Radio and Communications

monitoring® monthly

January 2008 £3.95
EDITED BY KEVIN NICE

The magazine for real listeners

3rd Year of MM

SHORT WAVE SUPREMO

JRC NRD-630 Full Review!

Himalaya DRM2900 Portable - Analogue - DRM - DAB

Colossus Works Again!

Bletchly Park Deciphering Event

SAVE AGAIN WITH MM

£43 OFF UBC3500XLT PACKAGE

WIN! A CloseCall UBC72XLT Worth £90!

Taking radio into the future...

...across the whole spectrum

ISSN 1749-7809
01
9 771749 780010
www.monitoringmonthly.co.uk

COLOSSUS DECIPHERS AGAIN!

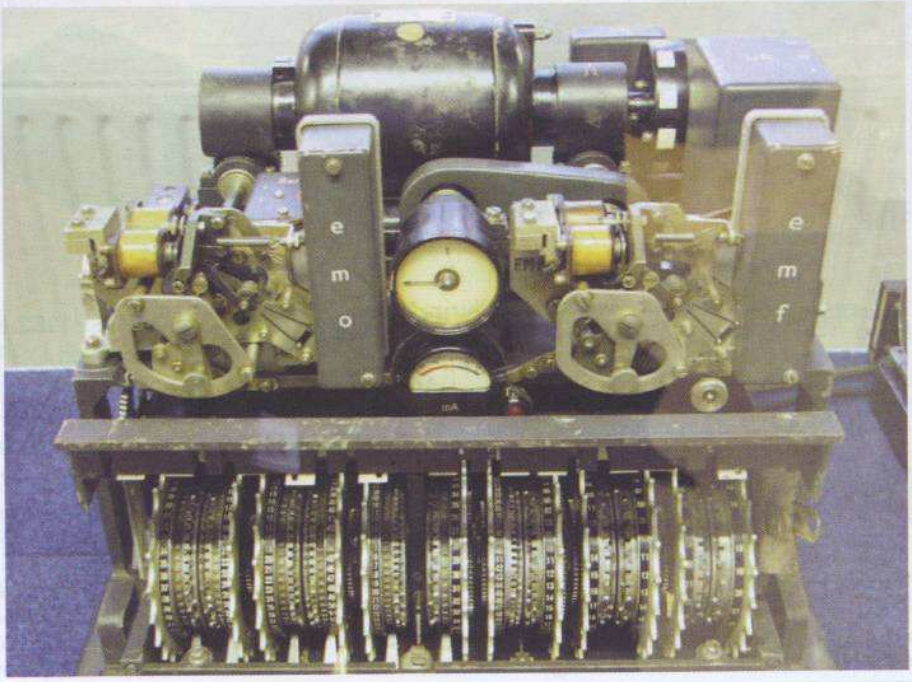
Cryptographic history was recreated on Friday 16 November 2007 when Colossus, for the first time in over sixty years, cracked an enciphered transmission from Germany. Milton Keynes ARS Members Andrew Thomas G8GNI/M5AEX, John Housego M0TIF, Graham Saville GIRNZ and David White G3ZPA bring us the details of the event.

Most people have heard about the Enigma machine, a typewriter-style device that was used to encipher transmitted messages during WWII and used primarily by the German field units. Perhaps less well known, are the Lorenz SZ42 (Schlüsselzusatz, meaning 'cipher attachment') machines. These were used for high-level communications and were large, heavy machines, measuring 510 x 460 x 460mm, which attached to a standard Lorenz teleprinter. There was a considerable amount of teleprinter traffic during the war, referred to as 'Fish' by British code breakers. The teleprinter traffic enciphered by the Lorenz machines was referred to as 'Tunny' see **Fig. 1**.

Enciphered Text

Teleprinter code - also known as ITA2 - is made up of seven and a half bits of information. Of the seven and a half bits, the first bit is the start bit, followed by five data bits, and ending with 1.5 stop bits. Each group of five data bits represents a letter, a number, or a control character (such as a letters shift, figures, shift, carriage return, line feed, space or un-performed tape), each bit being represented by a mark or a space. The Lorenz SZ42 machine consisted of 12 wheels, each one with between 23 and 61 unique positions - **Fig. 2**. The first five wheels, known as the K wheels, represented each of the five bits of the ITA2 character. These wheels were stepped in a regular order. The same process was then repeated with the next five wheels, known as the S wheels. These wheels stepped irregularly. The resulting letter represented the encrypted character. After each letter, the K wheels advanced one rotation, the movement of the S wheels being determined by the position of the final two wheels, known as the M wheels. In order to decipher a message that had been encrypted by the Lorenz SZ42 machine it was necessary to know the key, the key being the starting position of each of the 12 wheels. There were 16,033,955,073,056,318,658 possible starting positions!

The enciphered text was then transmitted as a radio-teleprinter (RTTY) signal using amplitude modulation (a.m.) and running at approximately 50baud. The transmitted signal was unusual as it comprised six tones - three separate two-tone RTTY streams each carrying the same information and with a 360Hz frequency shift. The transmitted tones are shown in **Table 1**.



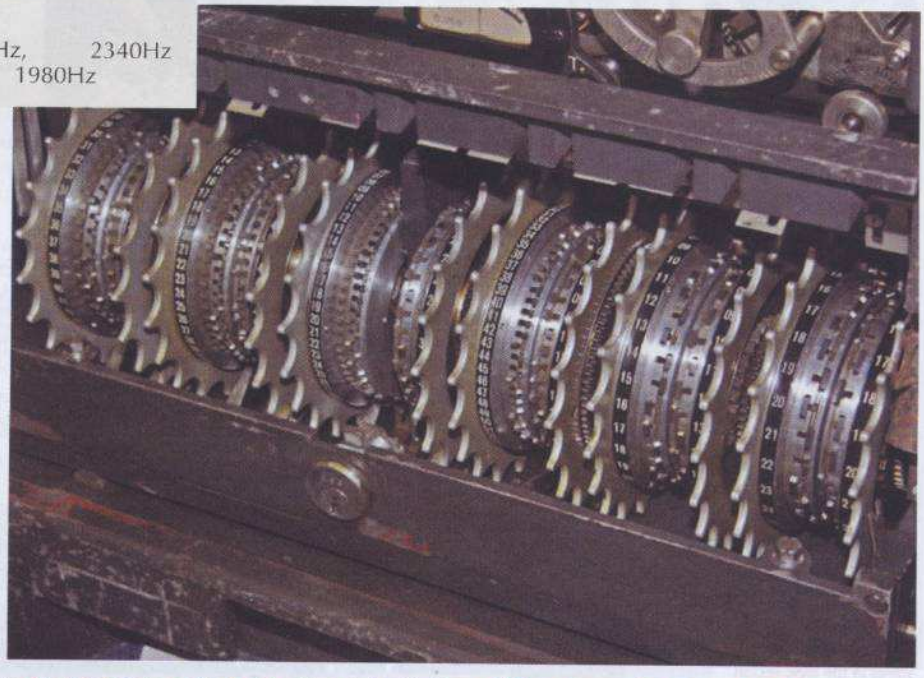
● *Fig. 1: The Lorenz SZ42 machine in all its glory Courtesy Matt Crypto.*

Table 1:

Mark:	900Hz,	1620Hz,	2340Hz
Space:	540Hz,	1260Hz,	1980Hz

Diversity reception was usually employed, each receiver being tuned to a different set of tones, thereby minimising the effects of selective fading and maximising the likelihood of 'good copy'.

The received text would then have been fed into a teleprinter, via a Lorenz SZ42 cipher machine. Providing the key had been correctly set up on the Lorenz machine, the output from the teleprinter would be plain text German.



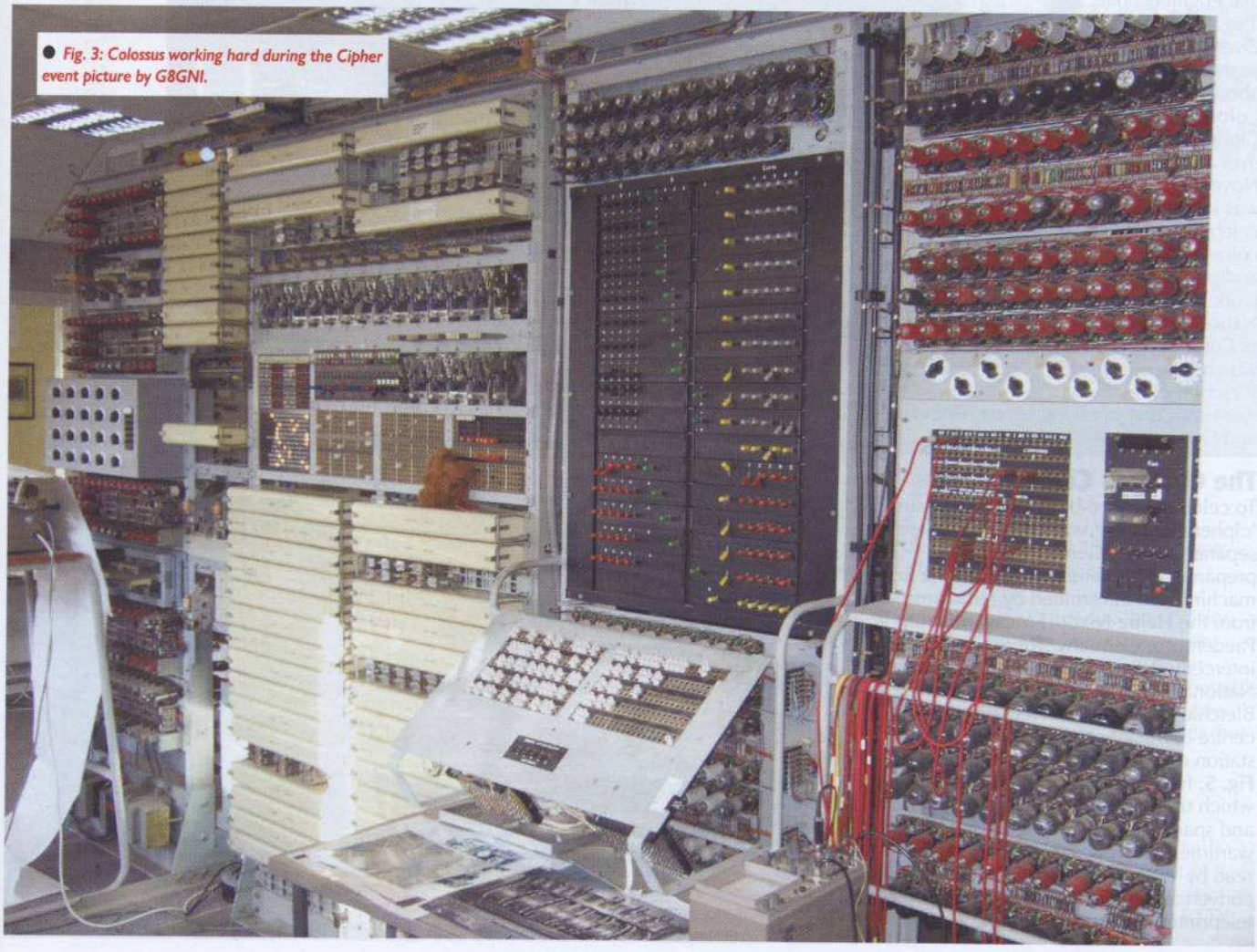
● *Fig. 2: A closer view of the 6 code setting wheels of the Lorenz SZ42 encipher machine Courtesy Matt Crypto.*

Critical Error

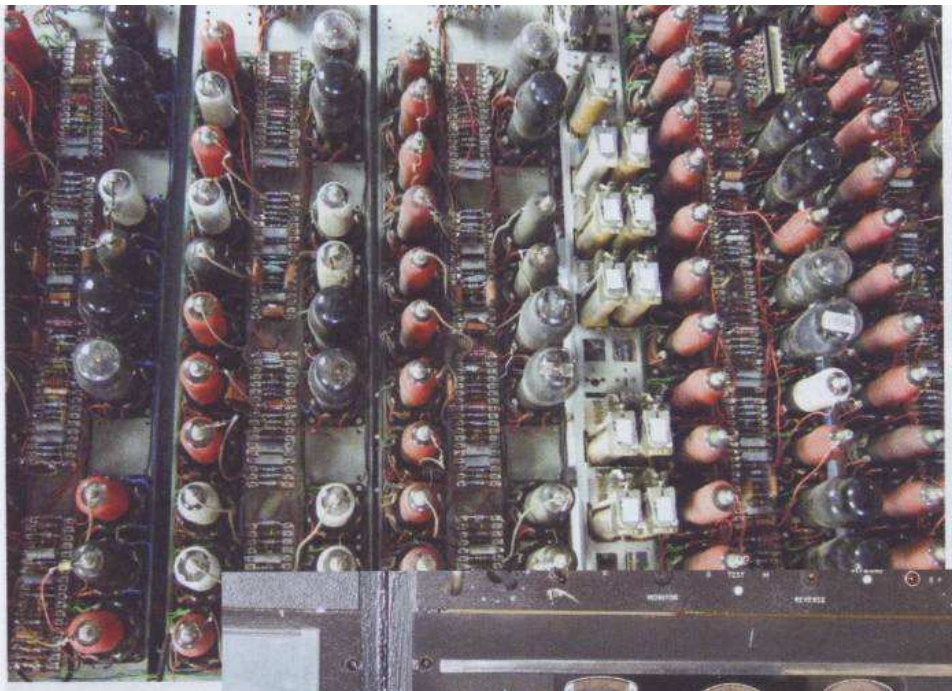
Following a critical procedural error made by a pair of German operators on the 30 August 1941, **Brigadier John Tiltman** was able to work out how the key stream from the Lorenz machine was produced. The Lorenz cipher could now be cracked, but it took weeks to do so. Enter Colossus, which reduced the 'cipher cracking' process from weeks to hours.

Colossus is a hard-wired and switch-programmed computer, similar to ENIAC. The war time Colossi - there were eventually 10 of them - were built by Post Office engineers at Dollis Hill under the direction of **Tommy Flowers**. After the war, eight of these were destroyed, the remaining two were taken to Eastcote in North London and then to GCHQ in Cheltenham, when in around 1960 they were eventually dismantled. All the drawings of Colossus were burnt, or at least most of them were.

In the early 1990s **Tony Sale** was able to obtain eight wartime photographs of Colossus plus some fragments of circuit diagrams



● *Fig. 3: Colossus working hard during the Cipher event picture by G8GNI.*



● *Fig. 4: Some of the valves in the logic secion of Colossus picture by G8GNI.*

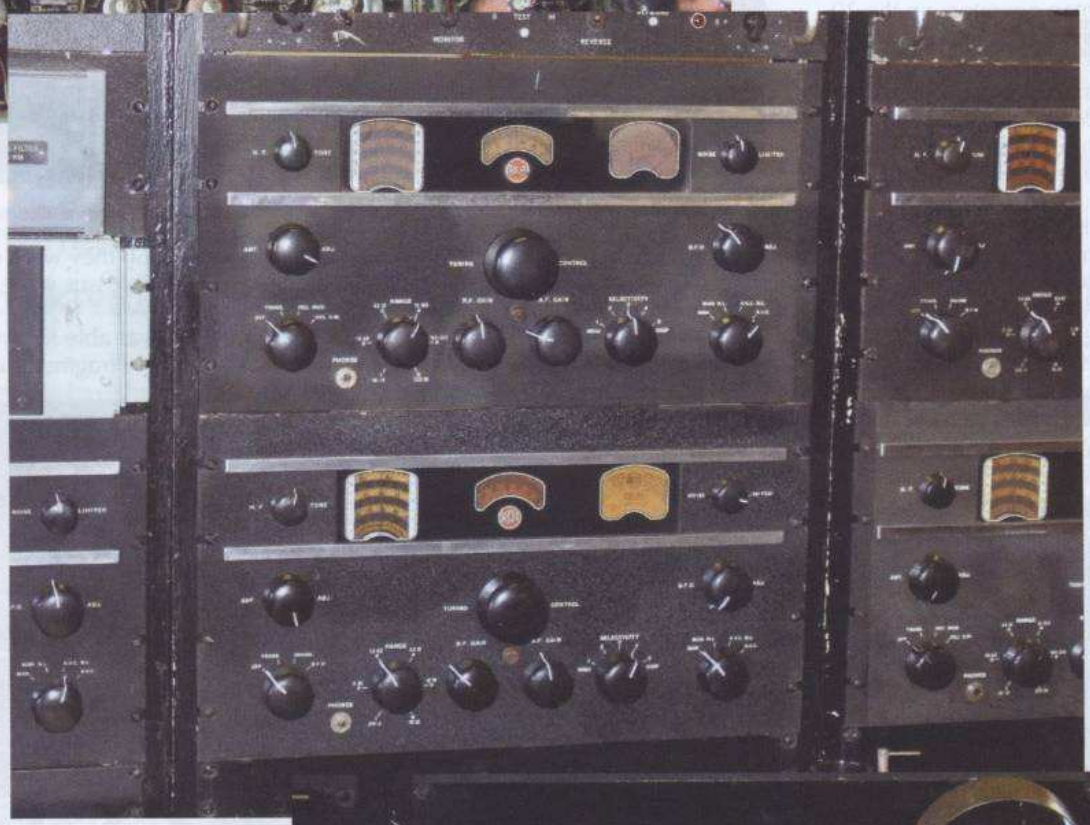
that engineers had illegally kept. Over the next 13 years Tony set about rebuilding Colossus. The Cipher event held over 15 and 16 November 2007 was intended to celebrate the colossus re-build and publicise the work of the National Museum of Computing, which is based at Bletchley Park, the war-time code-breaking centre. Both **Fig. 3** and **Fig. 4** show the rebuilt Colossus.

The Colossus Cipher Event

To celebrate the re-building of Colossus a 'cipher challenge' was proposed. Three separate, secret, German texts were prepared, enciphered using a Lorenz SZ42 machine and transmitted by radio amateurs from the **Heinz Nixdorf MuseumForum** in Paederborn, Germany. These were to be intercepted by a replica 'Y' station at the National Museum of Computing, based at Bletchley Park, the WWII code breaking centre in Buckinghamshire, UK. The Y station comprised AR88D receivers seen in **Fig. 5**, feeding an original undulator **Fig. 6**, which transferred the radio-teleprinter marks and spaces onto strip tape - **Fig. 7**. In wartime, these paper tapes would have been read by WRNS, the RTTY marks and spaces converted into characters and typed into a teleprinter machine, the output of which is a

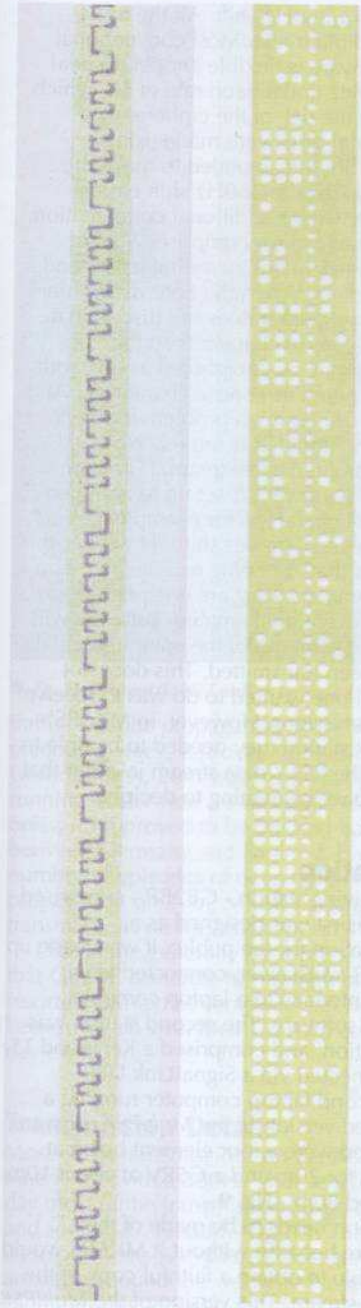
be read into Colossus which would then recover the Lorenz machine wheel settings used to encipher the plain text. The plain text messages would then be produced and sent back to the Heinz Nixdorf MuseumForum for validation. At the same time, radio amateurs around the world, would be able to receive the transmissions and have a go at deciphering the messages first.

The aim of the event was never to glorify war, nor to be seen as a competition between England and Germany. Rather, the event was designed to celebrate the re-building of the Colossus machine and in so doing to reflect on the outstanding intellectual and technical skills of those who originally designed and built the Lorenz SZ42 cipher machine and the Colossus computer.

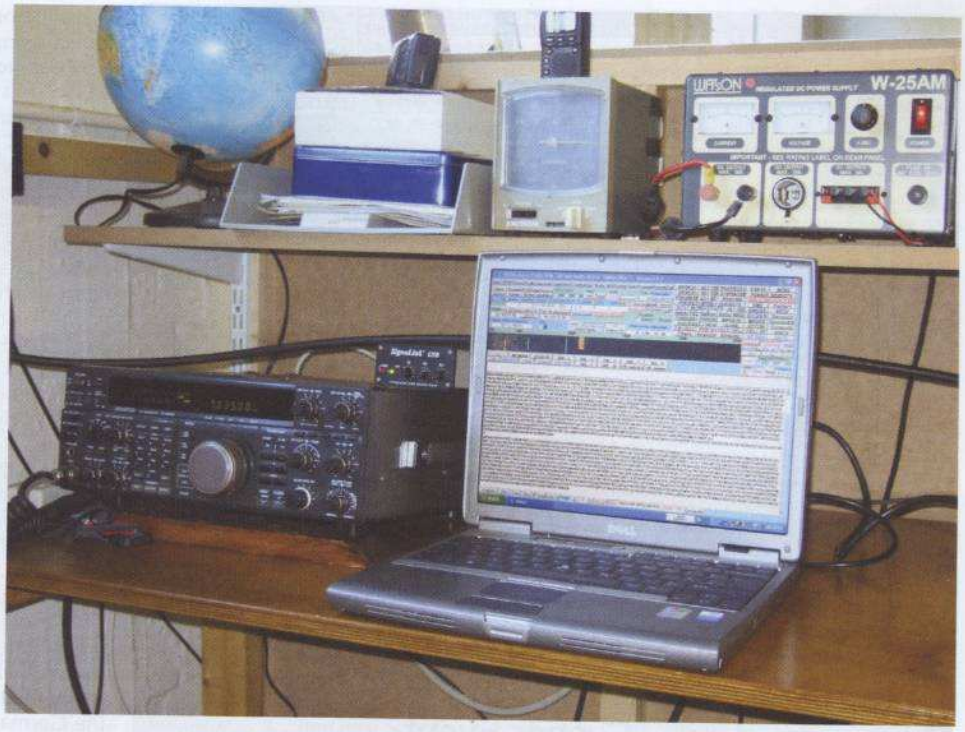


● *Fig. 5: The Y Station RCA AR88s. Picture by G8GNI.*

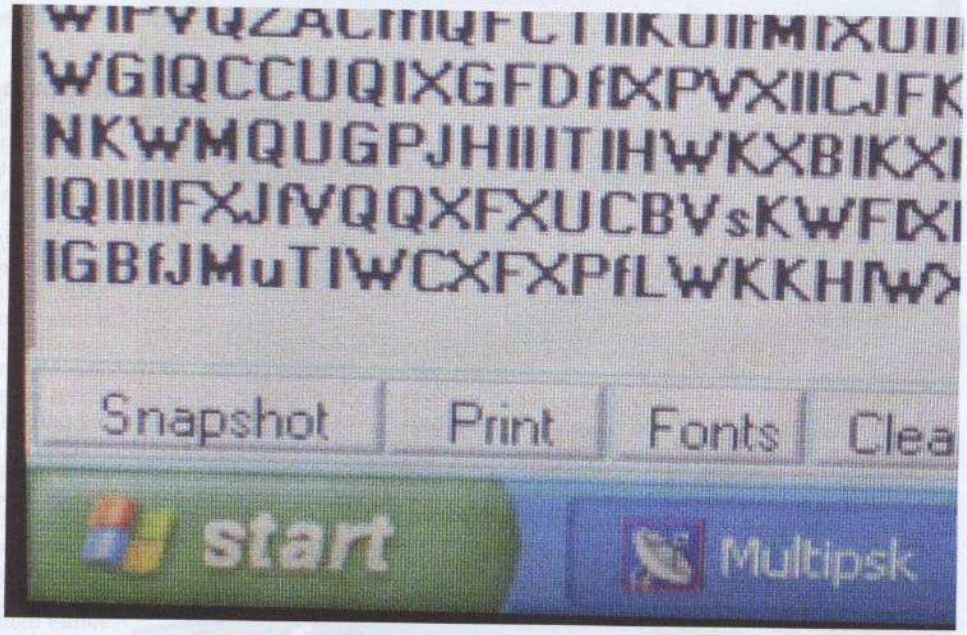
● *Fig. 6: The original undulator. Picture by G8GNI.*



● *Fig. 7: Undulator tape (left).* ● *Fig. 8: Teleprinter tape (right). Neither are of the ciphered text because the Y station was unable to properly incept them, but of a RTTY weather station transmission that was being used to test the undulators picture by G8GNI.*



● *Fig. 9: The MKARS intercept station picture by G8GNI.*



● *Fig. 10: The MultiPSK software in action during the event picture by G8GNI.*

The Role Of Amateur Radio

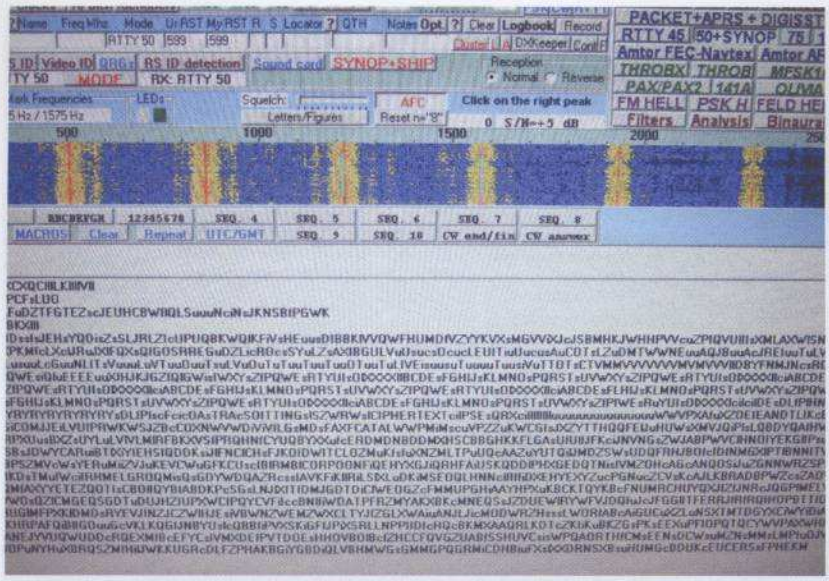
During the cipher event, the enciphered transmissions were sent by radio amateurs at the Heinz Nixdorf MuseumForum using the special event callsign **DL0HNF**. They had been given special dispensation to send enciphered messages as this would normally be in contravention of an amateur radio licence. At Bletchley Park there were two receiving stations - the replica Y station and **GB2BP**, the special event station owned and operated by the Milton Keynes Amateur Radio Society (MKARS). The role of MKARS was to provide a 'fall back', in case the replica Y station was unable to receive good copy, as well as to relay back the plain text message to Germany when Colossus had cracked the code.

In the two months prior to the cipher event, there were various test transmissions between DL0HNF and GB2BP that were designed to test the transmission and reception set-ups and to see how well the six tone generator would work. Propagation issues were also considered and the 80m, 40m and 20m bands were considered to be the most useable for the cipher event transmissions.

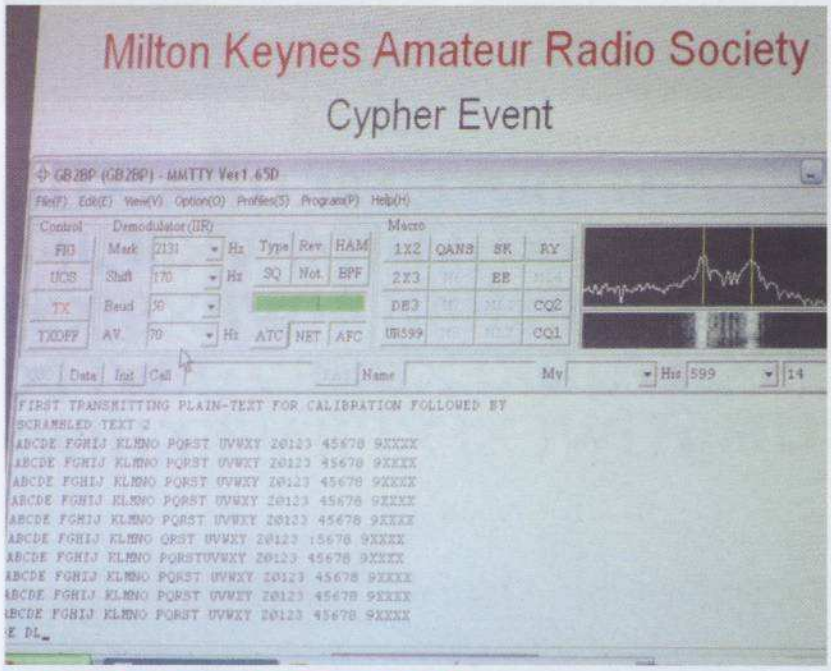
Although the wartime transmissions were a.m., the decision was made by DL0HNF to transmit using s.s.b. for the cipher event. This was in recognition that a high power transmitter would be required in order to give as wide a coverage as possible to the amateur community, but few amateur transceivers now produce 'true a.m.', nor with the requisite amount of power that would be needed.

Test Transmission

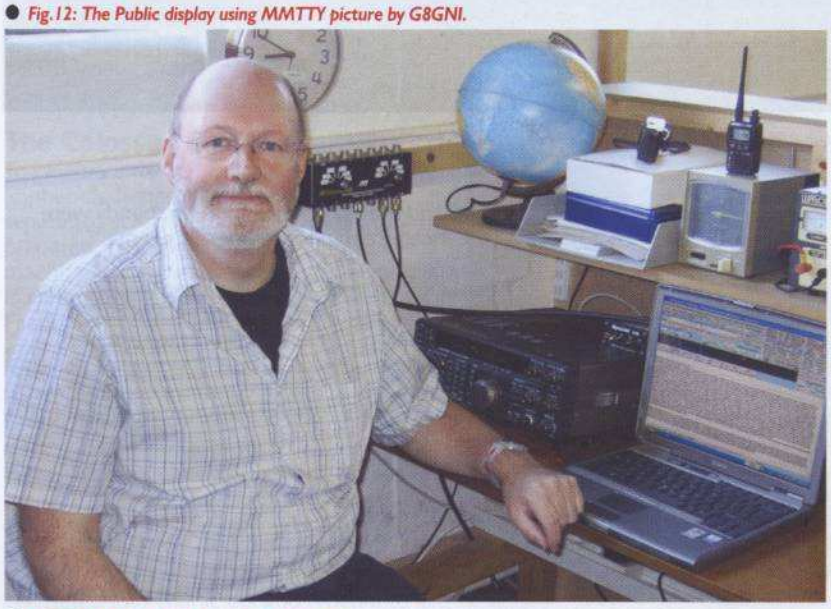
The initial test transmissions were made using 'standard' audio frequency shift keying (AFSK) RTTY with a frequency shift of 170Hz and a baud rate of 45.45, simply to test the equipment at both ends. Additional tests were made using the six tone RTTY



● *Fig.11: Plain text lead-in and switch to cipher using six-tone RTTY, 360Hz shift picture by G8GNI.*



● *Fig.12: The Public display using MMTTY picture by G8GNI.*



● *Fig. 13: Andrew G8GNI picture by G1RNZ.*

transmissions with a 360Hz shift. All the test transmissions used plain text. Most conventional amateur radio software is flexible enough to deal with a shift of 360Hz and a baud rate of 50, which would be used on the day of the cipher event. Indeed, all the initial tests were made using *MMTTY*, with the .ini file amended to make the switch over from 170Hz to 360Hz shift easier.

However, there was an additional complication. The ITA2 RTTY character set comprises a set of control characters (six in all) including letters and figures shift characters. When the Lorenz machine enciphers the data stream it does not discriminate between text and control characters so that the control characters may be enciphered as text and text may be enciphered as control characters. At the receiving end, this is not a problem for the Y station because the undulators are recording faithfully the transmitted data stream. However, conventional RTTY software is set up to act upon receiving a control character (for example implementing a letters / figures shift). However, the control characters that are being received are not really control characters, they are enciphered text! Consequently, conventional amateur software will not produce a true print out of the enciphered data stream that has been transmitted. This does not really matter if all one wanted to do was to receive the German transmissions. However, in MKARS' role as a fall back station they needed to be able to record faithfully the RTTY data stream in order that Colossus would have something to decipher.

Receiving Station

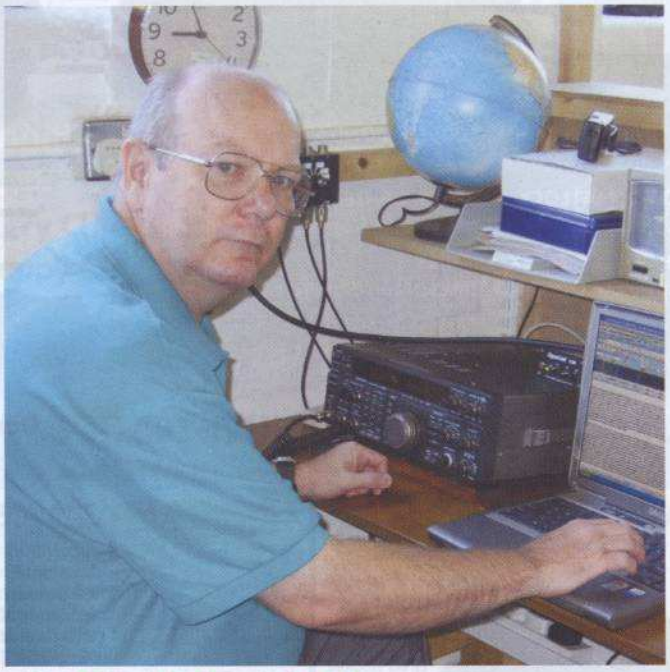
The MKARS receiving station - GB2BP - comprised two systems. The first was designed as a demonstration station for the public. It was made up of an Icom IC728 transceiver, connected via a SignalLink USB interface to a laptop computer running *MMTTY* software. The second station was the 'intercept station' and comprised a Kenwood TS-850S, again connected via a SignalLink USB interface to a second laptop computer running a specially modified version of the *MultiPSK* software. The antennas used were a four element beam at about 50m a.g.l. for 20m and a G5RV at about 10m a.g.l. for 40m and 80m - **Fig. 9**.

Special mention needs to be made of the *MultiPSK* software because without it MKARS would not have been able to obtain a faithful copy of the transmitted data stream. This version of the *MultiPSK* software was specially modified for MKARS by the software author, **Patrick Lindecker F6CTE**, and printed on screen all the RTTY control characters, rather than acting upon them, thereby providing an accurate representation of the RTTY transmission - **Fig. 10**.

The MKARS interception team comprised of the following people, **Andrew Thomas G8GNI/M5AEX - Fig. 13**, **Graham Saville G1RNZ - Fig. 14**, **John Housego M0TIF** and **David White G3ZPA**, with the event being recorded by **Charlie M0AIJ - Fig. 15**.

Transmission Schedule

A carefully planned schedule of transmissions had been laid down by the German team, with hourly transmissions from 0900 to 1800 on each of the two days of the event. Each transmission comprised one of three different enciphered texts. Initially starting on 40m, the transmissions moved up to 20m around mid morning, moving back to 40m and 80m later in the afternoon. Transmissions were made at the top end of the data mode segments in each band, in order not to interfere with other amateur RTTY



● *Fig. 14: Graham G1RNZ picture by G8GNI.*

traffic. Despite propagation on 20m being reasonable during the preceding week, it proved to be awful for the cipher event. Unfortunately, 20m was mostly unworkable despite DL0HNF running 400W into a 3-element beam. While 80m was often noisy, 40m proved to be the best band for solid transmissions between Germany and England. Even so, MKARS experienced a number of episodes of deep QSB (fading). Because of the poor propagation on 20m, MKARS arranged for some additional transmissions on the half hour on 40m and 80m.

Due to the generally poor propagation conditions and the fact that GB2BP is unable to run high power transmissions, MKARS resorted to Internet communications, using ICQ messaging, to keep in touch with their German colleagues throughout the two day event.

Transmission Details

Most of the transmissions on the first day of the event used six tone RTTY with a 360Hz shift sent at 50baud; on the following day most of the transmissions used two tones with a 170Hz shift and sent at 45.45baud.- **Fig. 11**. This was partly because there were problems with the six tone generator and partly to allow amateurs around the world an easier transmission to intercept. Each transmission was about 6000 characters in length and took around 15-18 minutes to transmit. The start of the transmission was in plain text and provided a greeting plus a test transmission of the alphabet. Following the sending of a 'QRX' the transmission then became enciphered. The screen picture **Fig. 12** shows the plain text at the start of the transmission. A brief plain text message ends the transmission. The public display, using conventional unmodified software, displayed gibberish as the software acted upon all the enciphered control characters. However, the MKARS intercept station, using *MultiPSK* in its modified form captured the data stream as it was being sent, with the control characters being substituted for lower case letters. If you look carefully at **Fig. 11**, you can see that the first half of the transmission is plain text. Just to the right of the middle of the text may be seen 'QRX' followed by a series of 'u's (un-perforated tape) and then the enciphered text begins.

During the event, the Y station was unable to receive any of the transmissions with sufficient accuracy to be of use by the Colossus team. However, MKARS was able to receive a number of very accurate transmissions, with the 1500 transmission on the first day being exceptionally clear and accurate. In order to 'play fair' and give the amateur world a chance to crack the code, Colossus did not start its deciphering run until the following day and was then held up for three-quarters of an hour when two of its 2500 valves had a problem. Just after lunch, the intercept that MKARS had obtained the previous day was deciphered by Colossus. As **Andy Clark** (National Museum of Computing) said on the BBC's News 24 website "For that, all credit must go to Milton Keynes Amateur Radio Society. They worked tirelessly yesterday."

In spite of the Bletchley Park team's success, as the world now knows, Colossus was beaten in the race by Bonn-based amateur **Joachim Schuth**. But, as Andy Clark, one of the founders of The National Museum of Computing, said "Colossus still did very well for a 60 year old machine".

Raised Profile

The event itself was enormous fun for the MKARS team. Not only did MKARS have unlimited access to Colossus and the Y station, but we made new friends in Germany and felt that we had been part of something historic. Plus it raised the MKARS public profile too, with local TV coverage, mentions on the BBC website and an enormous increase in hits on their own website. Talking to the public about the event, was also very rewarding, with a great deal of interest being shown in radio communications both vintage and modern.

Web sites

MKARS - **www.mkars.org.uk**
Bletchley Park - **www.bletchleypark.org.uk**
MMTTY - **http://amateur-radio.ca**
MultiPSK - **http://f6cte.free.fr/index_anglais.htm**
The National Museum of Computing - **www.tnmoc.org**

Notes

ENIAC - Electronic Numerical Integrator and Computer, constructed by the University of Pennsylvania's Moore School of Electrical Engineering from July 1943.

Tommy Flowers was a Post Office engineer who was asked by **Max Newman**, the mathematician, to build Colossus.

Y station - the name given to Royal Air Force listening stations.

MM

● *Fig.15: Left to right - Charlie M0AIJ, David G3ZPA and John M0TIF picture by G8GNI.*