Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

RECOVERING THE WIRING OF ENIGMA'S UMKEHRWALZE A

Philip Marks [a] & Frode Weierud [b]

[a] 139 Autumn Ridge Road, Bedminster NJ 07921 USA. Email: philmarks@worldnet.att.net.

[b] 4 Le Pre Vert, 1041 Rte de Mategnin, F-01280 Prevessin-Moens FRANCE. Email: Frode.Weierud@cern.ch.

Available online: 04 Jun 2010

To cite this article: Philip Marks & Frode Weierud (2000): RECOVERING THE WIRING OF ENIGMA'S UMKEHRWALZE A, Cryptologia, 24:1, 55-66

To link to this article: http://dx.doi.org/10.1080/0161-110091888781

RECOVERING THE WIRING OF ENIGMA'S UMKEHRWALZE A

Philip Marks[1] and Frode Weierud[2*]

ADDRESS: (1) 139 Autumn Ridge Road, Bedminster NJ 07921 USA. Email: philmarks@worldnet.att.net; (2) 4 Le Pre Vert, 1041 Rte de Mategnin, F-01280 Prevessin-Moens FRANCE. Email: Frode.Weierud@cern.ch.

ABSTRACT: *Umkehrwalze* A was the original reflector used in the version of the Enigma machine employed by the German armed services. Its wiring was originally deduced by the Polish cryptanalyst Marian Rejewski in December 1932 or January 1933, but details of the wiring have not previously been published. Sufficient information to recover the wiring analytically is provided in a wartime document by Alan Turing, and other sources have been found to confirm the solution. This paper presents the wiring, along with alternative methods of recovering it from Turing's data.

KEYWORDS: Enigma, *Umkehrwalze*, reflector, rotor wiring.

INTRODUCTION

Umkehrwalze A was the original reflector issued by the German army in 1930 when it adopted Enigma I, the "steckered" or *Wehrmacht* version of the machine, for widespread use [3, p. 97]. It remained in service until 1937 when it was superseded by *Umkehrwalze* B,[1] which itself remained in service until the end of the European war in 1945. Other reflectors were also introduced from time to time: *Umkehrwalze* C, whose wiring was recovered almost immediately by Hut 6 [12], was introduced briefly and then withdrawn; and the rewirable *Umkehrwalze* D which threatened to become a major problem to the Allies in 1944.[2] The wiring

*This article represents the views of the authors but not necessarily those of their employers or any other third party.

[1]Turing [11, p. 138] gives the date of the change as the summer of 1937. Rejewski [10, p. 264] gives the much more specific date of November 2nd, 1937; since the change invalidated about a year's worth of manual work spent on building a catalog of permutation cycles, he undoubtedly had good reason to remember the date.

[2]For a description of one of the machines developed by the Allies to recover the wiring of the unknown reflectors, see [2].

of *Umkehrwalze* A would have been recovered by Marian Rejewski during his original cryptanalysis of the machine as described in [10].

The authors are not aware of any surviving example of *Umkehrwalze* A, and so have been unable to measure its wiring directly. There is also no published source for this information, even though considerable wiring information has been published for the *Wehrmacht* Enigma and various other versions of the machine (see references [3, 5, and 7]).

In the sections that follow, it is assumed that the reader is familiar with the basic operation of the *Wehrmacht* Enigma. Details can be found in [3].

TURING'S DATA

In Chapter VII of [11], Alan Turing discusses the weaknesses of the original indicating procedure used to inform the intended recipient of the wheel starting positions (the so-called message setting) used to encrypt an Enigma message. This procedure called for the operator to first set the three wheels to a *Grundstellung* (basic setting or ground setting), which was distributed as part of the key for the period in question. The operator then selected three letters at random as the message setting, and encrypted them twice in succession starting at the *Grundstellung*. The resulting six letters formed the message indicator. The operator then set the wheels to the message setting and proceeded to encrypt the text of the message itself. The indicator was transmitted at the head of the ciphertext, and at the receiving end the whole procedure was simply reversed. Indicators of this form were known to Bletchley Park and the American agencies as "throw-on" or, for reasons that will subsequently become clear, as "boxing" indicators.

On page 129 of [11], Turing points out, as Rejewski had previously discovered, that "The weakness of this indicating system is that a great deal of information is given away about the '*Grundstellung*'. If there were no *Stecker* and a known diagonal,[3] and the traffic amounted to 100 messages per diem[4] it would be possible to find the connections of the machine, and if there were *Stecker* but the connections of the machine were known it would be possible to find the keys every day from the same amount of traffic."[5] To illustrate this point, Turing gives

[3] The diagonal is defined as the entry permutation of the machine, i.e., the mapping between the keyboard and the contacts of the entry wheel. For the *Wehrmacht* Enigma, as famously guessed by Rejewski, this is the standard alphabet. That is, the permutation is the identity permutation.

[4] Rejewski [10, p. 274] gives the number of messages needed as about 80 per key period.

[5] The Germans must have been aware of the weakness of this system since they abandoned the use of a fixed *Grundstellung* on September 15th, 1938 [3, p. 99]. The message setting was still doubly enciphered, but now from a starting position chosen supposedly at random by the operator for each message. Though not as weak, the new system still allowed solution by hand methods (for example, using the perforated sheets

the set of indicators shown in Figure 1 as an example of one period's traffic.

UJOOBL	AYIJPI	SMLKFX	CZNYOR	VZPEOW	GIILWI	JSWSAS
VEYITM	UJNOBR	RFXCVJ	RLFCMN	RSICAI	UAMODC	ZDIWXI
ALAJMB	OQBVCY	LGKZRP	LMMZFC	APTJNA	SCQKLE	KPBPNY
XDVBXV	FNXDUJ	BANRDR	MIDHWU	GJWLBS	DLYMMM	FTGDGT
QLYAMM	AFIJVI	GXJLEF	AUXJJJ	CWUYSQ	EYVXPV	HEKUTP
GRYLZM	MIEHWZ	EKXXYJ	UWIOSI	RBDCQU	JNZSUG	UHWOIS
JIPSWW	KMIPFI	TXNGER	FXRDEK	IHVQIV	UANODR	
YEIFTI	NUZIJG	OIKVWP	EYYXPM	OQFVCN	HALUDX	
BMARFB	IIFQWN	TIOGWL	ZCDWLU	RZHCOO	UOGOHT	
TZNGOR	KGAPRB	LNVZUV	EZSXOH	AVRJKK	ZFUWVQ	

Figure 1. Sample Message Indicators.[6]

From this information, the permutations linking the first and fourth letters, the second and fifth, and the third and sixth can be written down as shown in Figure 2 (where '.' indicates a letter is missing from the sample of data).

For future reference, let us call these permutations T, U, and V respectively. They can alternatively be written down as cycles:[7]

```
T:  ...NIQAJSKP...TGLZW... (DMHUOVEXBRCYF)
U:  (PNUJBQCLMFVKY)(OHIWSADXETGRZ)
V:  (V)(I)(JFNRKPWSHOLX) ...DUQEZGTABYMC...
```

The ellipses indicate where the cycles cannot be directly completed due to missing data. However, Turing points out that there is no doubt about how permutation V must be completed – only letter D is missing and the parentheses can be placed around the second group of letters. At first glance, permutation T could be completed in two ways, but since it must consist of pairs of cycles of equal length [11], and we already have one cycle of length 13, the two partial cycles NIQAJSKP and TGLZW can simply be concatenated to form a second cycle of length 13. This can be done in two ways, but they are equivalent to one another, and we can deduce that PT and WN are the missing pairs.

described in [12]), and the traffic was compromised still further by bad operator habits in choosing "guessable" starting positions. In May, 1940, most German networks abandoned double encipherment altogether [1], but astonishingly its use was reinstated in 1941 on some naval networks [4, 9], and also continued in a somewhat different form, but with similarly disastrous results, on some *Abwehr* networks.

[6]The indicator data reproduced here is taken directly from Turing's original document. However, the authors believe that the original contains a typographical error in one of the indicators: VEYITM (second indicator, first column). This value is not consistent with the cycle data that follows; the correct value should be either NEYITM or VEYETM.

[7]For details of this operation, see Rejewski [10, pp. 251–252] or Deavours and Kruh [3, pp. 106–108].

The lengths of these cycles are very characteristic of the position of the wiring of the three Enigma wheels at the *Grundstellung*, and the original Polish method of attack on each new key was to prepare a catalog of cycle lengths and the *Grundstellungen* that could produce them. Turing does this hard work for us, stating that the relevant wheel order is I, II, III (*Wehrmacht* Enigma, *Umkehrwalze* A), with *Grundstellung* 1, 1, 26. This last information must be interpreted as meaning window positions AAZ, with the rings set in the neutral position of AAA. Thus, since the Enigma machine steps when a key is pressed, with encoding taking place at the bottom of the keystroke, the first letter of each indicator is enciphered with the wheels in position AAA. Furthermore, since wheel III only steps the wheel to its left when the letter visible through its window advances from V to W, no middle wheel turnover will occur during the encipherment of the 6 characters of each indicator.

AJ	AD	AB
BR	BQ	BY
CY	CL	C.
DM	DX	DU
EX	ET	EZ
FD	FV	FN
GL	GR	GT
HU	HI	HO
IQ	IW	II
JS	JB	JF
KP	KY	KP
LZ	LM	LX
MH	MF	MC
NI	NU	NR
OV	OH	OL
P.	PN	PW
QA	QC	QE
RC	RZ	RK
SK	SA	SH
TG	TG	TA
UO	UJ	UQ
VE	VK	VV
W.	WS	WS
XB	XE	XJ
YF	YP	YM
ZW	ZO	ZG

Figure 2. Permutations Linking Indicator Letters 1&4, 2&5, and 3&6.

Turing next deduces the *Steckers* that were used. From the catalog, he gives the boxes for the (unsteckered) equivalents of permutations T, U, and V as shown

in Figure 3 (where the underlining indicates the end of a compartment within a box).

DT	PZ	CE
MG	RN	TQ
HL	UG	XU
UP	JL	JD
CK	BE	FO
AI	QX	RM
EJ	OD	NY
XV	TV	KB
BQ	MI	PV
NS	FW	WL
OR	AS	IG
YW	KH	HZ
FZ	YC	AS

Figure 3. Boxes for the Unsteckered Permutations 1&4, 2&5, 3&6.

"Boxing" is another way of representing the product of two permutations,[8] and is discussed at length in Chapter III of [11]. The pairs of equal-length cycles into which the product decomposes form the left-hand and right-hand columns of each compartment of the box. The cycles from these compartments must map into the cycles we have derived from the indicators via permutations T, U, and V, with any changes in letters due to the effect of the *Steckers*. Starting with the short compartment AS from the last permutation, the letters A and S must map to the cycles (V) and (I) from permutation V. Thus, either V is steckered to A and I to S, or V is steckered to I and A to S. Looking at the number of common letters and subsequences between the column ZNGLEXDVIWSHC of the middle permutation, and the cycle OHIWSADXETGRZ from permutation U, we can readily map these to one another as follows provided that V is steckered to A:[9]

```
(OHIWSADXETGRZ)
(CHSWIVDXELGNZ)
```

At the time this indicating system was in force, the German army used relatively few *Steckers*, not more than 6 in a key. Thus the presence of so many

[8] For boxing to be a meaningful operation, the permutations must be involutions; i.e., composed solely of transcriptions of pairs of characters. Due to the presence of the reflector, the permutation of the alphabet produced by the Enigma with the wheels set at any given position is always an involution. This was an operational convenience, since it made enciphering and deciphering into the same operation, but a cryptologic disaster.

[9] The order of letters in a cycle is significant, but the choice of starting letter is not. Rotations of the same set of letters yield cycles that are equivalent. Likewise, the pairs in a box compartment may be rotated in sequence, and for matching purposes the entire compartment may be reflected about its horizontal and vertical axes. For example, the middle permutation in Figure 3 can be regarded as beginning: CY, HK, SA, ..., and indeed this is necessary to permit the matching described in the text.

unchanged letters between these two cycles, along with the repeated substitution I/S and S/I, is a good confirmation that the cycles have been correctly matched. We can immediately deduce additional *Steckers*: O/C, T/L, and R/N. Matching the remainder of the cycles from the boxes and from permutations T, U, and V shows that these are the only *Steckers* for the key in question.

Turing goes on to discuss alternative methods of recovering keys from the message indicators, as well as the much stronger indicating system introduced by the German navy, but in this paper we are interested in determining the wiring of *Umkehrwalze* A.

RECOVERING THE UMKEHRWALZE WIRING

If we focus on permutation T, the mapping between the permutations produced by the first and fourth positions of the wheels following the *Grundstellung*, and the corresponding box in the first column of Figure 3, we find that the rows of this box are in fact the permutation produced by the (unsteckered) Enigma when enciphering the first letter of each indicator. The order of the rows is determined by the permutation produced when enciphering the fourth letter. This follows directly from the method of constructing the boxes. To illustrate, the first three rows of the first box are DT, MG, HL, which implies that the permutation produced at position four contains the pairs TM (linking rows 1 and 2), and GH (linking rows 2 and 3).

Let us define as permutation A the "inwards" permutation produced by the three wheels I, II, III at positions AAA (i.e., the positions used to encode the first letter of each indicator). By "inwards", we mean the combined effect of the wheels as the electrical input from the entry wheel traverses them in the direction towards the *Umkehrwalze*. Similarly, let us define permutations B, C, D, E and F as the successive inwards permutations produced by the three wheels at the positions at which the 2nd, 3rd, 4th, 5th, and 6th letters of the indicators are enciphered.

If we define the permutation produced by the *Umkehrwalze* itself as R, then the permutation produced by the (unsteckered) Enigma when in the position for enciphering the first indicator letter is:[10]

$$A^{-1}RA$$

And this must be the same as the permutation given by the rows of the first column of Figure 3. Since we know the wiring and positions of wheels I, II, III,

[10] This formula, and others given later, follow the normal mathematical convention in that they are intended to be read from right to left. In this case, permutation A is applied first, then permutation R, then permutation A^{-1}.

permutation A is known,[11] and we can readily obtain the value of permutation R, i.e., the wiring of *Umkehrwalze* A:

(AE) (BJ) (CM) (DZ) (FL) (GY) (HX) (IV) (KW) (NR) (OQ) (PU) (ST)

We can cross-check this result by following the same process using permutation B and the second column of Figure 3.

We could also take a somewhat more laborious approach to recovering the wiring that does not rely on the properties of boxes. If we define the *Stecker* permutation as S, we can write down the following equation for the relationship between the first and fourth letters of the indicators:

$$TS^{-1}A^{-1}RAS = S^{-1}D^{-1}RDS$$

Eliminating S from both sides, and multiplying on the right by D^{-1} we get:

$$TS^{-1}A^{-1}RAD^{-1} = S^{-1}D^{-1}R$$

Then multiplying on the left by DS and rearranging we get:

$$R = DSTS^{-1}A^{-1}RAD^{-1}$$

All of the permutations of this equation except R are known. Similar equations can be derived that relate R to permutations B, E, and U, and also to permutations C, F, and V. To make the remaining explanation easier to follow, the permutations corresponding to the subexpressions $DSTS^{-1}A^{-1}$ and AD^{-1} are shown expanded in Figure 4, which once again is intended to be read from right to left.

This is an equation in a single unknown, and a solution would permute the rows of the two columns to align them in such a way that each combined row would read across in a way consistent with all of the others. Suppose, for example, that the first row, ZA and GA had been correctly aligned. This would mean that the input letter to the right hand side of the transposition implied by the combined row, A, would map to the letter Z on the output side. But note that this would imply that the inner letters, A and G, would also have to map to one another under permutation R. This is clearly a contradiction, therefore the two partial rows are not correctly aligned. An alignment of any two partial rows, say CS and VR, is in effect a pair of hypotheses about letters that map to one another under permutation R, and each hypothesis implies the other. In this case, the two hypotheses would be C/R and S/V.

[11] It maps the standard alphabet into: ZNVAKQFMDWICLPYSRGUETBHJXO

		ZA		GA
		GB		KB
		XC		CC
		TD		ED
		FE		XE
		DF		OF
		KG		WG
		AH		MH
		NI		RI
		UJ		DJ
		YK		UK
		HL		AL
		MM		TM
R	=	VN	**R**	SN
		QO		QO
		WP		BP
		LQ		HQ
		PR		VR
		CS		ZS
		RT		IT
		IU		NU
		SV		PV
		JW		YW
		OX		FX
		EY		JY
		BZ		LZ

Figure 4. Permutation Equation for R.

Thus, given any starting hypothesis, we can quickly make from it chains of deductions which will lead to confirmations or contradictions. Since each inferred pair of letters from permutation R produces up to three further deductions (other partial rows can be aligned using either their "inside" pairs or their "outside" pairs), inferences propagate very rapidly and the starting hypothesis can quickly be tested.

We also have some very good choices for starting hypotheses. The right-hand column of Figure 4 contains the pair CC. This can only be aligned with another row that contains a repeated letter, since alignment with any other kind of row provides an immediate contradiction – C would have to be mapped to two different letters under permutation R. There is only one pair in the left hand column of Figure 4 that fits the bill: MM. Now we have a good starting hypothesis, and the inferred pair CM can immediately be used to align other partial rows: XC with MH, and CS with TM. This yields two new inferences for permutation R: X/H and S/T, and the solution proceeds rapidly, yielding the

same value for permutation R that we derived more directly by working from the boxes in Figure 3. When we arrive at a confirmation, i.e., we derive an inference that agrees with one of our earlier deductions, that particular chain of hypotheses can be taken no further. But due to the rapid rate at which inferences multiply, we will usually have plenty of as-yet-unexplored inferences to follow and we are unlikely to get stuck. Even if we did, we can take hypotheses derived from this equation and start other chains using the companion equations:

$$R = ESUS^{-1}B^{-1}RBE^{-1} \text{ and } R = FSVS^{-1}C^{-1}RCF^{-1}$$

In the general case, we might not have such a good starting hypothesis available to us, but other options are available. For example, if we write out the details of the equation resulting from the third and sixth indicator letters, $R = FSVS^{-1}C^{-1}RCF^{-1}$, we find the following sets of partial rows already aligned: LF LF; and VI VI. These are obviously consistent and form good starting points, but such configurations are not infallible. We find a similar situation from the remaining equation (second and fifth indicator letters): YE YE and AG AG. In this case, the pairings as found are incorrect and will quickly lead to a contradiction, but the alternative arrangement YE AG is obviously the next hypothesis to try and leads to the correct solution. If all else fails, even an exhaustive approach of picking a partial row and aligning with each of the possible alternatives in turn would not take long to yield the right result.

CONFIRMING THE SOLUTION

The value of permutation R that we have derived is fully consistent with Turing's data, but that is not an absolute guarantee that it truly represents *Umkehrwalze* A. Turing might, as elsewhere in [11], have simply constructed some self-consistent data for illustrative purposes. However, at the end of Chapter III of [11], Turing discusses the identification of wheels by their "class", which is a kind of signature derived from the cycle lengths of various permutations they produce. This is discussed at greater length in [7]. The class is an absolute property of the wiring pattern of a wheel and has the advantage of being invariant across the various orientations of the wheel that might be encountered in actual use; it is expressed as a series of numbers that add up to 26, by convention in descending order. Turing lists the classes of various wheels that had been identified as of the date of the document, including *Umkehrwalzen* A, B, and C. Unfortunately, the extant copy of [11] in the U. S. National Archives (NARA) is of very poor quality in places, and the classes are barely readable. We can state the following about the class of *Umkehrwalze* A with reasonable confidence: it consists of six

single-digit numbers; the third number is 4; the last number is 1; the fourth number is neither 4 nor 3; and the fifth number is not 1. The second number might be 8. Since the numbers are listed in descending order, the end of the sequence must be 4, 2, 2, 1, and since these total 9, the first two numbers must add to 17. The only combination of two single-digit numbers that adds to 17 is 8 and 9. So it appears that the class of *Umkehrwalze* A is 9, 8, 4, 2, 2, 1.

We take the class of an *Umkehrwalze* by setting out the permutation in full, and then deriving another permutation from the first by replacing each letter with the one preceding it in the alphabet.[12] We then compute the cycles of the result. For our derived solution, we set out the following permutations:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
EJMZALYXVBWFCRQUONTSPIKHGD
DILYZKXWUAVEBQPTNMSROHJGFC
```

From the first and third rows we derive the following cycles:

```
(ADYFKVHWJ)(BIUOPTRM)(CLEZ)(GX)(NQ)(S)
```

The lengths of these cycles agree with Turing's class data and provide additional confidence that the correct wiring for *Umkehrwalze* A has been identified.

Since the authors originally recovered the wiring using the methods described in the preceding sections, further confirmation that it is in fact correct has been obtained from two independent sources. The first is a report dated April 10th, 1944, sent to his commanding officer at Arlington Hall by Captain Fried of the US Signals Security Agency, stationed at the time at Bletchley Park [6]. At the time, Hut 6 was wrestling with the problems presented by the varying wirings encountered for *Umkehrwalze* D, and in the process of trying to determine its exact physical nature (and therefore its capabilities) had analyzed the wirings encountered to date, comparing them with each other and with those of the previously encountered versions A, B, and C. The report contains a table of intervals between the letters forming the 13 pairings of each reflector. Those given for *Umkehrwalze* A can be seen to correspond to the wiring given above: 1 pairing at each of the distances 1, 2, 5, 6, 12, and 13; two pairings at each of the distances 8 and 10; and three pairings at distance 4. The second source can be regarded as definitive: a handwritten document from the Bletchley Park archives found among papers attributed to Oliver H. Lawn, a member of the technical committee set up in 1944 to investigate *Umkehrwalze* D [8]. This gives the wiring of *Umkehrwalze* A as: 1/5, 2/10, 3/13, 4/26, 6/12, 7/25, 8/24, 9/22,

[12] More strictly, we take the letter preceding in the sequence of the diagonal, i.e., the entry permutation. But for the *Wehrmacht* Enigma the entry permutation is the standard alphabet.

11/23, 14/18, 15/17, 16/21, 19/20, which again can be seen to correspond with the solution given above.

ACKNOWLEDGMENTS

The authors thank Ralph Erskine, David Hamer, and Geoff Sullivan for their careful proofreading of this paper and for the various improvements they have suggested. David Hamer's help was decisive in providing the conclusive proof of the correctness of the solution.

REFERENCES

1. Bloch, Gilbert and Ralph Erskine. 1986. Enigma: The Dropping of the Double Encipherment. *Cryptologia* 10(3):134–141, reprinted in *Cryptology Yesterday, Today, and Tomorrow*, Cipher A. Deavours, David Kahn, Louis Kruh, Greg Mellen, Brian Winkel editors, Artech House, 1987.

2. Deavours, Cipher A. 1995. The Autoscritcher. *Cryptologia.* 19(2): 137–148.

3. Deavours, Cipher A. and Louis Kruh. 1985. *Machine Cryptography and Modern Cryptanalysis.* Norwood, MA: Artech House. See Chapter III.

4. Erskine, Ralph. 1996. Naval Enigma: An Astonishing Blunder. *Intelligence and National Security*, 11(3): 468–473.

5. Erskine, Ralph and Frode Weierud. 1987. Naval Enigma: M4 and Its Rotors. *Cryptologia.* 11(4): 235–244.

6. Fried, Walter J. 1944. *Fried Report #F19.* NARA College Park, Maryland, Record Group 457, Historic Cryptographic Collection, Box 880, NR 2612.

7. Hamer, David H., Geoff Sullivan, and Frode Weierud. 1998. Enigma Variations: An Extended Family of Machines. *Cryptologia.* 22(3): 211–229.

8. Hamer, David. 1999. Personal communication. The Lawn memorandum is dated May 9th, 1942, and contains wiring information for *Umkehrwalze* A and for the other two reflectors known to Bletchley Park at that time: *Umkehrwalzen* B and C. Information has been added to the original that differs in both handwriting and ink color; it lists the first wiring encountered for *Umkehrwalze* D and therefore cannot have been appended earlier than January, 1944.

9. Mahon, A. P. 1945. *The History of Hut Eight 1939 - 1945.* NARA College Park, Maryland, Record Group 457, Historic Cryptographic Collection, Box 1424, NR 4685, Chapters VI, X, and XI.

10. Rejewski, Marian. 1980. How the Polish Mathematicians Broke Enigma. Reprinted as Appendix D in: *Enigma.* Wladyslaw Kozaczuk. 1984. University Publications of America.

11. Turing, Alan M. 1940. *Turing's Treatise on Enigma.* NARA College Park, Maryland, Record Group 457, Historic Cryptographic Collection, Box 201, NR 964. This document is being edited by Frode Weierud, Ralph Erskine, and Philip Marks for publication on Frode Weierud's website. Several chapters have been published already, and the relevant URL is:
http://home.cern.ch/~frode/crypto/

12. Welchman, Gordon. 1982. *The Hut Six Story: Breaking the Enigma Codes.* Allen Lane (also published in the USA by McGraw Hill, and reprinted in 1997 by M & M Baldwin, Kidderminster, UK). Chapter 6.

BIOGRAPHICAL SKETCHES

Philip Marks is employed by AT&T in New Jersey where he works on financial computer systems. He has been following the Bletchley Park story since 1974 and is interested in computer simulations of the cryptanalytical methods and machines used by the British and American signals intelligence agencies during the Second World War.

Frode Weierud is employed by the European Organization for Particle Physics (CERN) in Geneva. He works as a programmer in one of the equipment groups. Cryptography has been his main interest for more than 30 years. His cryptological research is focused on cipher machines and cryptanalytical techniques.