A Colossal Challenge

The Cipher Event

Document Reference:	TNMOC.3.1
Document Status:	Issued
Document Version:	1.20
Issue Date:	4 November 2007
Deliverability:	See Section 1
Prepared by:	Andrew J Clark

Table of Contents

1 Introduction

1.1 Purpose

This document provides information on the planned cipher event to be staged on 15/16 November 2007

1.2 Scope

This document has been prepared to inform and share collected information with all those parties who will be directly and indirectly involved in the cipher event. It also provides background information that will be of interest to those planning to take part in the event.

The document owner is Andrew J Clark who will issue updates to the document from time to time as further information becomes available.

Definitive information on the event will be posted on www.tnmoc.org and updated from time to time.

1.3 Amendment History

Issue	Date	Author(s)	Revisions
0.10	1 Sep 2007	AJC	First Draft
0.20	3 Sep 2007	AJC	Included information on involved groups
0.30	9 Sep 2007	AJC	Added MOD contacts
0.40	1 Oct 2007	AJC	Added further info on SZ42 and supporting organisations. First information on transmission modes and times. Changed Appendix A to ITA No. 2.
0.50	2 Oct 2007	AJC	Minor typos and corrections, added Phil Fothergill to distribution, added Colossus image
1.00	4 Oct 2007	AJC	Issued for review
1.10	6 Oct 2007	AJC	Remove copyright, web links updated. Updated information on transmission times etc
1.20	4 Nov 2007	AJC	Incorporated time and frequency information, confirmed production of cipher, paper tapes etc.

1.4 References

Mnemonic	Document Details
[CIPHERCON]	Title: Notes, Actions & Contacts Doc Ref: TNMOC.3.2 Version: 0.10 Date: 1 Sep 2007

1.5 Deliverability

This document is distributed to the following named individuals:

Copy Number	Addressee
Original	Maintained in softcopy only by Andy Clark
1	Heinz-Peter Bleier - DL0HNF at HNF
2	John Housego – MKARS & GB2BP
3	John Pether – TNMOC
4	Jon Fell – TNMOC
5	Kevin Murrell – TNMOC
6	Norbert Ryska – Heinz Nixdorf MuseumsForum (HNF)
7	Rachel Burnett - BCS
8	Simon Greenish – BPT
9	Stephen Fleming – TNMOC/Palam
10	Tony Sale – TNMOC
11	Gareth Westlake – MOD
12	Nigel Sergeant – MOD
13	Phil Fothergill – TNMOC (Filming)

Although this document is not protectively marked, please do not disseminate the full contents further without approval from TNMOC as we will be co-ordinating publicity and press coverage.

Extracts from this document will be placed in the public domain from time to time at http://www.tnmoc.org/cipher1.htm

The primary contact for Media Relations is Stephen Fleming – his email address is stephen.fleming@palam.co.uk and his telephone number is +44 1635 299116 – please contact him before initiating any contact with media agencies so that such contact can be integrated into the main communications plan.

2 Background

2.1 The Lorenz Cipher Machine

In the 1930's the C. Lorenz Company of Berlin was the main supplier of teletype-machines (type LO14, LO15) to the German Army. They manufactured these under license from the US Teletype Corporation.

At that time the central office for the technical development and manufacturing of weapons, ammunition and equipment of the German army (the "Heereswaffenamt") wanted industry to produce a high security teleprinter cipher machine to enable them to communicate by radio in complete secrecy. In 1938 the Lorenz Company designed and constructed their SZ40 cipher machine beating competition from Siemens.

Chief engineer of the machine was Dr. Gerhard Grimsen from Brunswick. He had been working for Lorenz since 1926 formerly in the "Telegraphentechnisches Reichsamt". He designed a machine based on the additive method for enciphering teleprinter messages invented in 1918 by Gilbert Vernam in America.

Figure 1 - Dr. Gerhard Grimsen, Chief Engineer of the SZ40 and SZ42

While the well-known (man-portable) Enigma machine was generally used by field units, the Lorenz SZ40 and SZ42 (Schlüsselzusatz, meaning "cipher attachment") machines were used for high-level communications which could justify the heavy machine, teletypewriter and attendant fixed infrastructure. The machine itself measured 51cm × 46cm × 46cm (20in × 18in × 18in), and served as an attachment to a standard Lorenz teleprinter.

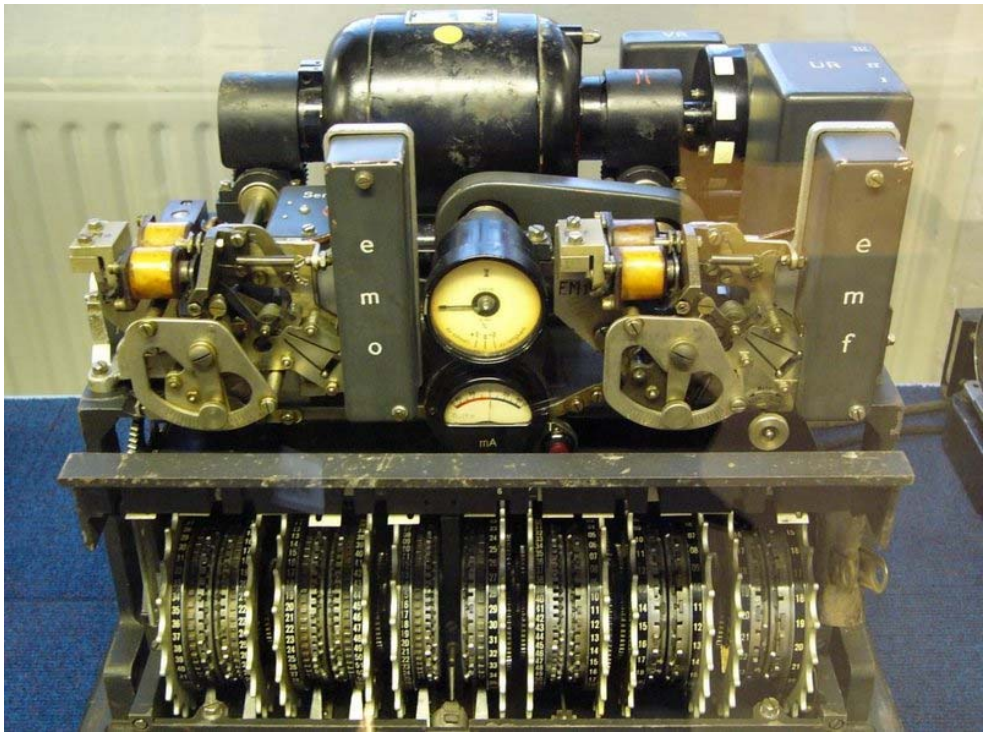

Figure 2 – A Lorenz SZ42 cipher machine on display at Bletchley Park[1]

The Vernam system enciphered the message text by adding to it, character by character, a set of obscuring characters thus producing the enciphered characters which were transmitted to the intended recipient. The simplicity of Vernam's system lay in the fact that the obscuring characters were added in a rather special way (known as modulo-2 addition[2]). Then exactly the same obscuring characters, added also by modulo-2 addition to the received enciphered characters, would cancel out the obscuring characters and leave the original message characters which could then be printed.

[1] Image credit – "Matt Crypto" - see http://en.wikipedia.org/wiki/Image:Lorenz-SZ42-2.jpg

[2] The working of modulo-2 addition is exactly the same as the XOR operation in logic.

The original Lorenz SZ42 machine consisted of 12 wheels, each one having 23 to 61 unique positions. Each position of a wheel represented either a one or a zero.

The first 5 wheels were called the K wheels. Each bit of the Baudot representation of a letter was xor-ed with the value showing on the respective wheel. The same process was repeated with the next 5 wheels, named the S wheels. The resulting value represented the encrypted letter. After each message letter the K wheels turn one rotation. The movement of the S wheels was determined by the positions of the final two wheels, called the M wheels.

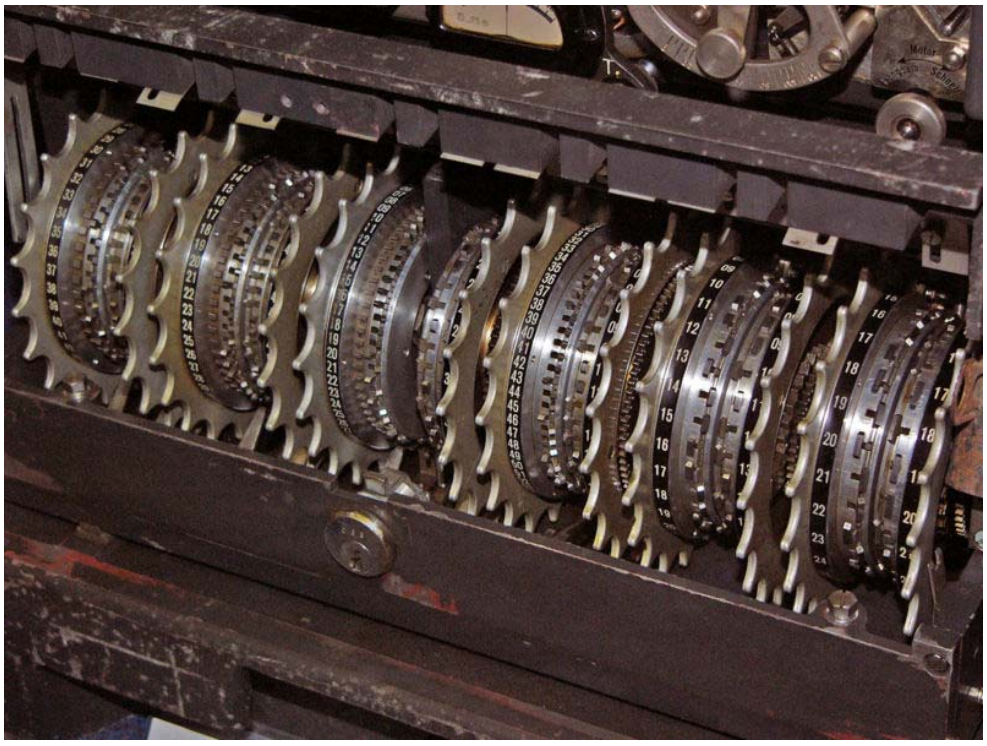

Figure 3 – Close up view of the twelve wheels[3]

Like most ciphers, the Lorenz machine also required a key. The key was the starting position of each of the 12 wheels. To decipher the message you simply need to start the wheels with the same position as was used to encrypt and enter the ciphertext. There were 16,033,955,073,056,318,658 possible starting positions.

[3] Image credit "Matt Crypto" – see http://en.wikipedia.org/wiki/Image:SZ42-6-wheels-lightened.jpg

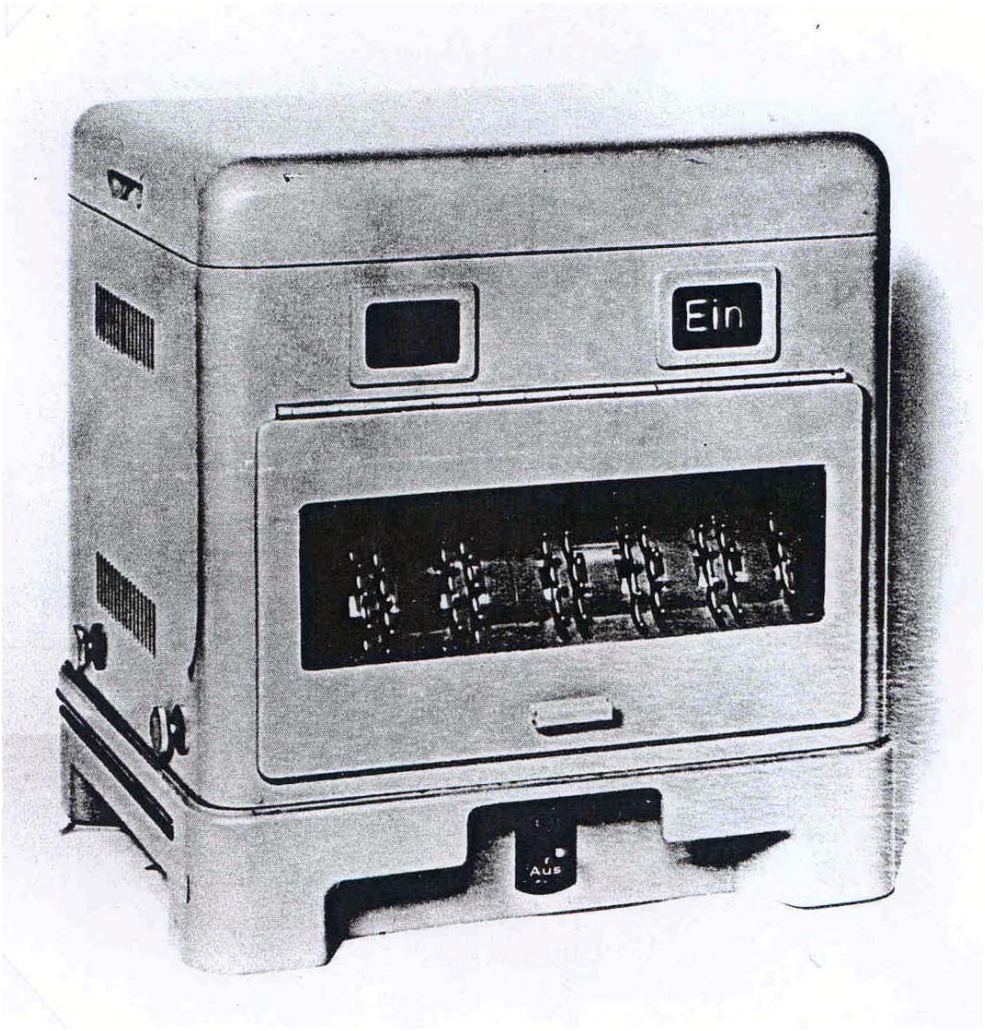

Figure 4 – in operation the SZ42 was enclosed within a sound proofing enclosure

2.2 British Cryptanalysis of the Lorenz Machine

The teleprinter signals being transmitted by the Germans and enciphered using Lorenz were first heard in early 1940 by a group of policemen on the South Coast who were listening out for possible German spy transmissions from inside the UK. Although unidentified at the time, the transmissions were from the "Oberkommando der Wehrmacht".

Brigadier John Tiltman, one of the top codebreakers in Bletchley Park, took a particular interest in these enciphered teleprinter messages. They were given the code name **Fish**. The messages which (as was later found out) were enciphered using the Lorenz machine were known as **Tunny**. Tiltman knew of the Vernam system and soon identified these messages as being enciphered in the Vernam manner.

Following a critical procedural error by a pair of German operators on 30 August 1941, Tiltman was able to determine the characteristics of the additive (obscuring) keystream being produced by the cipher machine. He passed his findings to **Bill Tutte**, who had recently come to Bletchley Park from Cambridge. Tutte started to write out in longhand the bit patterns from each of the five channels in the teleprinter form of the string of obscuring characters at various repetition periods. When he wrote out the bit patterns from channel one on a repetition of 41, various patterns began to emerge which were more than random. This showed that a repetition period of 41 had some significance in the way the cipher was generated.

Then over the next two months Tutte and other members of the Research section worked out the complete logical structure of the cipher machine which we now know as Lorenz. This was a fantastic tour de force and at the beginning of 1942 the Post Office Research Laboratories at Dollis Hill were asked to produce an implementation of the logic worked out by Bill Tutte & Co.

Frank Morrell produced a rack of uniselectors and relays which emulated the logic. It was called Tunny and now when the manual code breakers had laboriously worked out the settings used for a particular message, these settings could be plugged up on Tunny, the cipher text read in and, if the codebreakers had got it right, out came German. Unfortunately it was taking four to six weeks to work out the settings. This meant that although they had proved that technically they could break Tunny, by the time the messages were decoded the information in them was too stale to be operationally useful.

The mathematician **Max Newman** now came on the scene. He thought that it would be possible to automate some parts of the process for finding the settings used for each message.

He approached **TRE** at Malvern to design an electronic machine to implement the double-delta method of finding wheel start positions which Bill Tutte had devised. The machine was built at Dollis Hill and was known as **Heath Robinson** after the cartoonist designer of fantastic machines. Although it suffered from reliability problems, Heath Robinson worked well enough to show that Max Newman's concept was correct. Newman then went to Dollis Hill where he was put in touch with **Tommy Flowers**, the brilliant Post Office electronics engineer. Flowers went on to design and build **Colossus** to meet Max Newman's requirements for a machine to speed up the breaking of the Lorenz cipher.

2.3 Colossus

Colossus design started in March 1943. By December 1943 all the various circuits were working and the 1,500 valve Mark 1 Colossus was dismantled, shipped up to Bletchley Park, and assembled in F Block over Christmas 1943. The Mark 1 was operational in January 1944 and successful on its first test against a real enciphered message tape.

Colossus reduced the time to break Lorenz messages from weeks to hours. It was just in time for the deciphering of messages which gave vital information to Eisenhower and Montgomery prior to D-Day. These deciphered Lorenz messages showed that Hitler had believed the deception campaigns, the phantom army in the South of England, the phantom convoys moving east along the channel; that Hitler was convinced that the attacks were coming across the Pas de Calais and that he was keeping Panzer divisions in Belgium. After D-Day the French resistance and the British and American Air Forces bombed and strafed all the telephone and teleprinter land lines in Northern France, forced the Germans to use radio communications and suddenly the volume of intercepted messages went up enormously.

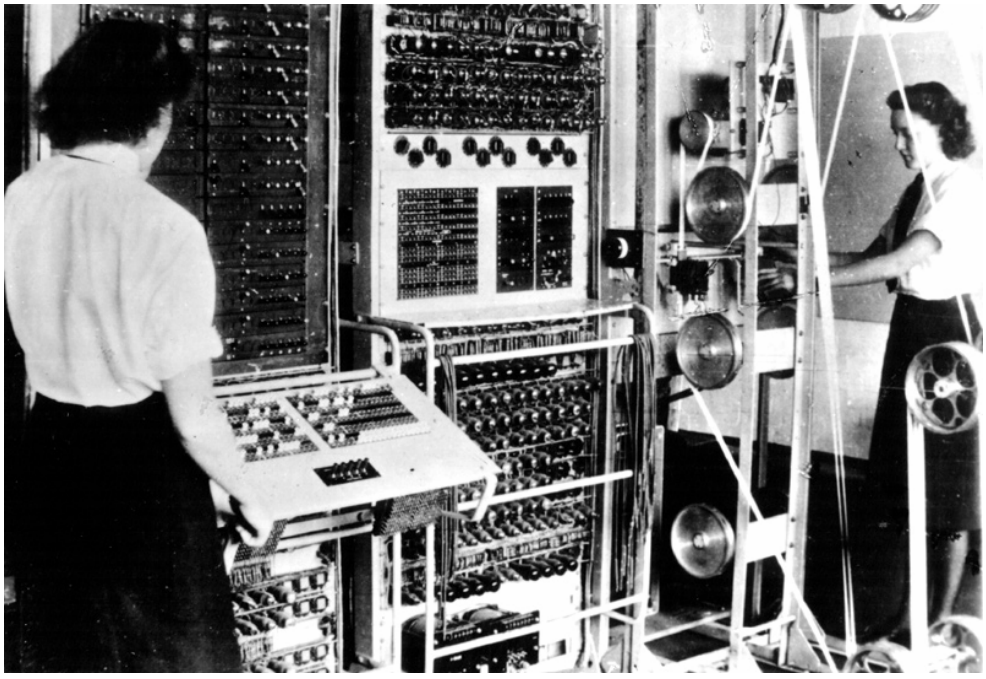

Figure 5 – a Colossus in operation in Bletchley Park during the war.

The Mark 1 had been rapidly succeeded by the Mark 2 Colossus in June 1944 and eight more were quickly built to handle the increase in messages. The Mark 1 was upgraded to a Mark 2 and there were thus ten Mark 2 Colossi in Bletchley Park by the end of the war. By the end of hostilities, 63 million characters of high grade German messages had been decrypted — an absolutely staggering output from just 550 people at Bletchley Park,

plus of course the considerable number of interceptors at Knockholt, with backups at Shaftesbury and Cupar in Scotland.

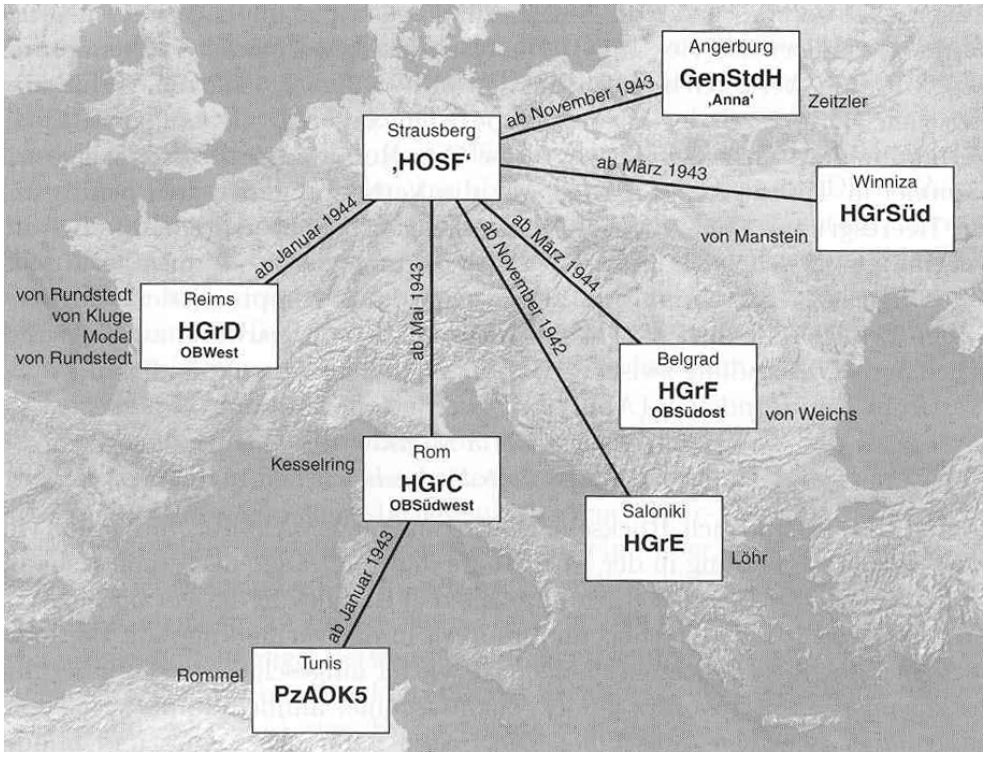

Figure 6 – The network of SZ40/SZ42 connections successfully broken by Bletchley Park – the first starting in November 1942 and the last in March 1944.

After VJ Day, suddenly it was all over. Eight of the ten Colossi were dismantled in Bletchley Park. Two went to Eastcote in North London and then to GCHQ at Cheltenham. These last two were dismantled in about 1960 and in 1960 all the drawings of Colossus were burnt. Its very existence was kept secret.

2.4 German Concerns over SZ42 Security

According to Wolfgang Mache, following debriefings of General Fellgiebel[4] after July 20, 1944, German cryptologists became concerned about the security of their cipher systems

As described by Dr. Hüttenhain (Ex-OKW Chi and ZfCH, Bonn) in a subsequent study they detected the breakability of the SZ40/42 in at least four "Betriebsarten" (operating modes). As a consequence the cryptologists requested operational restrictions for the machine and shorter message lengths. In practice these recommendations were not pursued.

[4] responsible for telecommunications in the "Oberkommando der Wehrmacht"

3 The Colossus Rebuild Project[5]

In the 1970s, information about Colossus began to emerge. Professor Brian Randell of Newcastle University started undertaking some research. Dr Tommy Flowers and some of the other design engineers presented papers in the 1980s describing Colossus in fairly general terms.

In 1991 when Tony Sale and some colleagues started the campaign to save Bletchley Park from demolition by property developers, he was working at the Science Museum in London restoring some early British computers. He believed it would be possible to rebuild Colossus (although nobody believed him at the time).

In 1993 he gathered together all the information available. This amounted to the eight 1945 wartime photographs taken of Colossus plus some fragments of circuit diagrams which some engineers had kept (quite illegally).

The first stage was to produce accurate machine drawings of the frames for Colossus (all the original machine drawings had been burnt in 1960). This involved three months of eyestrain poring over the photographs and using 3D projections to transfer the details to a CAD system.

The next problem was the optical paper tape reader system. The details of this are not shown in any of the eight photographs. However Tony managed to locate Dr Arnold Lynch who designed the reader system in 1942. Although well into his eighties Dr Lynch came to my house and using my CAD system we re-engineered the reader system to his original specifications.

In July 1994 His Royal Highness the Duke of Kent opened the Museums in Bletchley Park and inaugurated the Colossus Rebuild Project. At that point Tony had not managed to obtain any sponsorship for the project but in 1993 he and his wife Margaret decided to put their own money into it to get it started. Over the next few years various private sponsors came to their aid and some current and ex-Post Office and radio engineers formed the team that undertook the Rebuild.

Colossus first worked at two-bit level (out of the five-bit channels from the paper tape). HRH the Duke of Kent returned to the Park on 6 June 1996 to switch on the basic working Colossus.

[5] Excerpted from Tony Sale's history at http://www.codesandciphers.org.uk/lorenz/index.htm

In the past eleven years since that first switch on, Tony and his team have worked solidly towards completing the full rebuild of the Colossus Mark 2 at Bletchley Park. The Mark 2 machine implements Bill Tutte's method of **rectangling** that enables the Colossus to recover the Lorenz wheel settings using ciphertext only. This is the cryptanalysts holy grail.

The rebuild is marvellous tribute to Tommy Flowers, Allen Coombs and all the engineers at Dollis Hill and a great tribute to Bill Tutte, Max Newman, Ralph Tester and all the code breakers involved at Bletchley Park. We must also remember all the WRNS who operated and supported Colossus and the interceptors at Knockholt without whom there would have been no messages to break.

3.1 Performance of the Colossus

Colossus is not a stored-programme computer. It is hard-wired and switch-programmed, just like ENIAC[6]. Because of its parallel nature it is very fast, even by today's standards. The intercepted message, punched on to ordinary teleprinter paper tape, is read at 5,000 characters per second. The sprocket holes down the middle of the tape are read to form the clock for the whole machine. This avoids any synchronisation problems: whatever the speed of the tape, that's the speed of Colossus. Tommy Flowers once wound up the paper tape drive motor to see what happened. At 9,600 characters per second the tape burst and flew all over the room at 60 mph! It was decided that 5,000 cps was a safe speed.

At 5,000 cps the interval between sprocket holes is 200 microseconds. In this time Colossus will do up to 100 Boolean calculations simultaneously on each of the five tape channels and across a five character matrix. The gate delay time is 1.2 microseconds which is quite remarkable for very ordinary valves. It demonstrates the design skills of Tommy Flowers and Allen Coombs who re-engineered most of the Mark 2 Colossus.

Colossus is so fast and parallel that a mid-range modern PC programmed to do the same code-breaking task takes as long as Colossus to achieve a result.

[6] ENIAC, short for Electronic Numerical Integrator And Computer constructed by the University of Pennsylvania's Moore School of Electrical Engineering from July, 1943. It was unveiled on February 14, 1946

Figure 7 – Tony Sale programs the Mark 2 Colossus at Bletchley Park in January 2007[7]

[7] Image credit Mark Crick - http://www.markcrick.com/

4 The Cipher Event – Recreating the Past

On 15 and 16 November 2007 we shall celebrate the completion of the Colossus Mark 2 rebuild at Bletchley Park and recreate cryptographic history when an international team will:

1. Prepare three separate (secret) texts in German (the challenge plaintexts);

2. Encipher each of those plaintext messages using the Lorenz SZ42 cipher and prepare three paper tapes (the challenge ciphertexts);

3. Transmit each of those ciphertexts in turn using amateur radio operators in Germany;

4. Intercept the ciphertexts at a replica 'Y' station in the UK;

5. Interpret the ciphertexts using an original undulator and transfer those interpreted ciphertexts on to paper tape;

6. Load the paper tape ciphertexts on the Colossus Mark 2 rebuild in Bletchley Park Block H. Run the Colossus to recover the Lorenz machine wheel settings used to encipher the plaintext;

7. Recover the secret plaintext messages;

8. Validate the result.

At the same time as the international team receives the enciphered messages, radio amateurs around the world will be able to receive the same radio broadcasts and try their hand at decrypting it. It will be fascinating to see who completes the job first!

4.1 Encipher the Secret Message

Representatives from Heinz Nixdorf MuseumForum in Paderborn, Germany under the guidance of Norbert Ryska will prepare the challenge plaintexts (in German).

4.2 Transmit the Ciphertext

Radio amateurs at the radio station DL0HNF located in the Heinz Nixdorf MuseumForum, Paderborn will transmit the challenge ciphertexts. Heinz-Peter Bleier will lead the team and plans to operate a special event station with a dedicated callsign specifically for the purpose.

4.3 Intercept the Ciphertext

The Paderborn transmissions will be intercepted by two teams at Bletchley Park – the first will be led by John Housego and comprise members of the Milton Keynes Amateur Radio Society operating amateur radio station callsign GB2BP. They will use current technology receivers and signal capture methods.

Figure 8 – Paderborn is nearly due East of Bletchley Park and approximately 450 miles range.

The second team will be led by John Pether who will use the same type of equipment as used in the 'Y' (intercept) station in Knockholt in WWII. This equipment includes AR88 receivers with undulators connected for hardcopy output on strip tape.

Figure 9 – one of two undulators currently installed in the 'Y' station rebuild at Bletchley Park.

4.4 Interpret the Ciphertext

John Pether's team will interpret the output of the undulators by hand and punch paper tape directly for loading on to the Colossus Mark 2.

4.5 Run the Colossus Mark 2

Tony Sale and his team will load the paper tape containing the ciphertext on to the Colossus and run it to find the Lorenz machine wheel settings.

4.6 Recover the Plaintext

Once the Colossus has reported the wheel settings, Tony and his team will use the Tunny simulator to recover the plaintext (the TUNNY rebuild is not yet complete).

4.7 Validate the Result

Once the plaintext has been recovered, members of the MKARS will email and transmit the plaintext back to Germany using RTTY for validation and scoring.

5 The Cipher Challenge

There will be a series of transmissions of different ciphertexts representing different levels of cryptanalytic challenge.

5.1 Easy (1)

For the first challenge we shall provide:

- wheel patterns for all 12 wheels;
- start positions for the M and S wheels.

The cryptanalyst just needs to find the K wheel starts and then decipher.

5.2 Hard (2)

For the second challenge we shall provide:

- wheel patterns for all 12 wheels;
- start positions for the M wheels.

The cryptanalyst needs to find start positions for the K and S wheels and then decipher.

5.3 Hardest (3)

For the third challenge we shall provide:

- wheel patterns for all 12 wheels;
- no wheel start positions.

The cryptanalyst needs to find start positions for the S, K and M wheels and then decipher.

6 Background to the Organisations Taking Part

6.1 The National Museum of Computing

The National Museum of Computing is the operating name of CodesandCiphers Heritage Trust (CCHT). CCHT was incorporated as a company limited by guarantee on 30 March 2005 under company number 05407952. The company was granted charitable status in England and Wales on 6 June 2005 under charity number 1109874.

CCHT was formed in 2005 to protect the computing heritage at Bletchley Park – in particular the preservation of the Colossus computer. Following initial seedcorn fundraising it has started to establish The National Museum of Computing in Block H at Bletchley Park.

Built in 1944, Block H was designed to house the world's first digital computers, the Colossus machines.

The museum will allow visitors to follow the development of computing from the ultra secret pioneering efforts of Colossus, the post war innovations of the 1950s, through the mainframes of the 1960s and 1970s, and the rise of personal computing in the 1980s. Using original systems restored to working order with the help of the BCS's Computer Conservation Society, the museum will encourage visitors to operate and learn from our exhibits, and enjoy using machines they once used, programmed, or simply played with.

The Museum is currently seeking to raise £6M to preserve the UK computing heritage and establish a world-class museum facility in Block H at Bletchley Park.

6.2 Heinz Nixdorf MuseumForum

Heinz Nixdorf MuseumForum is the largest computer museum in the world and provides over 6,000 square metres of exhibition space showing over 5,000 years of world history.

It chronicles the emergence of numeracy and literacy from ancient times up to the 21st Century. More than 2,000 exhibits are shown within a social and economic context that makes them interesting to computer specialists and non-technical visitors alike.

The forum supplements the exhibitions with an extensive programme of meetings. Lectures, workshops and conferences stimulate discussions surrounding the influence of information technology on all aspects of human and society development.

6.3 Radio Amateurs at HNF

The radio amateurs in Heinz Nixdorf MuseumForum are a group that show visitors to the museum the theory and practice of operating an amateur radio station to communicate with others around the world.

The core of the group essentially consists of radio amateurs from “Funkamateure SNI Paderborn” and the local federation German amateur radio club (DARC) Paderborn Elsen.

The group operates the radio station DL0HNF that is located within the Heinz Nixdorf MuseumForum premises.

6.4 Bletchley Park Trust

In 1991, the site at Bletchley Park was almost empty and plans were afoot to demolish the buildings to make way for a housing development. The secrecy that had been so essential to Bletchley Park's success during the war was now counting against it. For secrecy meant ignorance, starving the Park of investment and resulting in its slow decline. By the time the public become aware of the Park's wartime and technological significance, it was almost too late.

In May 1991 the Bletchley Archaeological and Historical Society formed a small committee to bring together as many former codebreakers as could be traced, for a farewell 'thank you' before the site was destroyed. On 21st October 1991, the farewell party was held in the grounds. Over 400 codebreakers attended. As a result of the stories they told, it was decided to attempt to save the site for posterity.

Bletchley Park Trust was formed on 13th February 1992, three days after Milton Keynes Borough Council declared most of the Park a conservation area. Negotiations began with the site's landowners, the Government's land agency PACE (The Property Advisors to the Civil Estate) and British Telecom.

This group first opened the site to visitors in 1993 and, with the help of many volunteers and enthusiasts maintained a collection of independent and Trust exhibitions for the general public to enjoy. HRH The Duke of Kent became Chief Patron, officially opening the Museum in July 1994.

The landowners withdrew all planning applications when the Local Government Inspectorate recommended the historic nature of the site be taken into account in residential planning applications. But in the years that followed, the tortuous battle to save the site nearly foundered on a number of occasions, with hostile bids from property developers an ever-present threat.

In 1998 the Trust began fresh negotiations with the landowners to acquire a substantial part of the site in order to preserve and enhance it for the national good.

On 10th June 1999 the Trust celebrated a deal that secured the future of Bletchley Park. A formula was agreed that gave the Trust an initial 250-year lease on the core historic areas of the site. The Trust will automatically own the land freehold in due course.

In May 2000, the Trust's new strategic plan was approved. Its objective now is to secure a long-term future for Bletchley Park by building on the pioneering work of the codebreakers.

6.5 Milton Keynes Amateur Radio Society

Milton Keynes Amateur Radio Society was formed in 1958. It was originally known as Wolverton & District Radio Society. The society is now based in Bletchley Park where it has been for many years and its members (almost 70) meet weekly.

The Society maintains and runs on a voluntary basis GB2BP radio station located in Bletchley Park. The Society aims to promote and enjoy the hobby of amateur radio through training (intermediate / advanced / Morse) and general information exchange. Training is carried out by volunteer members of the society.

Among their members they have a wealth of knowledge on all aspects of amateur radio including digital modes, television, telephony, Morse code, construction and more.

6.6 British Computer Society

The British Computer Society (BCS), the leading industry body for IT professionals, has close links with Bletchley Park, recently through its generous donation of £75,000 to help secure the future of Colossus in its original location and thereby securing a vital part of our computer heritage.

As well as providing financial support for the project, BCS's Computer Conservation Society led the way with 6,000 volunteered man days in the rebuilding of the fully operational Colossus. BCS's Computer Conservation Society is dedicated to the conservation and restoration of early computers, preserving early computer software and other digital records of historical importance, and to recording the history of computing.

BCS is the Chartered industry body for IT professionals, the Chartered Engineering Institution for Information Technology and a Chartered Science Institution. With its rapidly growing membership in excess of 60,000, BCS is playing an increasingly pivotal role in leading the development and implementation of world class standards for the IT profession through innovative products, services and support.

Through its specific “Professionalism in IT” programme, BCS is leading and building IT professionalism to levels which are currently seen only in traditional long standing professions such as law, medicine, and accountancy, but which will increasingly become the de facto standards for IT professionals.

6.7 Government Communications Headquarters (GCHQ) & German Chancellery/German Defence Ministry

Organising the loan, care and return of such a sensitive piece of equipment as the SZ42 has required agreement at the highest levels within the UK and German defence and intelligence communities. We are particularly grateful that both countries authorities have responded positively and promptly to support this event.

Appendix A Encoding Modes

A.1 SZ42 serial encoding, tri-tone

SZ42 traffic will be transmitted first using the original serial encoding scheme - The International Telegraph Alphabet No.2 (or ITA No.2 for short).

ITA No. 2 is a five bit scheme allowing encoding of 32 different characters. To accommodate all the letters of the alphabet and numerals, two of the 32 combinations [letters] and [figures] are used to select alternate character sets.

	BIT					
LETTERS	**1**	**2**	**3**	**4**	**5**	**FIGURES**
A	M	M	S	S	S	-
B	M	S	S	M	M	?
C	S	M	M	M	S	:
D	M	S	S	M	S	WHO ARE YOU
E	M	S	S	S	S	3
F	M	S	M	M	S	%
G	S	M	S	M	M	@
H	S	S	M	S	M	£
I	S	M	M	S	S	8
J	M	M	S	M	S	BELL
K	M	M	M	M	S	(
L	S	M	S	S	M	)
M	S	S	M	M	M	.
N	S	S	M	M	S	,
O	S	S	S	M	M	9
P	S	M	M	S	M	0
Q	M	M	M	S	M	1
R	S	M	S	M	S	4
S	M	S	M	S	S	.'
T	S	S	S	S	M	5
U	M	M	M	S	S	7
V	S	M	M	M	M	=
W	M	M	S	S	M	2
X	M	S	M	M	M	/
Y	M	S	M	S	M	6
Z	M	S	S	S	M	+
CARRIAGE RETURN	S	S	S	M	S	CARRIAGE RETURN
LINE FEED	S	M	S	S	S	LINE FEED
LETTERS	M	M	M	M	M	LETTERS
FIGURES	M	M	S	M	M	FIGURES
SPACE	S	S	M	S	S	SPACE
ALL SPACE	S	S	S	S	S	ALL SPACE

Table 1 - letter mappings in the original International Telegraph Alphabet No.2

ITA No. 2 is transmitted as (M)arks and (S)paces. Marks are a "1" (a punched hole on paper tape), Spaces are "0" (NO punched hole on paper tape). Each five-bit word is bracketed by a start bit (space) and a stop bit

(mark). Idling is shown by the marking state. Words are transmitted in the bit order shown in Table 1, i.e. bit 1 then 2,3,4,5.

For example, the code letter "A" is sent in serial form as Space, Mark, Mark, Space, Space, Space.

The SZ42 traffic encoded Mark and Space as three simultaneously transmitted tones:

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

The SZ42 machine runs at a speed approximating to between 45 and 50 baud.

A.2 RTTY

Since many Radio Amateurs and Short Wave Listeners will not have the necessary equipment to receive and decode the original SZ42 signals, we shall also transmit the messages in radio teletype (RTTY) mode. We expect there to be a delay of up to 24 hours between the original format transmissions and the RTTY transmissions.

Radio teletype (RTTY) as used in amateur radio generally runs at a baud rate of 45.45 (and sometimes 50) with a Frequency shift of 170Hz. We expect to transmit the ciphertext using audio frequency shift keying (AFSK) with standard frequencies of 2125Hz for mark and 2295Hz for space.

Appendix B Transmission Modes

B.1 HF SSB

We anticipate that the ciphertexts will be transmitted using single sideband suppressed carrier modulation and frequency shift keyed audio tone. This mode is referred to under the Telecommunication Convention as J2B.

B.2 Internet Publication

To encourage worldwide participation in the breaking of the cipher traffic we also plan to publish the challenge ciphertexts on the web. The definitive location for this will be on www.tnmoc.org. We plan to publish the ciphertexts after a 48 hour delay from the original transmissions (although we expect there to be plenty of unofficial posts prior to that time).

Appendix C Transmission Format

C.1 Plaintext (Test) Transmissions

Plaintext test transmissions will allow listeners to calibrate their receiving equipment and filters. The transmission format will comprise three main sections:

C.1.1 Preamble

DE DL0HNF RYRYRYRYRYRYRYRY ...

GB2BP DE DL0HNF TEST TRANSMISSION

(repeat 2 times)

C.1.2 Body

ABCDE FGHIJ KLMNO PQRST UVWXY Z0123 45678 9XXXX

(repeat 10 times)

C.1.3 Close

DE DL0HNF PLS ACK K

C.2 Ciphertext Transmissions

Ciphertext transmissions will be of the same basic format with a preamble to indicate which challenge is being transmitted. The transmission format will comprise three main sections:

C.2.1 Preamble

DE DL0HNF RYRYRYRYRYRYRYRY ...

GB2BP DE DL0HNF CIPHER CHALLENGE 1 [8]

(repeat 2 times)

C.2.2 Body

(Stream of ciphertext)

(repeat 2 times)

[8] 1,2,3 or 4 depending on the challenge being broadcast

C.2.3 Close

DE DL0HNF PLS ACK K

C.3 Transmission Length

Each ciphertext transmission will total approximately 8000 characters and will take in the order of 20 minutes to transmit.

Appendix D Planned Transmission Timetable

We expect to be using the Amateur 20 Metre, 40 Metre and 80 Metre bands for the transmissions.

- The 20 Metre band lies between 14.000 MHz and 14.350 MHz
- The 40 Metre band lies between 7.000 MHz and 7.200 MHz
- The 80 Metre band lies between 3.500 MHz and 3.800 MHz

Each of these bands is split into sections with preferred operating modes. It is impractical to define exactly what frequency within each band will be used during the Cipher Challenge – the spot frequencies in the table below have proven workable during early testing.

There will be a variety of test transmissions between 1 October and the Cipher Challenge on 15/16 November; the following information will be updated as the planned timetable is refined based on those tests.

Date	Time (UTC)	Frequency	Encoding/Mode	Plain/Cipher
15 Nov 2007	09:00	~7.038 MHz	SZ42/J2B	P
15 Nov 2007	10:00	~7.038 MHz	SZ42/J2B	C
15 Nov 2007	11:00	~14.090 Mhz	SZ42/J2B	C
15 Nov 2007	12:00	~14.090 Mhz	SZ42/J2B	C
15 Nov 2007	13:00	~7.038 MHz	SZ42/J2B	C
15 Nov 2007	14:00	~7.038 MHz	SZ42/J2B	C
15 Nov 2007	15:00	~7.038 MHz	SZ42/J2B	C
15 Nov 2007	17:00	~3.590 Mhz	SZ42/J2B	C
15 Nov 2007	19:00	~3.590 Mhz	SZ42/J2B	C
16 Nov 2007	09:00	~7.038 MHz	SZ42/J2B	C
16 Nov 2007	11:00	~14.090 Mhz	SZ42/J2B	C
16 Nov 2007	12:00	~14.090 Mhz	SZ42/J2B	C
16 Nov 2007	13:00	~7.038 MHz	SZ42/J2B	C
16 Nov 2007	14:00	~7.038 MHz	SZ42/J2B	C
16 Nov 2007	15:00	~7.038 MHz	SZ42/J2B	C
16 Nov 2007	17:00	~3.590 Mhz	SZ42/J2B	C
16 Nov 2007	19:00	~3.590 Mhz	SZ42/J2B	C