&T. These gentlemen neither praised nor condemned the idea, but it was not taken up by the military. *JFB* evidently felt that he was getting the thin end of the stick, and wrote his book naming names and giving dates, with a final challenge to anyone to determine how the cipher is constructed. This challenge was particularly aimed at the NY branch of the ACA. As far as is known, no-one has solved the cipher.

A description of the cipher, and an extensive analysis of it by CODEX, were given in *Cryptologia* for April 1978 and July 1979. One of the features of Byrne's book is that he is very free with his plain/cipher text equivalencies, from which you might think it would be easy to find the method used. He gives 100 successive encipherments of "ALL GOOD QUICK BROWN FOXES..." etc, followed by a 250 char encipherment of a Latin text, seven encipherments of a 26 group text, and a speech by General MacArthur! 15,500 equivalencies!

The first few of the 100 encipherments are given below. An error in the sixth group LYWIQ of the 4th row is noted in Byrne's writing dated 1937, but the correction is not legible. These encipherments and the seven 130-char encipherments are available on TRS80 or IBM disks from Mike Barlow. Can you apply your computing power to find a pattern to the encipherment? Can you say what the next encipherment row will read? What conclusions can you draw about this cipher? (Maybe before you read the reference material).

Byrne states that he has used a "Q" for the comma between "GOOD" and "QUICK", and a "W" for the period after "PARTY".

```
    ALLGO ODQQU ICKBR OWNFO XESJU MPOVE RLAZY DOGTO SAVET HEIRP ARTYW
 1  CLYTZ PNZKL DDQGF BOOTY SNEPU AGKIU NKNCR INRCV KJNHT OAFQP DPNCV
 2  LTVFI COTSS LWYYI HBICF UTHXN UVKGI MVEZY WSTHE PIEWX NNGFT OGHSR
 3  TBZXT MVGLT JXCSQ XLNJT ENCSV LCWRT BENZL SUVYI DAXLA FATQS RNZOP
 4  HKYGQ JTOGY SDBNV DJOWH KECRM LYWIQ IFIKS CYJGC VXNSK YHRYV YEDSZ
 5  RIFFZ AQNHS OMJPO RWTJO IJIPK VHZGP WQKRX DMAUE FFXIA CFLCZ MAFZS
 6  JEOZI FKJCF METES YYHZU VLFFU RRHRI IFFDZ MTTOV KLZOV LPVPP GVGEW
 7  WEFRF YHKXO PKXRQ SZKLC ZKHZW XRJXL MVFGG FGYIF DAEIN IWPOM OUVRF
 8  BUZLA GDBCU AMFQL ACRWW TUGSM PPZBR FASRO YIRCA GVEYN SRTOQ TDLFJ
 9  RUTKF KASGV LVYYF VRAIY NIVJK IUWPF ZBVRU EOTEJ GLCGY SSNHH QTIQW
10  UKQAS XKGSP WHRYM TQSOQ BAMAP FQRLI IUGTI VBEBY XFBIU SEYHM LKGOE
11  CSWUH TBIZZ HLBND IWTQA MAZBM YMBEK CYKCA BLYQY MELPJ OWNRV FZVKR
12  EBVUJ EQIAE MOHTG FHFFI DIQQJ UAWDH LUYRE UGSKT IMDWR RNONJ KDPTC
13  JDCJN BVEOU TWXOF GRXND KITNL OXSLZ WQRDE RERHL XWAMY LRVPR JFHRA
14  SDJWW OIWEV AVMRR NLRJM IFDHH ADDQC BZWYK DVPAY NPIAX BYUKI JGVUC
15  ACJHF XRALO VRLZU VANAB NZDZT PFQRI YCLLZ YILTW JBPAF LPOIO ZTBPI
16  USRXC DCITE EKMJB HPPYO NYEGS ZWGUR IFIPW UMTLJ YVYNE ACGJX JAGCX
17  QPDLA BSYMU DOKYD WRXCJ UFPXC PBWYQ PHMTA XNROB ASQRZ YVJXO HUXFP
18  BIHGG PKRFD MWTOT MKBOL BRRNO CHWLQ DVNEE VXBNE GHJQQ CVIEF YMEQR
19  XSYEW VJZTQ XDEWK WSWIE EHDSN RHRCV DUYOG NGVDP RHUTY KPRAO IVCUJ
20  DYVLO WBMGS TFTXU VOXGZ ZUIIR YXSAV EPRWP KQJMS VGYBN ECJOK CNMFP
21  GPHLK QQMBS LPMAC OZCNB RYAUO HNHBE SMIZT CEOBF KWXCE IOXZX EEIVJ
22  HGLQP QHMNF HXETY YPEAQ BUDWK NDXDZ BSLXX XCTLH CIWBI QHXHN YYFNH
23  NHYXA RKZMC RNZTO NKZKO SGNWF KJXRP QZIBR CPXCW FCCIM EKLBA BSHYA
24  EYGFQ DVTSD RQBSV RFKQG UQVTK CBERO IETFA TNGHQ OAHBA MSXAK VKBSY
25  LRORO IXQEZ APHAF CFFQW OZJUL UZBEQ AGYIP ZPHAB QQRIX LHRMS LJTSD
26  HHCVA HUPWS FMHVH JTRHA FDJFW CLEWE KUMFJ INAYG KRSLH NJFXY THFPU
27  PHULQ IZGLQ IMGWB EAVTJ AAPUM PYEMG DMUAG MAMZO TIRTT OWFVN KCYAQ
28  GZRFG XMBAV IXJCW NLIEP ENPVK IMNSS QTWPR UMWEG GJUNR QXTAT EBLDI
```