History and Modern Cryptanalysis of Enigma's Pluggable Reflector

Olaf Ostwald and Frode Weierud

ABSTRACT: The development history of *Umkehrwalze Dora* (UKWD), Enigma's pluggable reflector, is presented from the first ideas in the mid-1920s to the last development plans and its actual usage in 1945. An Enigma message in three parts, enciphered with UKWD and intercepted by the British on 11 March 1945, is shown. The successful recovery of the key of this message is described. Modern computer-based cryptanalysis is used to recover the wiring of the unknown "Uncle Dick," which the British called this field-rewirable reflector. The attack is based on the known ciphertext and plaintext pair from the first part of the intercept. After recovery of the unknown reflector wiring and the daily key the plaintext of the second part of the message is revealed.

KEYWORDS: Enigma, cryptanalysis, Uncle Dick, *Umkehrwalze Dora*, UKWD, unsolved ciphers

Address correspondence to Frode Weierud, Bjerkealleen 17, 1385 Asker, Norway. Email: frode.weierud@gmail.com

1. Introduction

Uncle Dick,[1] as it was called by the codebreakers of Bletchley Park (BP), or *Umkehrwalze Dora* (UKWD), as designated by the Germans, was the nickname of a special pluggable reflector,[2] used as the leftmost wheel within the scrambler[3] of the Enigma.

The electro-mechanical cipher machine Enigma (from Greek αίνιγμα for "riddle") was the backbone of the German *Wehrmacht* during World War II. Arthur Scherbius, a German promoted electrical engineer and inventor of considerable standing, invented Enigma in 1918 [14]. Subsequently it was improved and then used by all three parts of the German armed forces, namely army (*Heer*), air force (*Luftwaffe*), and military navy (*Kriegsmarine*), for enciphering and deciphering of their secret messages. Figure 1 shows the principle of the machine and its four main elements. It is operated similarly to a typewriter, entering the plaintext via the keyboard. Each letter of the plaintext is enciphered individually [8]. By pressing a letter key a switch is closed and current from an internal battery flows over the closed contact through the plugboard (*Steckerbrett*) into the rotor set, where the letter is permutated several times by three rotating wheels. The current reaches the UKW, which is situated at the leftmost side of the rotor set, and functions like a reflector. It feeds the current back through the three rotating wheels of the rotor set and the plugboard. Finally the current reaches the lampboard and lights up a lamp. The illuminated lamp is the corresponding cipher letter of the plaintext letter. Similarly, as used for enciphering, Enigma can also be used for deciphering. For that, the ciphertext is simply entered via the keyboard, and the lamps now indicate the corresponding plaintext [7].

[1] It was also called Uncle Dora, Uncle D or simply UD.

[2] Also known a "reversal wheel", *Umkehrwalze* in German, and abbreviated UKW.

[3] Other expressions used for the scrambler are rotor set or wheel maze.

Postprint: The Version of Record of this manuscript has been published and is available in Cryptologia, January 2016, http://dx.doi.org/10.1080/01611194.2015.1028682

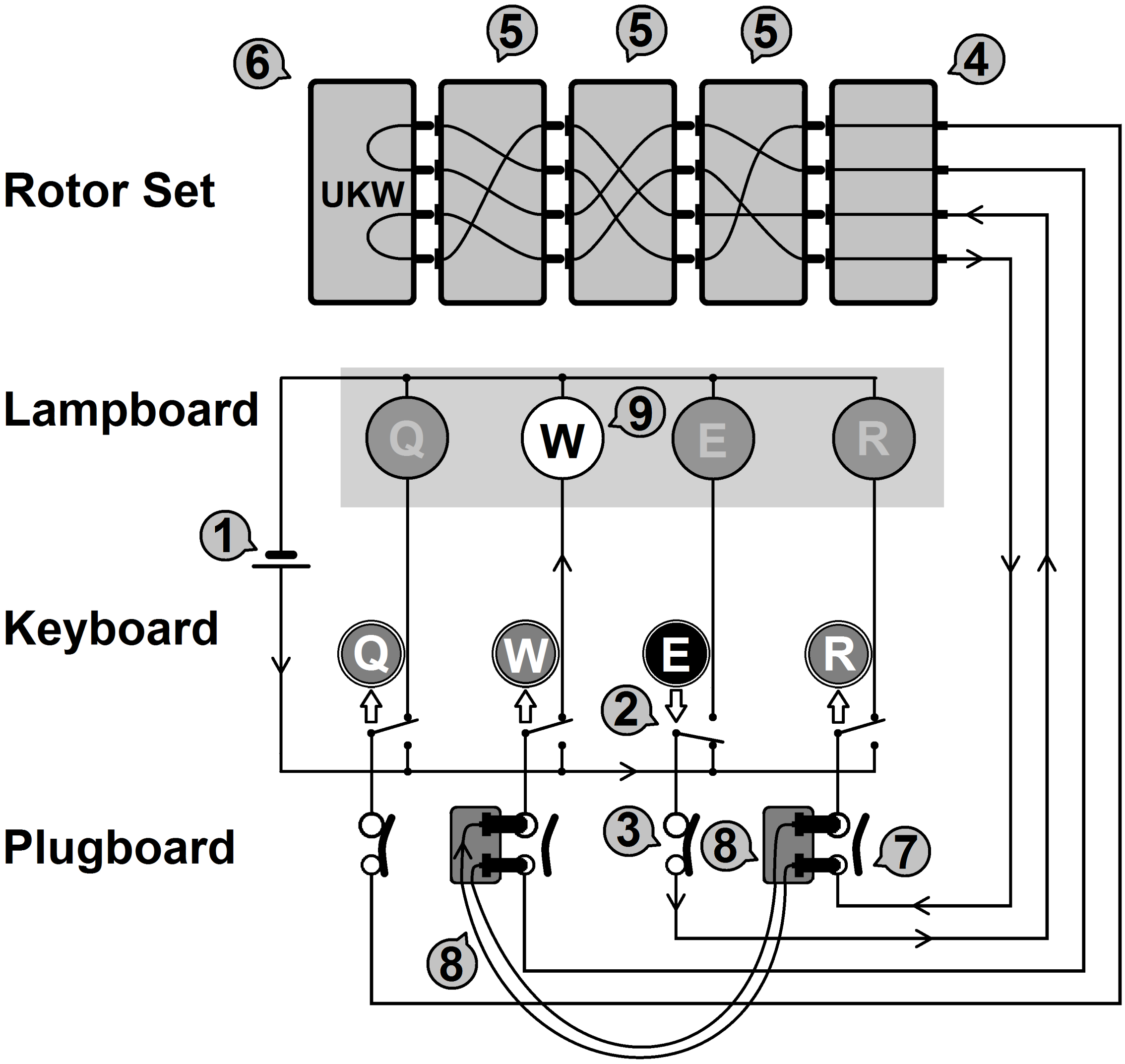


Figure 1. The current from the battery (1) flows through the pressed key (2) (here E) and the plugboard (3) via the entry wheel (4) (*Eintrittswalze* in German) through the three rotating wheels (5) of the Enigma to the *Umkehrwalze* (6) and is fed back again through the three rotating wheels, the *Eintrittswalze*, and the plugboard (7) with a *steckered* cable (8) and lights up a lamp (9) (e.g. W). Here, for simplicity, only four letters are shown instead of the actual 26. Source: Redrawn figure based on an illustration by Dirk Rijmenants.

2. The Beginning

The introduction of UKWD on the German Air Force (GAF) Enigma cipher networks in 1944 and the problems this caused for both the German cipher operators and for Allied codebreaking operations have been well explained by Philip Marks in his extensive *Cryptologia* article "*Umkehrwalze D*: Enigma's Rewirable Reflector" [10, 11, 12]. What is less known is the history about the German development of UKWD.[4] Contrary to what one would believe the pluggable reflector was not a wartime German invention. *Chiffriermaschinen Aktiengesellschaft* (ChiMaAG) had invented the concept of pluggable variations to the Enigma as early as 1926 and on 9 August 1926 it applied for a patent. The idea was to introduce elements that could easily be changed by plug connections either before or in the rotor system, thus covering all future developments such as

[4] The documents referred to in this section are part of the TICOM (Target Intelligence Committee) collections T 1715, T1716, T1717, and T1718 containing original documents from ChiMaAG and *Chiffriermaschinen Gesellschaft Heimsoeth und Rinke* (H&R). The collections are in the *Politisches Archiv des Auswärtigen Amts (PAAA), Berlin* [21].

the *Steckerbrett* (plugboard) and the pluggable UKW. This was to make the machine more variable and secure so that the possession of the wheel wirings alone would not allow the messages to be read.

The original patent application of 9 August 1926 is no longer to be found[5] but the original idea is explained in German patent no. 554421 published on 23 June 1932 with the title *"Elektrische Chiffriervorrichtung"* (Electrical cipher device) [15]. The patent describes one or two fixed stators situated in between the moveable rotors. A stator would take the form of two disks with contacts facing the movable rotors. On the inner sides of the disks the contacts would be equipped with short leads with plugs to allow for any contact on one disk to be connected to any other contact on the other disk. The patent became valid in Germany on 31 January 1928, 18 months after the original application, but now the plug connections outside the wheel system are no longer mentioned. This indicates that several changes were made to the original application.

The reason for these changes can be found in the discussions ChiMaAG had with the *Reichswehr* (RW) about the *Steckerbrett* for the new Enigma machines ordered by them. On 28 March 1927 a first secret and preliminary agreement about the new Enigma with plugboard was signed by director Bruno Weigandt for ChiMaAG, and *Regierungsrat* (senior civil servant) Wilhelm Fenner and First Lieutenant Walter Seifert for RW. This was changed into a formal secret contract between ChiMaAG and RW on 2 May 1927. The contract was signed by Weigandt for ChiMaAG and Lieutenant Colonel Karl von Roques as Chief of Staff for RW and countersigned by Major Rudolf Schmidt, the brother of the spy Hans Thilo Schmidt,[6] as chief of the *Reichswehr Chiffrierstelle* (Cipher Office).

However, Weigandt made a serious error when he signed these documents, especially the last formal contract. It states that the connections from the entry wheel (*Eintrittswalze*), here called *Abgreifer* (collector), will be transferred to a special switchboard (*Schaltbrett*) where all possible connections can be made, and that this device will be regarded as the property of the Army Administration (*Heeresverwaltung*). It also states that this device must only be used on Enigma machines delivered to the RW and that the alteration must be kept secret. It is not clear whether Weigandt informed RW about the patent application of 9 August 1926, however the patent is not mentioned in any of the official documents. Patent no. 554421 does not explicitly mention the *Steckerbrett* but it does promote the idea of using plug devices to easily change the cryptologic circuitry. However, the final patent no longer contains all the ideas in the original application because RW asked ChiMaAG either to completely withdraw its application or have it modified.

During two meetings to discuss technical details about the new Enigma with *Steckerbrett* (Figure 2), which took place on 14 and 17 February 1928, it became clear that ChiMaAG was not at all satisfied with the May 1927 agreement. The more technically oriented people of ChiMaAG, Dr. Arthur Scherbius and his chief engineer Willi Korn, stated that the original patent of August 1926 also covered the idea of the proposed *Steckerbrett.* They claimed that the patent in reality covered any modification to the cipher circuitry by variable plug connections. The *Reichswehr* on the other side did not agree.

The dispute continued and on 1 March 1928 a meeting took place in the *Reichswehrministerium* between Fenner, Seifert and Major Schröder from RW and Mrs Elsbeth Rinke, Scherbius and Korn representing ChiMaAG. The RW people expressed the opinion that Weigandt should either not have signed the contract of May 1927 or he should have dropped the patent application of 9 August 1926. In the end ChiMaAG expressed willingness to either remove and withdraw claims two and four of the patent application, or agree to these changes being part of a secret patent application. It is possible Weigandt's conduct of the RW contract sealed his fate of a future at ChiMaAG, because on 8 March 1928 he suddenly left his position as director.

[5] Many original German patent documents, including all secret patents, were destroyed in a fire started by Regierungsrat Franke on 30 March 1945 in an underground patent storage facility at Heringen in Hessen. Already in February 1945, when the building of the Reichspatentamt in Berlin-Kreuzberg was bombed, many documents were destroyed [9].

[6] For information about Hans Thilo Schmidt see Hugh Sebag-Montefiore [19].

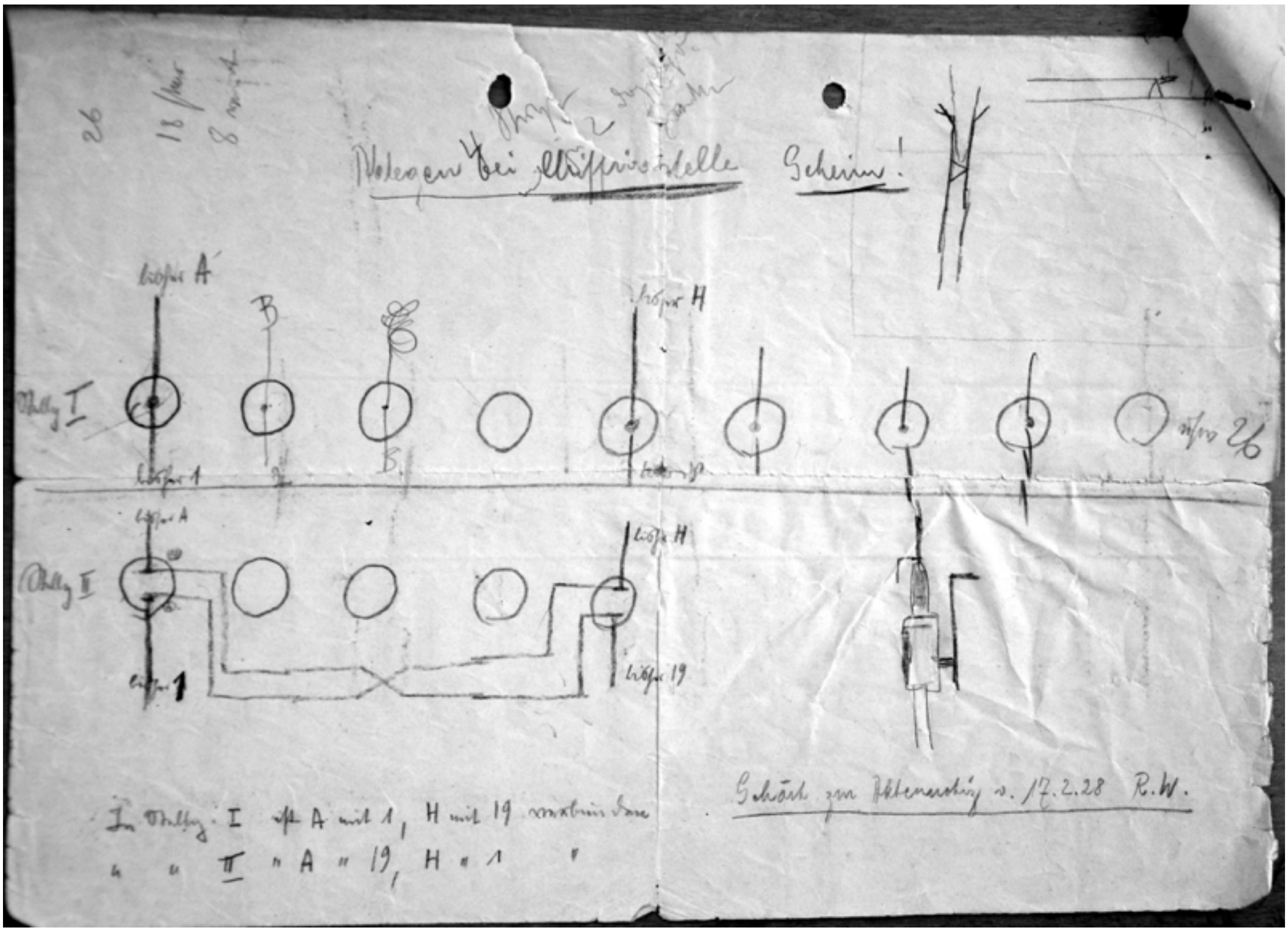

Ablegen bei Chiffrierstelle
Geheim!
Stöpsel A
B
Stöpsel H
Stellg I
Stöpsel 1
Stöpsel 19
Stellg II
Nr 26
In Stellg. I ist A mit 1, H mit 19 verbunden
" " II " A " 19, H " 1 "
Gehört zur Unterredung v. 17.2.28 R.W.

Figure 2. Authentic freehand sketch of a plug device as proposed during the meeting of 17 February 1928. The handwritten scribbles say: "To be filed at Cipher Office, Secret! In position 1, A is connected to 1 and H to 19; in position 2, A is connected to 19 and H to 1. Belongs to memo of 17.2.28 R.W." (*Source*: PAAA, Berlin; archive signature: T1718.)

On 30 March 1928 a new meeting took place between Rinke and Korn from ChiMaAG and Seifert, Fenner and Schröder from RW. The latter now made it clear that the fourth patent claim not only possibly but definitely had to be removed. However, they agreed using of plug connections to other parts of the Enigma machine apart from the *Eintrittswalze* did not break the May 1927 agreement.

On 9 March 1929 Korn composes a handwritten memorandum of a discussion he had with Scherbius the day before. The memo says that Scherbius and Korn have the opinion that their idea of a pluggable UKW using single ended plugs has nothing common with the double-poled *Steckerbrett* plugs suggested by RW. If the idea of a pluggable UKW was included in the original patent application of 9 August 1926 we do not know, but at least the idea existed in March 1929 and the idea was the creation of Scherbius and Korn.

Finally the story about pluggable variations to the Enigma and the patent conflict between ChiMaAG and RW comes to an end. In a letter dated 8 May 1929 RW informs ChiMaAG of the conditions pertaining to a secret patent that ChiMaAG has transferred to RW. It concerns the secret patent application C 38582 IX/42n of 9 August 1928 entitled *"Schaltanordnung für elektrische Leitungen von Chiffriervorrichtungen"* (Connection arrangement for electrical wires of cipher devices). This is the patent for the famous Enigma plugboard (*Steckerbrett*).

On 6 August 1929 the idea of a pluggable UKW pops up again. In a meeting between Fenner and Seifert from RW and Rinke and Korn from ChiMaAG to discuss technical details about the *Steckerbrett* production, ChiMaAG mentions its intention to use pluggable UKWs on its commercial machines. It explains that the pluggable UKW is both cryptographically and operationally a good solution and that it has already offered such an implementation to Hungary.

Fenner seems slightly upset about not having been informed about such a possibility earlier, but he explains that for legal reasons RW is not interested in such a solution. As the ChiMaAG memorandum says: "The gentlemen of the cipher office explicitly underlined that our proposal (tapping of the reflector)[7] is of no interest for them."

Seen in light of the Wehrmacht's adoption of the same device twelve years later it is of interest to look closer at what this implies. The RW's lack of interest seems to indicate that Fenner and his people had insufficient knowledge about the Enigma and machine ciphers to fully judge the cryptological strengths of the two solutions, the *Steckerbrett* and the pluggable UKW. Their legal reasoning is perhaps somewhat surprising but it is based on the fact that the contract between ChiMaAG and RW only covers the *Steckerbrett*. It is only this device that is secret and hence covered by the German laws about treason. If RW had chosen to adopt the pluggable UKW it would have had to renegotiate the original agreement. This is something it probably did not wish to do knowing ChiMaAG's growing reticence towards the Weigandt agreement. When ChiMaAG furthermore stressed that it would not protect [by patent] its new plug device, for instance for the Hungarians, the RW was possibly mollified.

However, something must nevertheless have happened, because we know from the inspection and study of one of the Hungarian machines, G 111, that the machines were not equipped with a pluggable UKW [16]. Neither have any other commercial Enigma machines equipped with pluggable UKWs ever been found, apart from Enigma KD that the *Militärisches Amt*, the successor to the *Abwehr*, started to use from the end of 1944.[8] Only a handwritten note written by Korn in July 1936 refers to something that might have been a commercial machine with a pluggable reflector. A variation of the Enigma G, Ch. 15 c, is described as having a fixed UKW and a *Steckerbrett*. Because the *Steckerbrett* connected to the entry wheel was a secret item only allowed for sale to the RW it is possible that we here have a *Steckerbrett* connected to the fixed UKW. Unfortunately no other information about Ch. 15 c has been found so far. Nor do we know why ChiMaAG dropped the pluggable UKW. Did RW force ChiMaAG to reconsider or was it simply that the Hungarians did not like the new device?

3. UKWD Takes Shape

Although we know that a pluggable UKW was invented in the 1920s and proposed to the Hungarians, it is not known when it was decided to equip the Wehrmacht Enigma machines with such a device. However, it seems most likely the decision was taken in early 1940. Engineering drawings of the UKWD all show a creation date in June 1940. Figure 3 shows one such drawing, number 24b D 65633 entitled *Stöpselbare Umkehrwalze D* (pluggable reflector D), was created on 18 June 1940 and later amended on 10 March and 8 August 1941.

On 13 January 1941 *Chiffriermaschinen Gesellschaft Heimsoeth und Rinke* (H&R) sends a letter to *OKH, Chef H Rüst u. BdE, Wa J Rü (WuG 7, VI a4)* concerning drawing modifications for the cipher machine Enigma and UKW according to the *Waffenamt* drawings 24 b 656.[9] Here H&R refers to discussions it had with Dr. Pupp and Ing. Hesse of *Wa Prüf 7/IV* on 7 and 16 October 1940 and 2 December 1940. This seems to agree well with the idea that UKWD was constructed in 1940 and prepared for production in 1941.

[7] The German expression is *Anzapfung Umkehrwalze*, which refers to connecting plugs to the UKW's internal wiring.

[8] The *Abwehr* was the German military intelligence service under the command of Admiral Wilhelm Canaris and the *Militärisches Amt* was the office within *SD-Ausland*, the foreign security service belonging to Himmler's *Reichssicherheitshauptamt* (RSHA), that took over some of the functions of the *Abwehr* after the 20 July plot in 1944.

[9] *Waffenamt* (WaA) was the German Army Weapons Agency responsible for research and development of the army's weapons and equipment.

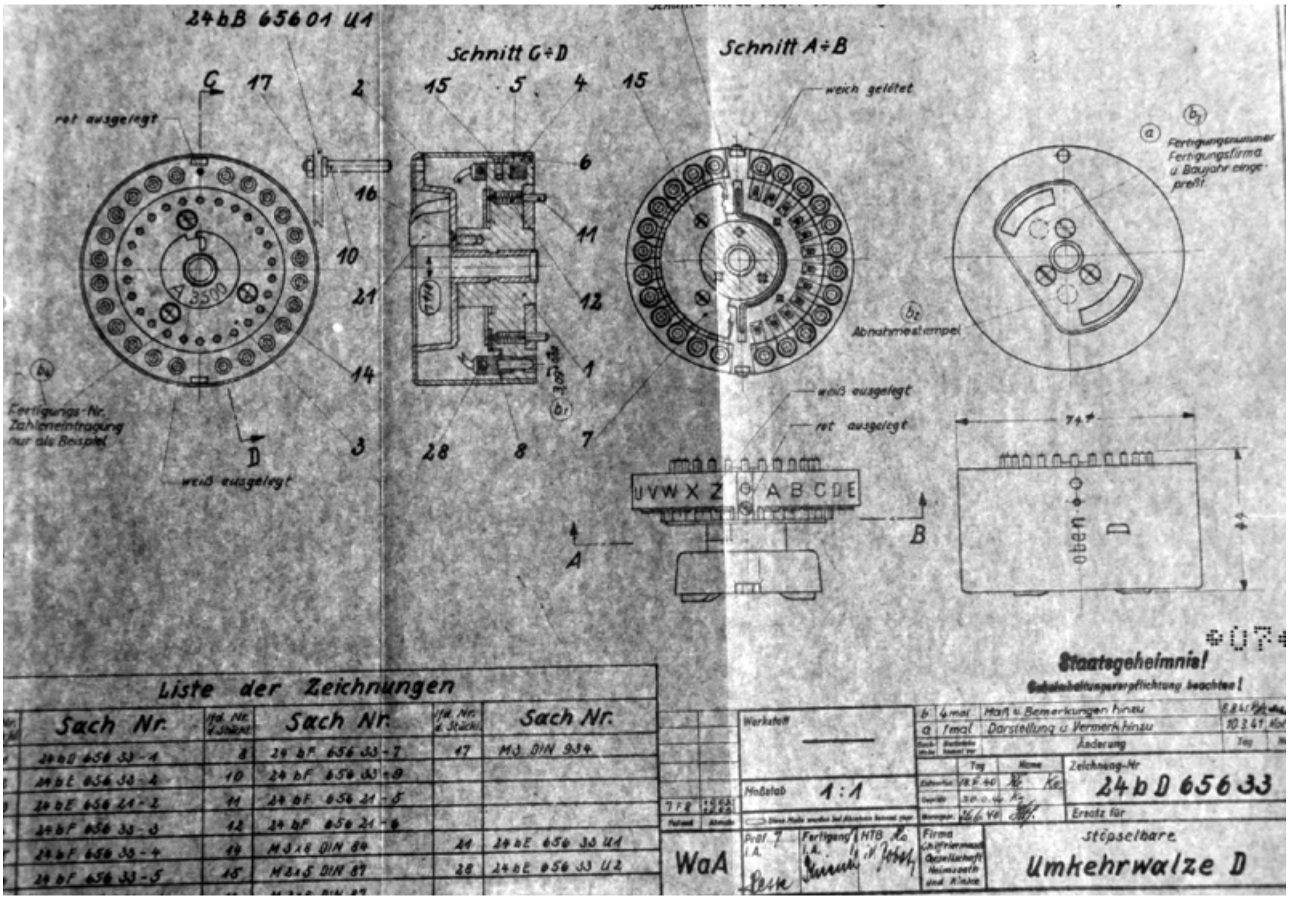


Figure 3. Authentic technical drawing of UKWD from 18 June 1940. The electrical wiring allows for an arbitrarily pluggable pairwise connection of letters with the exception of J and Y, which are permanently connected via a soldered wire. Here the missing Y between the letters X and Z can be spotted. The document is marked as *Staatsgeheimnis!* (State secret). Source: PAAA, Berlin; archive signature: T3771–T3774.

In a new letter also addressed to *WuG 7, VI a4* and dated 15 February 1941 H&R again urgently asks for the official engineering drawings for 24 b 656. Without the drawings H&R and its production firm, *Konski und Krüger* (K&K), are not able to prepare the necessary tools and parts. Concerning UKWD, H&R states that it does not possess its own drawings and it adds: “It should be noted that this wheel (*Walze*) is urgently needed.”

Two days later, on 17 February 1941, a meeting took place at *OKH, Wa Prüf 7/IV* to discuss UKWD. Present were Lieutenant Colonel Karn, Dr. Pupp, Dipl.-Ing. Voss, and Ing. Hesse from *Wa Prüf 7/IV*, Krüger from K&K and Korn from H&R. It is reported that a sample piece from the series production is available, the tool for pressing the letters in the rotor core is ready and that soon the production of the various parts can begin. UKWD was considered a secret item and the engineering drawings were marked as being state secrets (*Staatsgeheimnis*).

The first orders for UKWD are 222–2542/40 of 19 July 1940 for 4000 units and 222–2543/40 of 12 October 1940 for 6048 units. This confirms that 1940 was the year it was decided to equip the Wehrmacht Enigma machines with a pluggable reflector. Additionally, existing Enigma machine orders received add-on orders for UKWD. These concerned the orders 222–2515/39 for 500 units, 222–2–2501/40 for a first delivery of 480 units and again in February 1941, for the same order, a second delivery of 1200 units. Hence, in 1940 alone a total of more than 11,000 UKWDs were ordered.

In addition to these orders, UKWD orders were also placed for the new naval Enigma M4. On 13 September 1940 the *OKM, Inspektion der Marine, Zeugamt, Wilhelmshaven* placed order no. 18824 G for 1891 UKWD wheels. The order was later amended for an additional 2218 units. On 30 April 1941 OKH placed an order, SS 222-2-6401/41, for 1200 *Heeres* Enigmas equipped with

UKWD. In September 1942 yet another 310 units were added to the order 222–2543/40 of 12 October 1940 making it a total of 6358 units. Furthermore, in 1942 two more orders were placed for Enigma machines, which partly included some UKWD wheels. How many UKWDs that were included in these orders is not known, but order SS 222–2–6404/42 was for 2400 *Heeres* Enigmas and order OKM SS 7121–0571/42 for 2099 naval Enigmas M4.

The UKWD development story does not end here; in 1942 Korn had further ideas on how to improve Enigma's security. On 10 December 1942 ChiMaAG informed OKH about three new patent applications and asked if they were to be treated as secret patents or not. The patent applications are:

a) C 57786 IX b/42n – *Chiffrierorgan* (Cipher device)
b) C 57795 IX b/42n – *Chiffrierwalze* (Cipher wheel)
c) C 58002 IX b/42n – *Umkehrwalze für elektrische Chiffriergeräte*
(Reflector for electrical cipher devices)

Patent a), *Chiffrierorgan*, was for a rotor with programmable transport notches, both in position and number. This was the so-called *Lückenfüllerwalze* (variable notch rotor) as it was planned for use in *Heeres* Enigma and the commercial machines Enigma K and Enigma T [17].

Patent b), *Chiffrierwalze*, also concerned the *Lückenfüllerwalze* but here in a version equipped with *Käfigwalze*,[10] the removable rotor core that was used in the naval Enigma machines M4.

And finally, patent c), *Umkehrwalze für elektrische Chiffriergeräte*, a new development of a pluggable UKW, which differed from UKWD in the sense that it was planned to be settable, driven, and that all the 26 letters could be plugged freely.

Further communications with OKH took place on 11 December 1942 and 23 February 1943. The last letter, which also was sent to OKW/Chi, explained in detail the three patents and their importance for increasing the Enigma's cipher security. The *Lückenfüllerwalze* went into production in 1944 and it was planned to introduce it in large numbers in 1945. On 24 July 1944 the *Ertel-Werk*, a firm in Munich building Enigma machines under licence to H&R, received an order for 8000 *Lückenfüllerwalzen*, which later was increased to 12,000 units.

The development of a new pluggable UKW, which was planned to be settable, driven, and where all the 26 letters could be plugged freely, certainly represented the ultimate in the long history of Enigma's pluggable reflectors. It would have seriously threatened the Allied capabilities of breaking the Enigma if it had come into service. However, we lack sufficient information to properly assess its real security value. The open question is how it was planned to drive this reflector. To increase Enigma's cipher security it would have to be driven frequently during the encipherment of a single message.

It is not known what happened to this new driven, settable, and freely pluggable reflector, which never seems to have been put into production. One reason is undoubtedly the state of the German industry which was so disrupted during the final phase of the war. However, a more likely reason is the conflicting views among the various participants on how German cipher systems should evolve and a clear lack of drive in implementing the chosen ideas. There are many examples of this situation but here it suffices to look at UKWD. It took almost four years from the first orders until it was put into service.

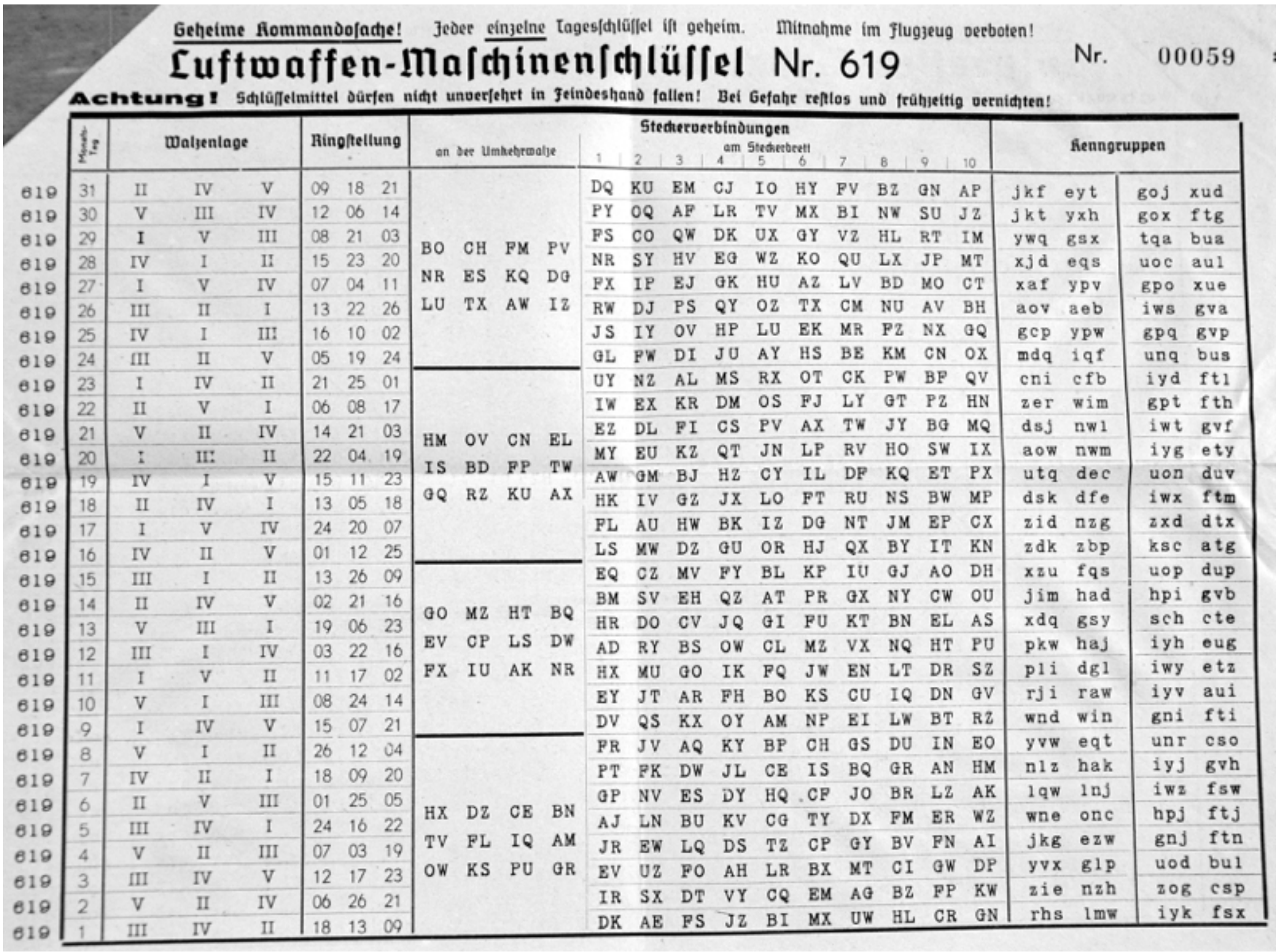
4. Uncle Dick in Action

The German Air Force introduced *Umkehrwalze Dora* on 1 January 1944 [10, p. 107]. In contrast to all other wheels (I to VIII, β, and γ) and reflectors (UKWA, UKWB, and UKWC) of Enigma, UKWD was the only one which could be rewired by the operator in the field. This allowed the wiring to be a part of the key (Figure 4), thus drastically increasing the overall key space of the Enigma, and substantially improving its cryptographic strength [22, p. 39]. This could have caused

[10] *Käfigwalze* (cage wheel) was a new naval Enigma wheel construction that was introduced with Model M3 from serial number M 1822 and onwards. The wired core of the wheel was constructed as an insert that with the removal of one screw allowed the core to be removed from the rest of the wheel, its cage.

more than quite a headache for the codebreakers at Bletchley Park, the centre of British cryptanalysis during World War II, if it had been introduced abruptly and extensively. A report of the Army Security Agency [2, p. 13], written shortly after the war, states: “How close the Anglo-Americans came to losing out in their solution of the German Army Enigma is a matter to give cryptanalysts pause. British and American cryptanalysts recall with a shudder how drastic an increase in difficulty resulted from the introduction by the German Air Force of the pluggable reflector (‘*Umkehrwalze* D’, called ‘Uncle Dick’ by the British) in the spring of 1945 [this should read: 1944]. [...] Only a trickle of solutions would have resulted if the pluggable reflector had been adopted universally; and this trickle of solutions would not have contained enough intelligence to furnish the data for cribs needed in subsequent solutions. Thus even the trickle would have eventually vanished.”

Luckily, UKWD was not adopted universally, but only used for the most sensitive messages [10, pp. 108 and 124], while the majority of messages continued to be enciphered using the long-serving *Umkehrwalze Berta* (UKWB). In fact, this was yet another fatal cryptographic error in the long list of German errors concerning the Enigma. Even more disastrous was the German common practice of using the same key sheet for both sets of messages: those enciphered with UKWB and those enciphered with UKWD.



Geheime Kommandoſache! Jeder einzelne Tagesſchlüſſel iſt geheim. Mitnahme im Flugzeug verboten!

Luftwaffen-Maſchinenſchlüſſel Nr. 619 Nr. 00059

Achtung! Schlüſſelmittel dürfen nicht unverſehrt in Feindeshand fallen! Bei Gefahr reſtlos und frühzeitig vernichten!

	Monats-Tag	Walzenlage			Ringſtellung			Steckerverbindungen											Kenngruppen			
								an der Umkehrwalze	am Steckerbrett 1	2	3	4	5	6	7	8	9	10				
619	31	II	IV	V	09	18	21	BO CH FM PV NR ES KQ DG LU TX AW IZ	DQ	KU	EM	CJ	IO	HY	FV	BZ	GN	AP	jkf	eyt	goj	xud
619	30	V	III	IV	12	06	14		PY	OQ	AF	LR	TV	MX	BI	NW	SU	JZ	jkt	yxh	gox	ftg
619	29	I	V	III	08	21	03		FS	CO	QW	DK	UX	GY	VZ	HL	RT	IM	ywq	gsx	tqa	bua
619	28	IV	I	II	15	23	20		NR	SY	HV	EG	WZ	KO	QU	LX	JP	MT	xjd	eqs	uoc	aul
619	27	I	V	IV	07	04	11		FX	IP	EJ	GK	HU	AZ	LV	BD	MO	CT	xaf	ypv	gpo	xue
619	26	III	II	I	13	22	26		RW	DJ	PS	QY	OZ	TX	CM	NU	AV	BH	aov	aeb	iws	gva
619	25	IV	I	III	16	10	02		JS	IY	OV	HP	LU	EK	MR	PZ	NX	GQ	gcp	ypw	gpq	gvp
619	24	III	II	V	05	19	24		GL	FW	DI	JU	AY	HS	BE	KM	CN	OX	mdq	iqf	unq	bus
619	23	I	IV	II	21	25	01	HM OV CN EL IS BD FP TW GQ RZ KU AX	UY	NZ	AL	MS	RX	OT	CK	PW	BF	QV	cni	cfb	iyd	ftl
619	22	II	V	I	06	08	17		IW	EX	KR	DM	OS	FJ	LY	GT	PZ	HN	zer	wim	gpt	fth
619	21	V	II	IV	14	21	03		EZ	DL	FI	CS	PV	AX	TW	JY	BG	MQ	dsj	nwl	iwt	gvf
619	20	I	III	II	22	04	19		MY	EU	KZ	QT	JN	LP	RV	HO	SW	IX	aow	nwm	iyg	ety
619	19	IV	I	V	15	11	23		AW	GM	BJ	HZ	CY	IL	DF	KQ	ET	PX	utq	dec	uon	duv
619	18	II	IV	I	13	05	18		HK	IV	GZ	JX	LO	FT	RU	NS	BW	MP	dsk	dfe	iwx	ftm
619	17	I	V	IV	24	20	07		FL	AU	HW	BK	IZ	DG	NT	JM	EP	CX	zid	nzg	zxd	dtx
619	16	IV	II	V	01	12	25		LS	MW	DZ	GU	OR	HJ	QX	BY	IT	KN	zdk	zbp	ksc	atg
619	15	III	I	II	13	26	09	GO MZ HT BQ EV CP LS DW FX IU AK NR	EQ	CZ	MV	FY	BL	KP	IU	GJ	AO	DH	xzu	fqs	uop	dup
619	14	II	IV	V	02	21	16		BM	SV	EH	QZ	AT	PR	GX	NY	CW	OU	jim	had	hpi	gvb
619	13	V	III	I	19	06	23		HR	DO	CV	JQ	GI	FU	KT	BN	EL	AS	xdq	gsy	sch	cte
619	12	III	I	IV	03	22	16		AD	RY	BS	OW	CL	MZ	VX	NQ	HT	PU	pkw	haj	iyh	eug
619	11	I	V	II	11	17	02		HX	MU	GO	IK	FQ	JW	EN	LT	DR	SZ	pli	dgl	iwy	etz
619	10	V	I	III	08	24	14		EY	JT	AR	FH	BO	KS	CU	IQ	DN	GV	rji	raw	iyv	aui
619	9	I	IV	V	15	07	21		DV	QS	KX	OY	AM	NP	EI	LW	BT	RZ	wnd	win	gni	fti
619	8	V	I	II	26	12	04	HX DZ CE BN TV FL IQ AM OW KS PU GR	FR	JV	AQ	KY	BP	CH	GS	DU	IN	EO	yvw	eqt	unr	cso
619	7	IV	II	I	18	09	20		PT	FK	DW	JL	CE	IS	BQ	GR	AN	HM	nlz	hak	iyj	gvh
619	6	II	V	III	01	25	05		GP	NV	ES	DY	HQ	CF	JO	BR	LZ	AK	lqw	lnj	iwz	fsw
619	5	III	IV	I	24	16	22		AJ	LN	BU	KV	CG	TY	DX	FM	ER	WZ	wne	onc	hpj	ftj
619	4	V	II	III	07	03	19		JR	EW	LQ	DS	TZ	CP	GY	BV	FN	AI	jkg	ezw	gnj	ftn
619	3	III	IV	V	12	17	23		EV	UZ	FO	AH	LR	BX	MT	CI	GW	DP	yvx	glp	uod	bul
619	2	V	II	IV	06	26	21		IR	SX	DT	VY	CQ	EM	AG	BZ	FP	KW	zie	nzh	zog	csp
619	1	III	IV	II	18	13	09		DK	AE	FS	JZ	BI	MX	UW	HL	CR	GN	rhs	lmw	iyk	fsx

Figure 4. Formerly Top Secret (*Geheime Kommandosache*) authentic key sheet, *Luftwaffen-Maschinenschlüssel* No. 619 as an example, showing the different parts of the Enigma key, i.e. wheel order (*Walzenlage*), ring setting (*Ringstellung*), wiring of UKWD (*Steckerverbindungen an der Umkehrwalze*), and plugboard settings (*Steckerverbindungen am Steckerbrett*). The *Kenngruppen* (indicator groups) serve as discriminators for the used message key, and are no direct part of the key. The fact of the always-missing letters J and Y can be verified by inspecting the middle column (*an der Umkehrwalze*). Source: PAAA, Berlin; archive signature: T3399.

As with *Berta*, the designation *Dora* was used by the Germans to avoid possible misunderstandings, which might happen by a confusion of B and D, when alternatively using UKWB and UKWD. The names *Berta* and *Dora* derive from the German phonetic alphabet, which was used at that time, mainly based upon first names, beginning with *Anton*, *Berta*, *Caesar*, *Dora*, *Emil*, and so forth. The German and the British sides used different designations to describe the 26 contacts of UKWD. Naturally, for the Germans there was no need to meet any cryptanalytic criterion when labelling the contacts. The labels could be freely chosen, as long as each contact got a unique mark and the mark was used uniformly for both the UKWD and the key sheets. In contrast to all the other wheels of the Enigma, which utilized a clockwise lettering of the contacts, the designation of the contacts of UKWD was chosen in an anti-clockwise direction. The reason for that was possibly to ease operation when altering the plugging of UKWD, as in this case the operator is looking at the contacts from the other side and now perceives a clockwise lettering (Figure 5).

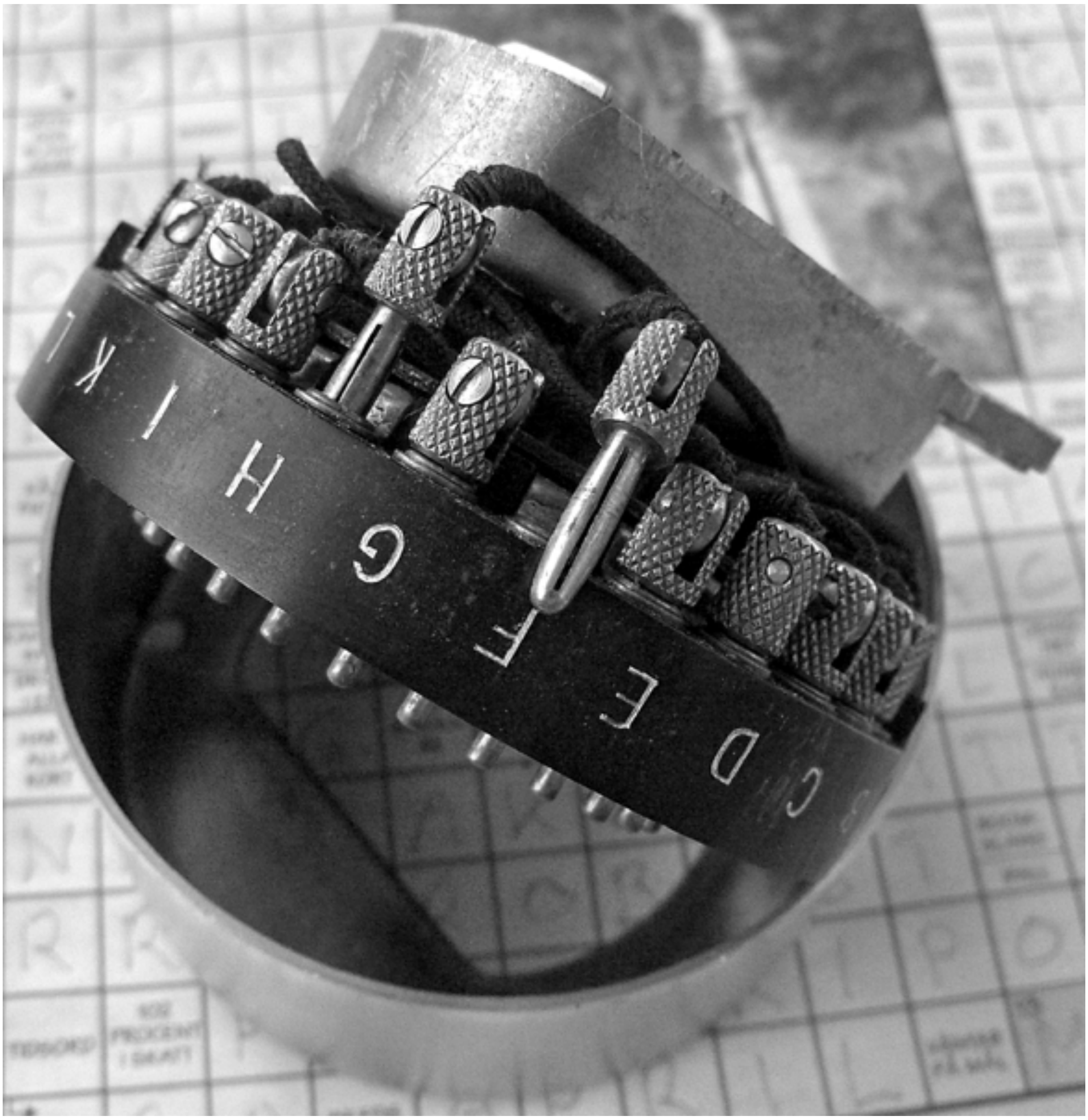


Figure 5. The anti-clockwise designations of the contacts of Uncle Dick, when looking from the entry wheel, and the omission of the letter J between the visible letters I and K can be clearly seen. Photo © 2014 Ingvar Eriksson.

One peculiarity has to be emphasized. Because of mechanical reasons and lack of space, there was one fixed connection between a single pair of contacts. That is the reason why the number of arbitrarily pluggable connections was reduced from 26 to 24 and the number of pluggable wires from 13 to 12. The Germans simply omitted the letters J and Y for the letter designation of the contacts. Therefore, when describing the wiring of UKWD, on German key sheets, the letters J and Y are always missing.

The British codebreakers were not aware of this. For a rather long period, they did not see a German key sheet and they did not know the physical design of UKWD. However this was not needed for cryptanalysis. For that, it was sufficient simply to designate the contacts in a pure logical sense. The BP cryptanalysts followed the current path of each letter from the keyboard through the plugboard and the wheel maze right up to Uncle Dick. They were certainly aware of the one fixed connection, which was detected early in 1944, and helped in breaking successive keys. Because of the clockwise labelling of all the other wheels, BP consistently used a logical and also clockwise labelling for the contacts of UKWD. In BP notation, the fixed connection occurred between the letters B and O. The following table shows the different nomenclatures of the contacts of UKWD, as it was used in GAF key sheets (*Schlüsseltafeln*) and for cryptanalysis at BP [10, p. 103].

GAF	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**-**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**-**	**Z**
BP	**A**	**Z**	**Y**	**X**	**W**	**V**	**U**	**T**	**S**	**O**	**R**	**Q**	**P**	**N**	**M**	**L**	**K**	**J**	**I**	**H**	**G**	**F**	**E**	**D**	**B**	**C**

For cryptologic reasons, it may be interesting to calculate the number of possibilities, which are added to the overall number of combinatorial possibilities of Enigma. The Enigma key space is the product of four distinct factors. The first factor is given by the number of ways of arranging three wheels out of a set of five in different orders. In total, there are 5×4×3 or 60 possible wheel orders (*Walzenlagen*) to be treated. The second factor is given by the adjustment of the rings, which determine an offset between the inner wiring of each wheel and the transport notch, which is the trigger for the neighbouring wheel on the left. Each ring has 26 positions. As the leftmost wheel does not initiate any stepping of another wheel, only the 26 ring positions of the middle and right-hand wheels have to be considered. This gives a factor of 26×26 or 676 possible ring settings (*Ringstellungen*). The third factor is produced by the plugboard. In total, ten *Steckers* can be connected in 150,738,274,937,250 different ways (e.g., [3, p. 254]).

The fourth factor is given by the initial setting of the three rotating wheels. Each of them can be set to an arbitrary letter, A to Z, giving 26 possibilities for each wheel, hence 26×26×26 or 17,576 for three wheels. Because of a minor important but well-known effect of double stepping of the middle rotor [6], the period of the cipher machine is reduced. This means, that the interval after the initial settings of the three wheels repeat is not 17,576, but smaller by 676. In other words, the wheel settings, which can be seen through the three windows of the Enigma, e.g. AAA, does not repeat after 26×26×26 keystrokes, but, due to the double stepping of the middle wheel, after 26×25×26 or 16,900 pushes of a key.

While the fact of the slightly reduced machine period is well known and accepted, the key space is also affected by the double stepping of the middle wheel. This becomes evident when recalling that the double stepping is the reason why some of the initial settings are redundant. These positions are known from the mnemonic Royal Flags Wave Kings Above [5, p. 158]. Here, the initial letters R, F, W, K, and A indicate the position of the used middle wheel (I, II, III, IV, or V), after a double step occurred. As an example, for wheel order I, II, III, and rotor no. II used as the middle wheel, the double stepping occurs when it is one position before the letter F, namely E. Now, with the next step of the rotor set, not only the right hand and left hand rotors will advance, but also the middle wheel performs its anomalous stepping. This is the reason why the initial rotor position AEX, for instance, will advance to BFY with the next keystroke. With the alternative initial rotor position BFX the following position is also BFY. So, both different initial positions, AEX and BFX, give an identical encipherment, and are therefore cryptologically redundant. This is true, for 26×26 or 676 initial wheel settings, which, as a consequence, have to be subtracted from the key space. Thus, the fourth factor of the key space, given by the setting of the three wheels, is

16,900.

In total, Enigma using ten *Steckers* and UKWB has a selection of 103,325,660,891,587,134,000,000 different keys (approximately 76 bits). By introducing UKWD, a fifth factor becomes effective, which is given by the number of possible different wirings of UKWD. This can be calculated by use of the double factorial. The first wire, after connected at one end to one of 24 contacts, can with its other end be connected to one out of 23 contacts. The second wire with its other end to one out of the remaining 21, and so on, yielding 23×21×19×...×5×3×1, or 23!!, or 316,234,143,225 different possibilities for the wiring of UKWD. The overall key space of Enigma using UKWD results in 60×676×150,738,274,937,250×16,900×316,234,143,225 or 32,675,101,845,207,946,930,923,267,150,000,000 keys. This corresponds to almost 115 bits, quite an impressive number, even nowadays.

5. The Three-part Message

On 11 March 1945 a GAF unit sent a longish message, consisting of 496 letters, to another unit. Under the German Enigma regulations for *Heer* and *Luftwaffe*, no transmitted ciphertext message was to exceed the length of 250 characters [13, p. 5]. The plaintext was therefore split into three parts of 242, 224, and 30 letters, which were enciphered individually, using the Enigma machine, with the same basic settings for the daily key (*Tagesschlüssel*), but with different initial positions for the three rotating wheels. All the three message parts were intercepted by the British Y-service, which sent them via secure teleprinter to the Government Code and Cypher School at BP (Figure 6). There, the message key could be determined by the codebreakers of Hut Six, the organisational unit at BP dealing with the cryptanalysis of Enigma messages stemming from the German Army and German Air Force [23].

Eventually the plaintext was recovered using a modified British TypeX machine, which was used as an emulator of the German Enigma. A "Wren", a member of the Women's Royal Navy Service (WRNS), decoded the ciphertext. She adjusted her TypeX to the recovered key and entered the ciphertext on her machine exactly as the German receiver of the message would do on his Enigma. The TypeX produced a long strip of paper carrying the plaintext, which was cut in pieces of suitable length by the Wren, and glued on the back of teleprinter message forms (Figure 7).

The message forms of all three parts survived the war, and are available at Bob Lord's cryptological Web pages.[11] Interestingly, the back of the forms, showing the plaintexts of part one (KTZDY) and part three (YXJRK) are also published there, while the reverse side of part two (DKRKI) is missing. So, the plaintext of the middle part of the GAF message is unknown.

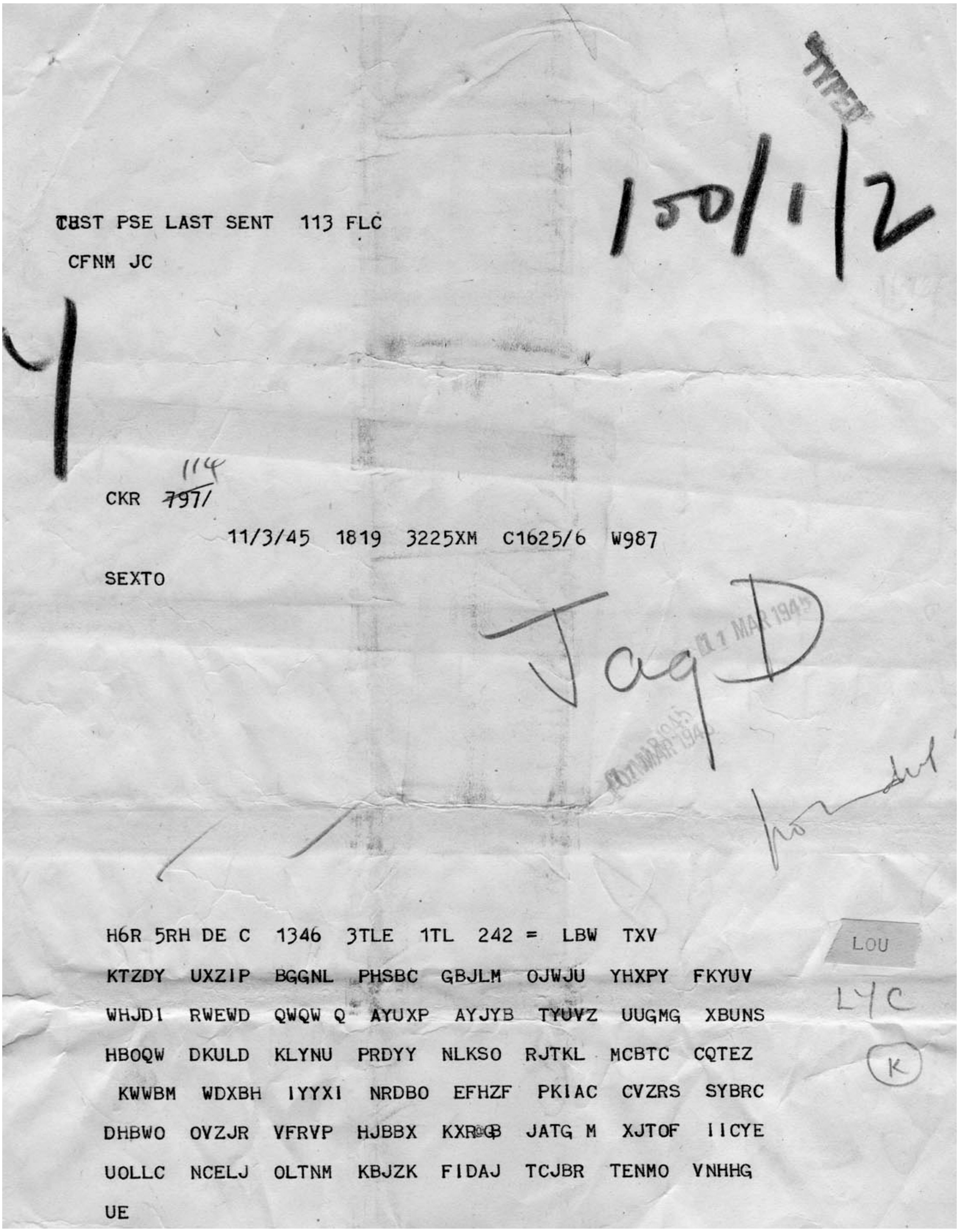
In the following, the ciphertext of all three intercepted messages is shown:

```
KTZDY UXZIP BGGNL PHSBC GBJLM OJWJU YHXPY FKYUV
WHJDI RWEWD QWQWQ AYUXP AYJYB TYUVZ UUGMG XBUNS
HBOQW DKULD KLYNU PRDYY NLKSO RJTKL MCBTC CQTEZ
KWWBM WDXBH IYYXI NRDBO EFHZF PKIAC CVZRS SYBRC
DHBWO OVZJR VFRVP HJBBX KXRGB JATGM XJTOF IICYE
UOLLC NCELJ OLTNM KBJZK FIDAJ TCJBR TENMO VNHHG
UE
```

```
DKRKI CUZAF MNSDC AWXVJ DVZNH DMOZN NWRJC KKJQO
ELWIK XDUUF RCEGN OUNNQ CIIZX FUTNF BTNWI GOECK
CMYUC KTTYB ZMDTU WCNWH OXOFX ERVQW JUCVY PQACQ
EBMXE NOQKF LWRWR LGKXZ BPYWR GQVYG WJDGA QXKVC
MQQJJ PVSLG WFZJZ HHWQG YFCQQ RMVRR QQIDQ QVVIW
LJLBH LHHDI OFWUY JJQGX BWPZ
```

```
YXJRK QVTKA EZZJU NYNKY XZQSS WLAZT
```

[11] The messages can be found here: http://www.ilord.com/bp-decrypts.html (accessed 8 December 2014).



TYPED

150/1/2

```
TEST PSE LAST SENT  113 FLC
 CFNM JC

CKR ~~797~~ 114/
            11/3/45  1819  3225XM  C1625/6  W987
SEXTO

H6R 5RH DE C  1346  3TLE  1TL  242 =  LBW  TXV
KTZDY  UXZIP  BGGNL  PHSBC  GBJLM  OJWJU  YHXPY  FKYUV
WHJDI  RWEWD  QWQW Q  AYUXP  AYJYB  TYUVZ  UUGMG  XBUNS
HBOQW  DKULD  KLYNU  PRDYY  NLKSO  RJTKL  MCBTC  CQTEZ
 KWWBM  WDXBH  IYYXI  NRDBO  EFHZF  PKIAC  CVZRS  SYBRC
DHBWO  OVZJR  VFRVP  HJBBX  KXR@GB  JATG M  XJTOF  IICYE
UOLLC  NCELJ  OLTNM  KBJZK  FIDAJ  TCJBR  TENMO  VNHHG
UE
```

Jag D

11 MAR 1945

11 MAR 1945

LOU

LYC

K

Figure 6. The first part of the three-part message. Photo © 2014 Robert Lord.

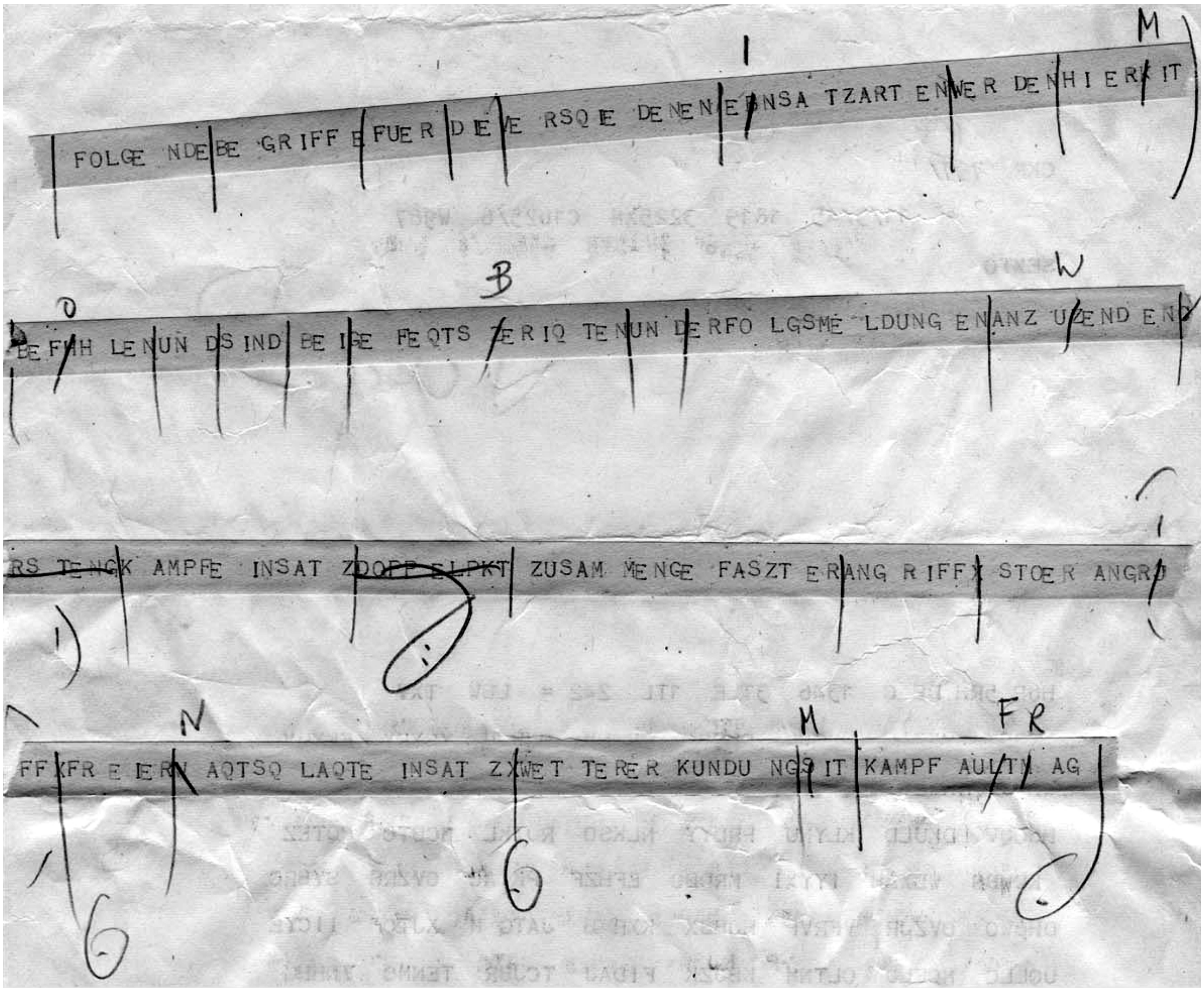


Figure 7. The deciphered text on the back of the first part. Photo © 2014 Robert Lord.

On the reverse side of the first message form the following plaintext can be read.

FOLGE NDEBE GRIFF EFUER DIEVE RSQIE DENEN EBNSA
TZART ENWER DENHI ERKIT BEFHH LENUN DSIND BEIGE
FEQTS ZERIQ TENUN DERFO LGSME LDUNG ENANZ UZEND
ENCRS TENGK AMPFE INSAT ZDOPP ELPKT ZUSAM MENGE
FASZT ERANG RIFFX STOER ANGRJ FFXFR EIERW AQTSQ
LAQTE INSAT ZXWET TERER KUNDU NGSIT KAMPF AULTM
AG

This version of the plaintext of part one of the message, decoded by a Wren as described, was then transferred to one of the intelligence people in Hut Three. There, some obvious garbles were corrected manually using a pencil. Additionally, word separations were indicated, and some punctuation marks and abbreviations were added, as for instance correcting *CRSTENG* to *ERSTENS* (firstly) and replacing it by 1). This gave the following emended plaintext, which is visible using the handwritten notes on the form.

FOLGENDE BEGRIFFE FUER DIE VERSQIEDENEN EINSATZARTEN WERDEN HIERMIT BEFOHLEN UND SIND BEI GEFEQTSBERIQTEN UND ERFOLGSMELDUNGEN ANZUWENDEN 1) KAMPFEINSATZ: ZUSAMMENGEFASZTER ANGRIFF STOERANGRIFF. FREIER NAQTSQLAQTEINSATZ. WETTERERKUNDUNG MIT KAMPFAUFTRAG.

This version of the plaintext was sufficiently readable for the intelligence people, although it still contains some original abbreviations and transcriptions and is therefore not identical to a modern German plaintext. For instance, the German Wehrmacht used Q as a replacement for CH, in order to avoid this frequent bigram within their enciphered messages. So, VERSQIEDENEN means *verschiedenen* (different).

In modern German, part one reads as follows:

Folgende Begriffe für die verschiedenen Einsatzarten werden hiermit befohlen und sind bei Gefechtsberichten und Erfolgsmeldungen anzuwenden. 1) Kampfeinsatz: Zusammengefasster Angriff, Störangriff, freier Nachtschlachteinsatz, Wettererkundung mit Kampfauftrag.

Translated: "The following terms for the different types of operation are hereby ordered and have to be used for combat reports and success messages. 1) Battle actions: Combined attack, intruder attack, free night battle action, meteorological reconnaissance combined with combat mission."

6. Recovering the Key

Initially, only the second part of the three-part message was available from the Internet, as can be seen in Figure 8. Klaus Schmeh has also presented this ciphertext as an example (E08) of an unsolved Enigma message [18, p. 264]. The form gives a clear indication of a message enciphered by the Enigma and it was first believed, to be an ordinary one using the common UKWB. Therefore, we attempted to break it with the aid of a software tool utilizing the hill climbing technique, similar to that described by James Gillogly [4]. The tool is able to decrypt standard Enigma messages of a length of approximately 50 characters or more, and it should succeed in finding the key and plaintext of a rather long message such as part two, containing 224 letters. But it did not succeed. The message form for part two alone gave no further hints, why it was unbreakable, as no date or information concerning the sender or addressee was available.

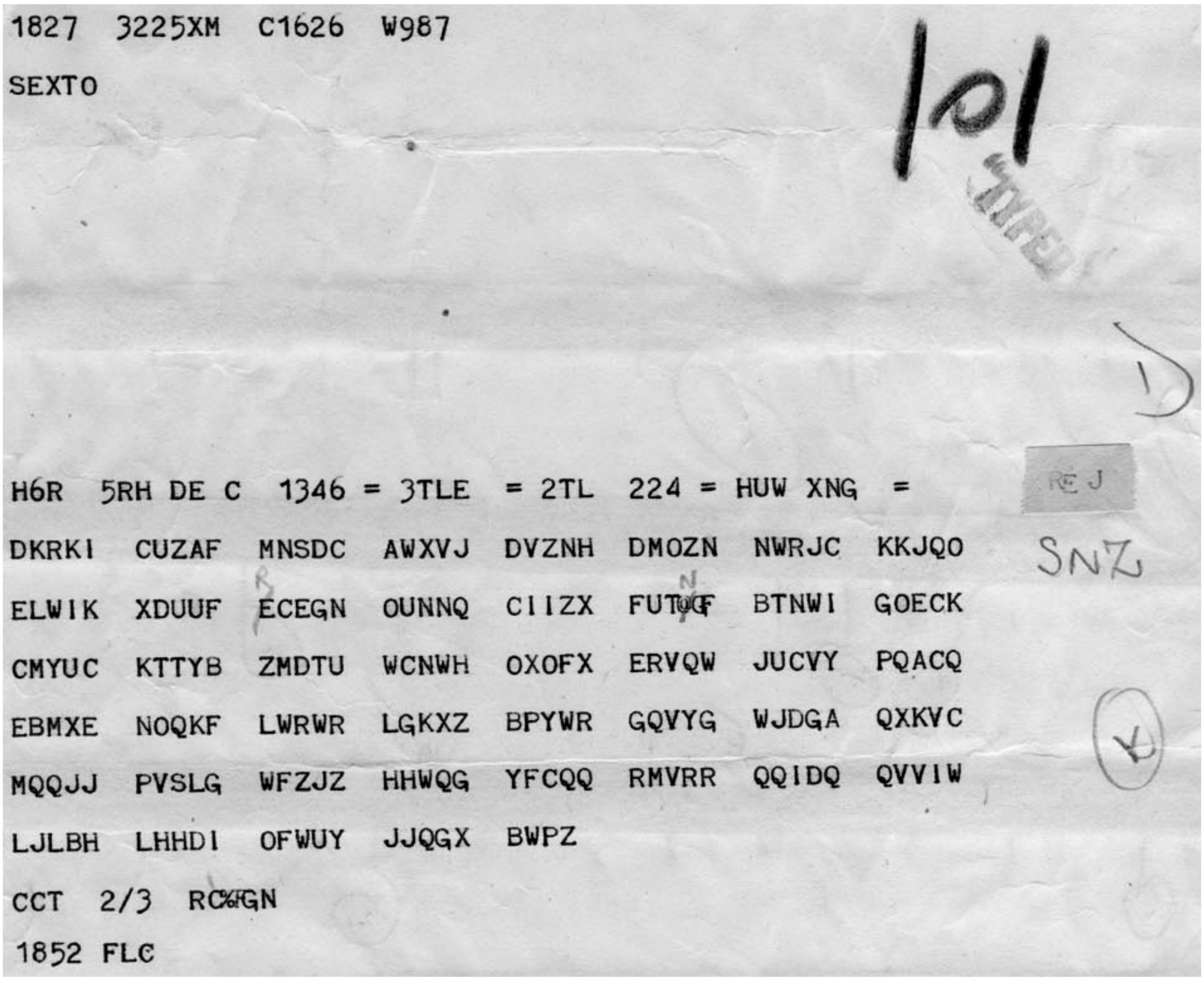
Some time later, the situation changed drastically, after the two companion parts of part two were accidentally found at Bob Lord's site together with the plaintexts of part one and part three, as deciphered at BP. The contents of the plaintext of part one gave strong indication of it being from the GAF. The date of transmission and interception was given as 11 March 1945. Together with the handwritten note "Jag D", at first misinterpreted by us as "Tag D", these were obvious hints that the message was enciphered by the GAF with the aid of UKWD. Jag D is the short form of Jaguar D, the BP code name of one of the GAF's principal networks, namely *Luftwaffenkommando West* [10, p. 125].

Immediately after the ciphertext together with the plaintext of part one was available, it seemed possible to recover the wiring of UKWD, and afterwards to break part two. Obviously, part three was sent on the same day as part one, as can be seen from the ciphertext forms. Therefore, it is safe to assume that part two also stems from the same day and all three parts have been enciphered using the same daily key. This includes the basic settings of the machine (wheel orders, ring settings, *Steckers*) and, of course, the wiring of UKWD. To read the plaintext of the second part of the three-part message, it is first necessary to find the key used for enciphering part one. Then the recovered key can be used to decipher part two.

For recovering the key including the wiring of UKWD, a technique similar to Hand Duenna, as described by C. H. O'D. Alexander in his paper [1], was used; further information about Hand Duenna and more generally about the cryptanalysis of UKWD can be found in [11]. The exhaustion of the key space includes all five possible wheels (I, II, III, IV, and V) at the right-hand side, and the remaining four as the middle wheel, in total twenty wheel combinations. The left-hand wheel, which is supposed not to step, is, together with the unknown Uncle Dick, treated as one unknown, compound or "thick" reflector, here called the "Thick Uncle", with *completely unknown* wires.

In contrast to Alexander's Hand Duenna method, which used only the 26 possible *relative* positions of the middle and the right-hand wheels, here all 26 initial positions of both wheels were exhausted, and all 26 ring positions of the right-hand wheel as well. As runtime was not critical, this approach has the advantage of directly revealing the absolute values of the key. Together with the

20 wheel orders, altogether a search space of 20×26×26×26 or 351,520 "locations", where a solution will be attempted, has to be examined. For each of these locations one has to try to find *Steckers* which do not lead to a contradiction for the flow of the current within the wheel maze, as formed by the scrambler. For that, one starts with a bigram, here called the "primary bigram", i.e. a pair of a corresponding ciphertext and plaintext letter, at an arbitrary text position. In BP such a bigram was called a "constatation". Now, one assumes an arbitrary *Stecker* partner for the plaintext letter and an arbitrary *Stecker* partner for the ciphertext letter. Again, at each location all possibilities have to be exhausted.



```
1827  3225XM  C1626  W987
SEXTO

H6R  5RH DE C  1346 = 3TLE  = 2TL  224 = HUW XNG  =
DKRKI  CUZAF  MNSDC  AWXVJ  DVZNH  DMOZN  NWRJC  KKJQO
ELWIK  XDUUF  ECEGN  OUNNQ  CIIZX  FUTQF  BTNWI  GOECK
CMYUC  KTTYB  ZMDTU  WCNWH  OXOFX  ERVQW  JUCVY  PQACQ
EBMXE  NOQKF  LWRWR  LGKXZ  BPYWR  GQVYG  WJDGA  QXKVC
MQQJJ  PVSLG  WFZJZ  HHWQG  YFCQQ  RMVRR  QQIDQ  QVVIW
LJLBH  LHHDI  OFWUY  JJQGX  BWPZ
CCT  2/3  RC%FGN
1852 FLC
```

101
TYPED
D
RE J
SNZ
R
N
K

Figure 8. The second part of the three-part message, from which the deciphered text was missing. Photo © 2014 Robert Lord.

The plaintext letter can be steckered with 26 different letters. This includes the case of self-steckering, actually an unsteckered plaintext letter, and the singular case of the plaintext letter being steckered with the ciphertext letter. In the latter case, also the ciphertext letter is steckered with the plaintext letter (first case). If the plaintext letter is self-steckered, then there exist 25 different possibilities of *Steckers* for the ciphertext letter (25 further cases). If the plaintext letter is neither steckered with the ciphertext letter nor self-steckered, then there are 24 different letters to which it can be steckered. The same is true for the ciphertext letter, as it can then be steckered with one of 26 letters except two letters, namely the plaintext letter and its *Stecker* partner. In total, there are 1+25+24×24 or 602 possible *Stecker* cases to be considered for the primary bigram. This has to be done for each of the 351,520 locations, which gives the overall workspace of 351,520×602 or 211,615,040 cases.

For each of these cases it is possible to follow the current flow starting at the ciphertext letter and respectively, because of the reciprocity of the Enigma, starting at the plaintext letter, via the plugboard and the entry wheel, the right-hand and middle wheels to the contacts of the thick Uncle. Consequently one wire of the thick Uncle is determined.

In each case, this technique can be used for other text positions as long as no new information is needed. Therefore, in the first instance, only text positions can be utilized, which contain bigrams consisting of one or both letters of the primary bigram, or one or two of the *Stecker* partners of them. For this, the reciprocity of the plugboard is used. If, for instance, A is steckered with B, then B is also steckered with A. So, for other text positions, the current can be traced starting at bigrams identical to the primary bigram, or bigrams, which consist of one of the letters of the primary bigram and one of the assumed *Stecker* partners, or bigrams, which consist of the two *Stecker* partners. After that, either some further wires of the thick Uncle are possibly known or a contradiction has been found. In case of a contradiction, the supposed *Steckers* are wrong (at this location), and the next *Stecker* assumption out of the 602 possibilities has to be checked for the current location.

If no contradictions have been found till now, then further bigrams of the ciphertext and plaintext pairs can be checked. Now one uses bigrams, which consist of only one of the four formerly used letters, i.e. the two letters of the primary bigram and the two letters of their *Stecker* partners. (In some cases, less than four letters are available. This is the position when one or both letters of the primary bigram are self-steckered, or when they are steckered vice versa.) The second letter of the new bigrams to be checked is fully arbitrary, as it has not yet been used.

But the first letter is very useful on its own, as its *Stecker* partner is known by exhaustion, and the current flow starting at this letter can again be traced through the *Eintrittswalze* and the right-hand and middle wheels to the contacts of the thick Uncle. No new wire is directly derived, but at least one contact of the thick Uncle is. If this contact is connected to a known wire, then the current can be further traced through the thick UKW and through the wheel maze back to inner contacts of the *Stecker* board. Here, the formerly useless second letter at the outer contact must be connected to the now known inner contact, thus either leading to a contradiction, or revealing a new *Stecker*.

Subsequently further bigrams become useful, as now for some of them, their *Stecker* partners are recently discovered. So, further wires of the thick Uncle can be recovered, and so on. Finally, by completely extracting all available information from the ciphertext and plaintext pairs, either all 13 wires of the thick Uncle as well as all ten *Steckers* have been discovered, or a contradiction occurs. The latter, actually, is sooner or later the case for nearly all locations. Again, we have Turing's *reductio ad absurdum*, which finally yields the correct solution, i.e. the designation of the middle and the right-hand wheels, the initial setting of both, and the *Ringstellung* of the right-hand wheel. Additionally, the complete *Stecker* board (ten *Steckers*) and the wiring of the thick Uncle (13 wires) are virtually simultaneously recovered. This technique is so powerful, that the whole message length is not needed. The text may be divided into two halves or even four quarters, which helps in case of a lobster (a stepping of the left-hand wheel) or to avoid garbles.

When a solution with ten *Steckers* and 13 wires for the thick Uncle has been found, then, in a last step, the thick Uncle has to be divided into the real (thin) Uncle Dick and one of the three wheels not used as middle or right-hand wheels. For that, three wheels with 26 possible initial positions, in total 78 cases have to be investigated, and the solution is complete.

To manage the final step, it is most helpful to know that the genuine UKWD always paired B with O (in BP notation). In the specific case of the first part (KTZDY) of the described message, just four of the final 78 cases yield a UKWD candidate with B and O connected together. This simplifies the final exhaustion and the finding of the real Uncle Dick. The recovered wiring of Uncle Dick is

AF BO CW DU EL GQ HY IS JR KT MZ NV PX

By deciphering part three of the three-part message the solution can be checked further. If this produces a plaintext identical to the plaintext given at the rear of the BP form, then the key is confirmed. Fortunately, this succeeded, verifying D 125 plx HUP AJ CP DO FU GI MX QZ RW

SV TY as the key (meaning UKW Dora, wheel order I, II, V, *Ringstellung* plx, initial position HUP, and *Steckers* as given).

7. The Plaintext of Part Two

As described, the plaintext of the second part (DKRKI) of the three-part message was not available. After recovering the key together with the wiring of the used Uncle Dick, however, it can simply be decoded, exactly as the entitled receiver would do it. The missing initial setting for the three wheels is given in code on the message form as part of the indicator (*Spruchkopf*), which ends = HUW XNG =. The meaning of this is, use an Enigma set up corresponding to the known daily key, turn the three wheels manually to the basic setting (*Grundstellung*) HUW, and enter XNG via the keyboard. Now three lamps will light up, indicating the initial setting for the three wheels, needed to decode the message. Doing this, the lamps REJ light up successively. Exactly these three letters are printed on a small strip of paper stuck right besides the ciphertext on the sheet, as shown in Figure 8, whereas the handwritten three letters SNZ right beneath the strip indicate the final rotor position, which is reached after all the 224 letters of the ciphertext have been entered.

If neither the initial setting nor the indicator were available, then a last complete search had to be performed. For that, all the 26×26×26 or 17,576 possible initial positions of the three wheels are checked until the plaintext comes out. The recovered key and plaintext reads as follows.

```
D 125 plx REJ AJ CP DO FU GI MX QZ RW SV TY

ZWEIT ENSJA GDEIN SATZD OPPEL PKQJA BOJAG DIMER
WEITE RTENG ESQWA DERUN TETBR INGBN GSRAU MXARI
UNDTI EFFLI EGERB EKAEM PFUNG XJAGD VORST OSZXA
LARMS TARTX PLATZ BEZIE HUNGS WMISE BEGLE ITSQU
TZXWE TTERE RKUND UNGXD RITTE NSAUF KLAER UNGSE
INSAT ZXLUF TBILD ERKUN DUNG
```

With correct word spaces it reads:

Zweitens Jagdeinsatz Doppelpkq Jabojagd im erweiterten Gesqwaderuntetbringbngsraum x Ari und Tieffliegerbekaempfung x Jagdvorstosz x Alarmstart x Platz beziehungswmise Begleitsqutz x Wettererkundung x Drittens Aufklaerungseinsatz x Luftbilderkundung

The plaintext contains a few garbles and the usual replacements, such as Q for CH. In modern German, part two reads as follows:

2) Jagdeinsatz: Jabo [Jagdbomber]-Jagd im erweiterten Geschwaderunterbringungsraum. Ari- [Artillerie-] und Tieffliegerbekämpfung, Jagdvorstoß, Alarmstart, Platz- bzw. Begleitschutz, Wettererkundung. 3) Aufklärungseinsatz: Luftbilderkundung.

Translated: “2) Fighter missions: Fighter-bomber chase within the extended squadron mission area. Combat against artillery and strafers (low-flying aircraft), fighter attack, scramble start, airfield protection and flying escorts, meteorological reconnaissance. 3) Reconnaissance mission: Photographic air reconnaissance.”

8. Redeciphering Part One

By knowing the key, it is not only possible to decode part two (DKRKI) but also redecipher part one (KTZDY), using the key D 125 plx LOU AJ CP DO FU GI MX QZ RW SV TY. This seems to be of no use, because the German plaintext is already known from the reverse side of the message form (Figure 7), but the plaintext as printed on the strips is slightly garbled. These garbles were avoided by simply omitting these text positions and the corresponding constatations during the described key recovery procedure. The garbles are marked here with the @ symbol in the following transcription.

```
FOLGE NDEBE GRIFF EFUER DIEVE RSQIE DENEN E@NSA
TZART ENWER DENHI ER@IT BEF@H LENUN DSIND BEIGE
FEQTS @ERIQ TENUN DERFO LGSME LDUNG ENANZ U@END
EN@RS TEN@K AMPFE INSAT ZDOPP ELPKT ZUSAM MENGE
FASZT ERANG RIFFX STOER ANGR@ FFXFR EIER@ AQTSQ
LAQTE INSAT ZXWET TERER KUNDU NG@IT KAMPF AU@T@
AG
```

An interesting question, which might be asked, is, who made the mistakes? As usual, the lazy or stressed German cipher clerk or wireless operator, or was it one of the Wrens at BP? The unexpected answer is that in this case the British made more mistakes than the Germans. Re-deciphering the intercepted German ciphertext with the newly recovered key shows this to be true and results in the following plaintext.

```
FOLGE NDEBE GRIFF EFUER DIEVE RSQIE DENEN EINSA
TZART ENWER DENHI ERMIT BEFHH LENUN DSIND BEIGE
FEQTS BERIQ TENUN DERFO LGSME LDUNG ENANZ UWEND
ENERS TENSK AMPFE INSAT ZDOPP ELPKT ZUSAM MENGE
FASZT ERANG RIFFX STOER ANGLI FFXFR EIERN AQTSQ
LAQTE INSAT ZXWET TERER KUNDU NGMIT KAMPF AUFTR
AG
```

The former twelve garbles, as shown in the original BP plaintext, now reduce to only two garbles, i.e. BEFHHLEN and ANGLIFF. Interestingly enough, one new corruption occurs, namely "L" in ANGLIFF, which is correctly written as "R" in the BP decrypt ANGRJFF (although the following letter is garbled). So, this might be the not totally unlikely but rather improbable accidental case (with a chance of 1 in 26), that a German mistake together with a British mistake compensated each other and produced a correct plaintext letter.

9. Conclusion

Based on new research in the German archives, the development history of *Umkehrwalze D*, Enigma's pluggable reflector, has been presented from the mid-1920s to its actual usage in 1945. As an example, a German *Funkspruch* (radio message) enciphered with UKWD and transmitted on 11 March 1945, is shown. The three-part message was intercepted by the British Y-service and subsequently broken by the codebreakers at Bletchley Park. While the decrypts of the first and third parts are known, the plaintext of the second part was not available. To break part two, the recovery of the unknown wiring of UKWD was needed.

For that purpose the ciphertext and plaintext pair of the first part of the intercept was used together with modern computer-based cryptanalysis. The presented key recovery technique utilises constatations, which are available as text pairs, making logical deductions, which mostly lead to contradictions, similar to Turing's *reductio ad absurdum*, and eventually unveils the wiring of the UKWD. In GAF notation it is AV BO CT DM EZ FN GX HQ IS KR LU PW. Simultaneously, the described method recovers the daily key of the Enigma, including all *Steckers* as well as the initial setting of the three rotating wheels. Thereby the decryption of the second part of the message became possible. The technique works generally and can be used to break other Enigma ciphertexts, enciphered on a machine equipped with an UKWD with unknown wiring, when a sufficiently long crib is available (e.g., 60 letters, in some cases even only 48 letters proved to be sufficient).

In contrast to the task of breaking one of the German Army ciphers [20], where the main and most critical part is the hill climbing for recovering the *Steckers* [4], the detection of the key of the *Luftwaffe* with Uncle Dick and the aid of a known ciphertext and plaintext pair (i.e. a very long crib), is perfectly deterministic, without any hill climbing problems. The runtime for the whole search space of 351,520 locations with 602 possible *Stecker* cases each, which yields 211,615,040 cases, is approximately half an hour on a standard desktop computer, in this case an Intel i7-3770 processor running at 3.4 GHz. Tests have shown that running the same executable in several instances (e.g. four times on a quad core computer, each core working on a different part of the key space) reduces the runtime even further. Alternatively, the different cores can work on different parts of the ciphertext, for example the first core dealing with the first quarter of the text, and so on. Subsequently, either a solution is found or, for instance because of a lobster or unknown garbles, it is missed. If the correct wheel order is one of the first of the search space, the solution is found in a few minutes. Using another sufficiently frequent constatation as the primary bigram has little influence. If a solution is found, it yields the identical key and plaintext.

Acknowledgments

We should like to thank Bob Lord, Ingvar Eriksson, and Dirk Rijmenants for their generosity in allowing us to use their photos and illustration for our article. Very special thanks are directed to Bernhard Richt for many valuable crypto talks and Ralph Erskine for his thorough review. The second author should like to especially thank the staff of the *Politisches Archiv des Auswärtigen Amts* in Berlin whose arrangements and friendly help made his research there a great success.

About the Authors

Olaf Ostwald is a microwave engineer working with Rohde & Schwarz in Munich on the design of electronic measuring equipment. He is interested in historical cryptography and cryptanalysis, especially in the techniques of breaking the Enigma.

Frode Weierud is a retired electronics engineer formerly employed by the European Organization for Particle Physics (CERN) in Geneva where he worked as a programmer in one of the equipment groups. Cryptography has been his main interest for more than 40 years. His cryptological research is focused on cipher machines and cryptanalytical techniques.

References

1. Alexander, C. H. O'D. 1944. "Hand Duenna." Addendum to Captain Walter J. Fried's report No. 62 of 13 July 1944. National Archives and Records Administration (NARA), College Park, Md., Record Group 457, NSA Historical Collection, Box 880, No. 2612. Edited by Frode Weierud, June 1998. http://cryptocellar.org/alexander/duenna.pdf (accessed 8 December 2014).

2. Army Security Agency. 1946. "Notes On German High Level Cryptography and Cryptanalysis, European Axis Signal Intelligence in World War II," Vol. 2, Washington, (D.C.). http://www.nsa.gov/public_info/_files/european_axis_sigint/volume_2_notes_on_german.pdf (accessed 8 December 2014).

3. Bauer, C. P. 2013. *Secret History: The Story of Cryptology*. Boca Raton: CRC Press.

4. Gillogly, J. J. 1995. "Ciphertext-only Cryptanalysis of Enigma," *Cryptologia*, 19(4):321–413.

5. Good, I. J. 1993. Enigma and Fish. In *Codebreakers : The Inside Story of Bletchley Park* edited by F. H. Hinsley and Alan Stripp, 149–166. Oxford: Oxford University Press.

6. Hamer, D. H. 1997. "Enigma: Actions Involved in the 'Double Stepping' of the Middle Rotor," *Cryptologia*, 21(1):47–50. http://home.comcast.net/~dhhamer/downloads/rotors1.pdf (accessed 8 December 2014).

7. Hamer, D. H., Sullivan, G., and Weierud, F. 1998. "Enigma Variations: An Extended Family of Machines," *Cryptologia*, 22(3):211–229. http://cryptocellar.org/pubs/enigvar.pdf (accessed 8 December 2014).

8. Kruh, L. and Deavours, C. 2002. "The Commercial Enigma: Beginnings of Machine Cryptography," *Cryptologia*, 26(1):1–16.

9. Mächtel, F. 2009. *Das Patentrecht im Krieg*. Tübingen: Mohr Siebeck.

10. Marks, P. 2001. "Umkehrwalze D: Enigma's Rewirable Reflector – Part I," *Cryptologia*, 25(2):101–141.

11. Marks, P. 2001. "Umkehrwalze D: Enigma's Rewirable Reflector – Part II," *Cryptologia*, 25(3):177–212.

12. Marks, P. 2001. "Umkehrwalze D: Enigma's Rewirable Reflector – Part III," *Cryptologia*, 25(4):296–310.

13. Oberkommando der Wehrmacht. 1940. *Schlüsselanleitung zur Schlüsselmaschine Enigma*, H.Dv.g. 14, Reichsdruckerei, Berlin. http://www.ilord.com/enigma-manual1940-german.pdf (accessed 8 December 2014).

14. Patent. *Chiffrierapparat* (Cipher device), Reichspatentamt, DRP No. 416 219, 23 February 1918. http://www.cdvandt.org/Enigma%20DE416219C1.pdf (accessed 8 December 2014).

15. Patent. *Elektrische Chiffriervorrichtung* (Electrical cipher device), Reichspatentamt, DRP No. 554 421, 31 January 1928. http://www.cdvandt.org/Enigma%20DE554421C1.pdf (accessed 8 December 2014).

16. Reuvers, P. and Simons, M. 2013. *Enigma G-111: A rare version of Zählwerk Enigma G31*. Crypto Museum, Eindhoven, The Netherlands. http://www.cryptomuseum.com/crypto/enigma/g111/files/g111.pdf (accessed 8 December 2014).

17. Reuvers, P. and Simons, M. 2014. *Lückenfüllerwalze: Programmable Enigma cipher wheel*. Crypto Museum, Eindhoven, The Netherlands. http://cryptomuseum.com/crypto/enigma/lf/index.htm (accessed 8 December 2014).

18. Schmeh, K. 2012. *Nicht zu knacken*. München: Carl Hanser Verlag.

19. Sebag-Montefiore, H. 2000. *Enigma: The Battle for the Code*. London: Weidenfeld & Nicolson.

20. Sullivan, G. and Weierud, F. 2005. "Breaking German Army Ciphers," *Cryptologia*, 29(3):193–232. http://www.tandf.co.uk/journals/pdf/papers/ucry_06.pdf (accessed 8 December 2014)

21. TICOM. 1945. ENIGMA Documents from Heimsoeth & Rinke. Bestand Rückgabe TICOM, Politisches Archiv des Auswärtigen Amts. Berlin. Archive Signature: T 1715, T1716, T1717, and T1718.

22. US 6812 Bombe Report. 1944. "6812th Signal Security Detachment," APO 413, US Army. NARA, College Park, Md., Record Group 457, NSA Historical Collection, Box 970, No. 2943 Formatted by Tony Sale, Bletchley Park (2002), 39-40. http://www.codesandciphers.org.uk/documents/bmbrpt/usbmbrpt.pdf (accessed 8 December 2014).

23. Welchman, G. 1982. *The Hut Six Story: Breaking the Enigma Codes*, London: Allen Lane.