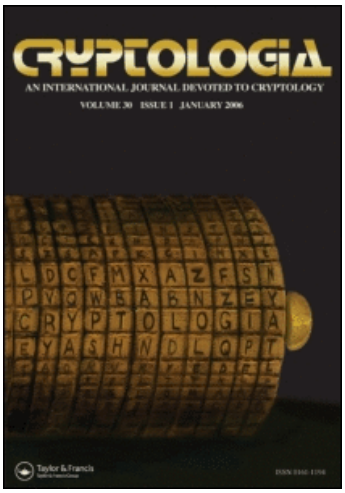

Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t725304178

Resurrecting Bomba Kryptologiczna: Archaeology of Algorithmic Artefacts, I

David Link

Online Publication Date: 01 April 2009

To cite this Article Link, David(2009)'Resurrecting Bomba Kryptologiczna: Archaeology of Algorithmic Artefacts, I',Cryptologia,33:2,166 — 182
To link to this Article: DOI: 10.1080/01611190802562809
URL: http://dx.doi.org/10.1080/01611190802562809

Cryptologia, 33:166–182, 2009

ISSN: 0161-1194 print
DOI: 10.1080/01611190802562809

Taylor & Francis
Taylor & Francis Group

Resurrecting *Bomba Kryptologiczna*: Archaeology of Algorithmic Artefacts, I

DAVID LINK

Abstract The procedure executed on the Polish *Bomba Kryptologiczna* is reconstructed on the basis of Marian Rejewski's accounts and simulative experiment. An original Wehrmacht message from the period in question is broken to illustrate the effectiveness of the hardware and the routines employed. The authenticity of the indicators given in Rejewski's first and later reports is investigated and the circuitry of a simplified version of the bomba presented.

Keywords Bomba Kryptologiczna, cryptanalysis, Enigma

1. Introduction

Shortly before the Second World War, the Polish mathematicians Marian Rejewski, Henryk Zygalski and Jerzy Różycki of the German section BS-4 of the *Biuro Szyfrów* devised a semi-automatic device to break the German "Enigma." Although this is by now an established fact,[1] the exact cryptanalytic method employed remains remarkably obscure, and there is no detailed description in Rejewski's accounts. The aim of this paper is to shed light on this important early stage in the attack on the German encryption device by simulating the Polish artefact in software and trying to determine a procedure simple enough to solve the rotor order, ring setting and Steckers within the reported two hours [15, p. 290].

From September 1938 to May 1940, Enigma was employed in the following way: for each day, the operator on the sending side would locate the order of the three rotors, the five to eight pairs of letters to be permuted by the plugboard, and the so-called *Ringstellung* on a sheet listing the settings for the month. (The circumferential alphabet could be rotated with respect to the core of the wheels and its inner wiring. When the right ring was advanced one step, the permutation that had been at indicators `AAA` was now found at `AAB`, etc.) He "randomly" selected a *Grundstellung* (basic setting) on his own that was transmitted two times in clear, followed by the doubled message key encrypted with it and the telegram enciphered with the latter. (For a detailed description of the machine and the procedures employed at the time, see [8, p. 247ff].) The result was communicated acoustically in Morse code

Address correspondence to David Link, Centre for Art and Media Technology, Lorenzstr. 19, 76135 Karlruhe, Germany. E-mail: david@khm.de

[1]This has not always been the case, as the heated discussion almost 40 years after the end of the war shows, cf. [14].

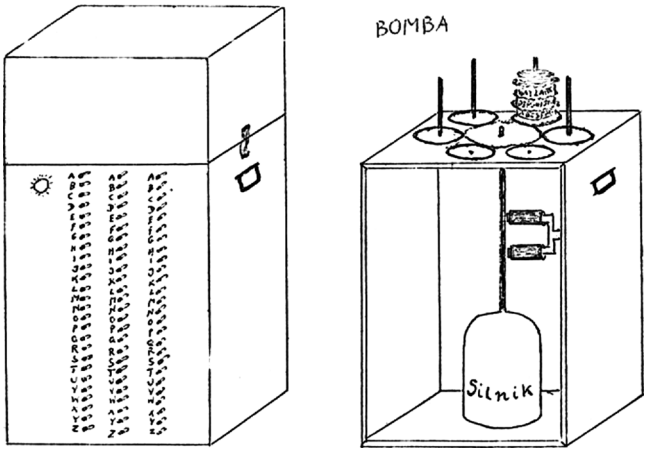

Figure 1. Outside and interior of Polish "bomba", drawing by Rejewski, 1978 [7, p. 316].

on short wave radio links and could be intercepted by listening stations of the Poles, the British, and other European countries.

2. The Machine

In their attack, the Polish codebreakers relied on the phenomenon that in a number of intercepts, one letter of the message key, which was doubled to protect it against transmission errors, was encrypted to the same character. This resulted in groups like **W**AV**W**HA, in which the first symbol was enciphered as W on the first and the fourth position. These doublings were called "females" by the Poles (the modern term is "fixpoint", cf. [2, p. 396]) and also occurred at the second and fifth or third and sixth letter. According to Kozaczuk, the equivalent Polish term "samiczka, Plur. samiczki" resulted from a diminutive of the word "te same" (the same). It was later adopted by the Britons, who ignored the meaning of the term [8, p. 63]. Females could be employed to deduce the ring setting of the wheels, to recover the plugs and finally the message key, allowing to read all dispatches of a day, but 105,456 rotor positions had to be searched for a specific pattern. If manual testing of an indicator would have taken a minute, the time needed for the whole operation would have amounted to more than two months, and by then, the content of the messages would have been strategically worthless.

Consequently, the Poles mechanised the task. The *bomba kryptologiczna* ("cryptologic bomb", Figure 1) consisted of three pairs of Enigma rotor sets driven by an electric motor via a planetary gear. Six "bomby" (Polish plural of "bomba") were quickly built by the AVA Radio Manufacturing Company ("Wytwórnia Radiotechniczna AVA") in Warsaw in November 1938, one for each of the possible wheel orders. The firm, which at one point employed more than 200 workers, had previously built the Polish rotor encryption device Lacida, Enigma doubles and another cryptological apparatus, the Cyclometer. Apparently, at least some copies of the first artefact have survived [8, pp. 211, 134, 25, 263].

The offsets of the simultaneities were set up on the hardware of the machine. If three dispatches beginning GKD **W**AV**W**HA, JOT I**W**AB**W**N and MDO OT**W**YZ**W** had

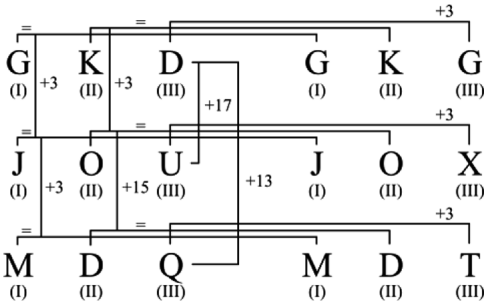

Figure 2. Bomba setup for breaking females of indicators GKD, JOT and MDO.

been received, the first three letters of each being the Grundstellung in clear, and the last six the encrypted doubled message key containing females on positions 1–4, 2–5, and 3–6, it was "programmed" corresponding to Figure 2.[2]

Different witnesses have given various explanations for the name of the device, "bomba kryptologiczna," but none is easy to believe. Rejewski wrote they had designated it thus "for lack of a better idea" [13, p. 267]. After escaping from occupied France over Spain, Portugal and Gibraltar, the two remaining cryptanalysts worked for a Polish signal battalion stationed in Stanmore, England, from August 1943 on. (Jerzy Różycki had perished in the sinking of a passenger ship when returning from an outpost in Algiers to France on 9 January 1942.) Its commander, Tadeusz Lisicki, originated the most popular legend: the mathematicians had come up with the idea of the device while eating a popular ice-cream dessert called "bomba" (Letter by Tadeusz Lisicki, 30 August 1982, quoted in [8, p. 63, n. 1]). The third explanation is found in an internal U.S. American military report written four years after the bomby had been destroyed, on 11 October 1943: "This term ['bombe'] was used by the Poles and has its origin in the fact that on their device when the correct position was reached a weight was dropped to give the indication." [1, p. 1]

3. The Procedure

Usually, the following account of the procedure executed on the bomba is given: the operator set the first pair of Enigmas to the indicators that had produced the coincidence at the first and fourth position of the doubled key, GKD and GKD+3 = GKG. The offset of three reflected the fact that in females, the same letter was produced three steps apart. He then turned the second pair to JOU, the indicator at which the second simultaneity had occurred, JOT, augmented by one, because it had happened one step later than the first (at symbols two and five). Again, he offset the second machine of the couple by three relative to the first, JOX. The same consideration led to indicators MDQ (MDO+2) and MDT (MDQ+3) for the third pair

[2]The example is taken from the earliest of Rejewski's accounts, [11, p. 29]. The document was prepared in France to be included into an internal report by the head of the Cipher Bureau, Col. Gwido Langer, dated 12 May 1940. The same indicators are repeated in [12, p. 1] and [9, p. 203]. Most discussions of the bomba quote the example RTJ–DQX–HPL, given much later in an article published posthumously, [13, p. 266]. Cf. for example [2, p. 395f.]. The authenticity of these examples will be investigated in Section 7 of the present article.

of Enigmas. Current was switched on at the contact corresponding to the repeated letter of the females (in our example, W), and the apparatus automatically stepped through all possible wheel positions of one rotor order, until each couple output two identical characters and reproduced the three-fold simultaneity.[3] In this case, the machine stopped lighting a lamp and permitted the operator to note the indicators [8, p. 53]. Revolving the rotors through all possible 17,576 positions on six bomby in parallel each working on one wheel order took about 100–120 minutes. That allows the estimate that it was testing two to three settings per second, at a speed between 5.6 and 6.8 rpm (revolutions per minute).[4] From the indicators and rotor order found, the ring setting, plugs and message key could be deduced, permitting to read all messages of a day. At a conference near Warsaw in late July 1939, shortly before their country was invaded by German troops, the Poles handed two Enigma replicas, technical drawings of the Cyclometer and the Bomba over to the Britons and French [8, p. 59].[5] All their bomby were destroyed in September 1939, before the cryptologists were forced to flee over Romania, Serbia, Croatia, and Italy to Paris [8, p. 77, n. 5 and 14, p. 81].

It is an irritating fact that the procedure published in Rejewski's accounts and subsequently in many of the books on the topic does not effectively solve Enigma cryptograms when tried out on an emulator. Most descriptions assume that one of the indicator settings the machine had halted at would translate the enciphered six letters into "something of the form XYZXYZ", the doubled message key in clear [4, p. 244]. In 2005, Heinz Ulbricht, who served the German Air Force during World War II, submitted his detailed and methodically novel Ph.D. dissertation at Technical University Braunschweig, in which he simulated all methods used by the Poles and Britons with computer programs.[6] In his account of the bomba, he omitted the question how to convert the rotor positions found into ring settings by directly turning the circumferential alphabets in his software, an operation technically impossible on the original machine. But even then, the resulting indicators do not easily allow reconstructing the message key, because around half of the symbols, three of six, were steckered on the plug board at the time [17, pp. 100–106]. After five pages of complicated argumentation and experiment, Ulbricht arrives at a solution of the cryptogram. It seems improbable that the method described by him allowed the Poles to read Enigma traffic on a regular basis. When his example was set up

[3]The notches that moved the neighbouring wheel forward had all been set to Z to allow regular turning of the rotors. Cf. [17, p. 101].

[4]Cf. [15, p. 290]. The speed of its successor, the Turing bombe, was about 10 times higher, testing 26.6 indicators per second, at a speed of 61.5 rpm: "Our machine [the Turing bombe rebuild] will complete a full unsuccessful run in 11 minutes." (John Harper, personal communication, 31 March 2008)

[5]In the National Archives, London, ref. HW 25/9, a document is located named "ZYKLOMETER schematic", probably being the only remaining or at least the only declassified item of the exchange, annotated in perfect German. The location of the two Enigma doubles is unknown. The replica in Sikorski Institute, London, was manufactured at a later date by a French company, as proven by the word "Controle" printed on the top right corner. Cf. [8, p. 178, caption on photo on the right side]. The history of cryptology would be furthered if these items were finally, 70 years after they were handed over, declassified.

[6]The simulative work has added many valuable details on the concrete operations in codebreaking Enigma. It is typical for the exact history of algorithmic artefacts that it is almost impossible to understand the dissertation without performing the procedures and consequently, reconstructing the machines, at least in software.

on the author's bomba emulator, it did not stop at all in the wheel order it was based on. The reason was that the last of his basic settings, UQR, produced a turnover of the middle and left rotor while encrypting the doubled message key, since the notch in the middle wheel, number 1, is at Q. It is known that two conditions are necessary for the procedure to work:

1. The repeating character in the female must not be steckered. The fulfilment of this condition is due to chance. If 5 to 8 pairs of letters are exchanged, as was the case in November 1938, when the bomba was built, it will be met half the time on the average [17, p. 101].
2. Only the right-hand wheel can move during encryption of the six signs of the doubled message key [4, p. 241]. Since the positions of the notches on the rotors were known at the time, this was easy to arrange. For wheel order 312 the last letter of the basic setting has to be smaller than Z and greater than E, because drum 2 steps its neighbour forward at E, and the middle indicator should not be Q, its turnover position.

4. Reconstructing the Polish Routine

Fortunately, Rejewski provided a theoretical hint at the method of solution in his discussion of the bomba:

> Let us assume, for a moment, that permutation S [the exchange of letters on the plugboard] is identical. If, as well, there were no setting of rings, and we also knew the sequence of the drums on the axle, it would suffice to set the drums to position RTJ [the basic key of the first female], and a depression of the key "w" would cause one and the same lamp to light within the interval of three strokes. The same would happen in position HPN and position DQY [the basic keys of the other two females incremented by their relative offsets] of the drums. The setting of the rings causes the positions of the drums at which this will occur to be unknown to us. However, the differences in the positions will be preserved, and are therefore known to us. [13, p. 266]

After programming the emulator of the bomba, numerous experiments generating message keys and trying to break them were unsuccessful, because the indicators at which it came to a halt were not easily interpreted.[7] Trying to simplify the process, females for ring setting AAA were produced and run on the virtual machine.[8] It stopped at the first, the starting position, and proved Rejewski's above statement practically: If the circumferential alphabets are not rotated, the solution is produced immediately. For females of ring setting AAB the machine halted at the very last position, and for AAZ at the second, always relative to the Grundstellung of the 1–4 repetition (Figure 3).

[7]The program can be found on the author's website, http://alpha60.de/research/bomba_krypt/. In parallel to the historical developments, the Enigma simulator Andy Carlson has provided at http://homepages.tesco.net/~andycarlson/enigma/enigma_j.html has been reverse-engineered to assemble a bomba out of six German encryption machines.

[8]The other settings were: wheel order 213, plugs AM, CQ, DF, EY, HL, JX, OZ. All cryptograms in this paper are based on reflector ("Umkehrwalze") B, which was the one employed from autumn 1937 on [13, p. 264].

Ring setting	*Females*	*Message key in clear*	*Start position (a)*	*Stop position (b)*	*c = stop – start*	AAA – *c*
AAA	HDW **B**JZ**B**SR OOC B**B**LQ**B**Z TWB LM**B**VE**B**	HRF NYT RQI	HDW	HDW	ZZZ	AAA
AAB	FUE **B**JI**B**US PTB A**B**ZI**B**D TZD AF**B**FV**B**	NZL WZX HHI	FUE	FUD	ZZY	AAB
AAZ	HGJ **B**UB**B**SI WAA S**B**CF**B**Y OCX AE**B**GD**B**	IHC MYU NCY	HGJ	HGK	ZZA	AAZ
AZA	YSX **B**ED**B**PA QLC Y**B**IQ**B**R FHF FV**B**II**B**	PRK PHB DTM	YSX	YTX	ZAZ	AZA
ZAA	ZKE **B**PA**B**AE ALY B**B**NZ**B**B CWI RW**B**QP**B**	NCL TKZ NBF	ZKE	AKE	AZZ	ZAA
XYZ	IKW **B**DT**B**OX FPZ W**B**WS**B**G HXB QW**B**AG**B**	RNU LTC JZE	IKW	LMX	CBA	XYZ

Figure 3. Bomba stops for different ring settings and their interpretation.

Experimental evidence suggested it was not the indicators at which the machine stopped that were of importance, but the offset from the starting position at which that occurred. The ring setting could then be directly derived by subtracting this value from AAA.

5. An Authentic Message

To illustrate the full decoding process, the authentic message provided by David Kahn and first published by Cipher A. Deavours and Louis Kruh [5, p. 342] will now be broken using Polish methods and the bomba emulator.[9] It was sent by Generaloberst Walther von Brauchitsch to Heeresgruppenkommando 2 (later Army Group C) at Frankfurt-am-Main on 21 September 1938.

The three parts of the encrypted message read:

```
Fernschreiben H.F.M.No. 563
+HRKM 13617 1807 =
AN HEERESGRUPPENKOMMANDO 2=
2109 -1750 - 3 TLE - FRX FRX - 1TL —172=

~~HCALN U~~QKRQ ~~AXPWT~~ WUQTZ KFXZO MJFOY RHYZW VBXYS IWMMV WBLEB
DMWUW BTVHM RFLKS DCCEX IYPAH RMPZI OVBBR VLNHZ UPOSY EIPWJ
TUGYO SLAOX RHKVC HQOSV DTRBP DJEUK SBBXH TYGVH GFICA CVGUV
OQFAQ WBKXZ JSQJF ZPEVJ RO -

2TL - 166 - ~~ZZWTV S~~YBDO ~~YDTEC~~ DMVWQ KWJPZ OCZJW XOFWP XWGAR
KLRLX TOFCD SZHEV INQWI NRMBS QPTCK LKCQR MTYVG UQODM EIEUT
VSQFI MWORP RPLHG XKMCM PASOM YRORP CVICA HUEAF BZNVR VZWXX
MTWOE GIEBS ZZQIU JAPGN FJXDK I -
```

[9]Frode Weierud has published important corrections to this article on his website [18]. Frank Carter from Bletchley Park has provided a similar account of the Polish methods, which I was not aware of when investigating the bomba, cf. [3]. There is only a minor difference in the calculation of ring settings, his "null" position being ZZZ and mine, AAA.

3 TL - 176 - ~~DHHAO F~~WQQM ~~EIHBF~~ BMHTT YFBHK YYXJK IXKDF RTSHB
HLUEJ MFLAC ZRJDL CJZVK HFBYL GFSEW NRSGS KHLFW JKLLZ TFMWD
QDQQV JUTJS VPRDE MUVPM BPBXX USOPG IVHFC ISGPY IYKST VQUIO
CAVCW AKEQQ EFRVM XSLQC FPFTF SPIIU ENLUW O
=1 ABT GEN ST D H NR. 2050/38 G KDOS +

The Grundstellung chosen by the operator was FRX, and the crossed-out first six letters of each segment represent the encrypted message keys, which constitutes the following indicators:[10]

1. FRX HCALNU
2. FRX ZZWTVS
3. FRX DHHAOF.

Since additional keys for the day in question have not been preserved, the author has generated these using the wheel order, ring setting and Stecker connections of the message.[11] On that day, the Poles could have received the following three females,

4. BOP **A**DD**A**KS
5. KFY I**A**QH**A**U
6. IDB PN**A**OU**A**,

and six further message keys,

7. AAA QZMOMS
8. ABC RQBKQR
9. OKW OQEUMA
10. REX VSERNC
11. NAX DJWLOO
12. KFZ XOHYST.

The Enigma doubles in each of the six bomby (each testing one of the six possible wheel orders) are set to indicators

I. BOP – II. BOS
III. KFZ – IV. KFC
V. IDD – VI. IDG,

and are rotated through all positions while applying current to the letter repeated in the females, A. The machines stop at the indicators shown in Figure 4:

In the first column, the rotor order is found, and in the second, the halting positions of the six Enigmas in the bomba, followed after the arrow by the three couples of identical letters they produce. To calculate the ring settings in the last column from the stop positions, the table in Figure 5 was employed. For the first halt OVO with start position BOP, the first letter of the latter indicator, B (2), needs to be subtracted from O (15), which equals 13. Looking up 13 in the third row of the table, N is

[10]The crossed-out third group in each part was the identification group (“Kenngruppe”) designating the cipher net the dispatch was adressed to. Cf. [10, p. 6f].

[11]Also the indicator generator can be found on the author’s website, http://alpha60.de/research/bomba_krypt/.

obtained. If the difference is negative, the fourth row can be used. Correspondingly, V (22) − O (15) = 7 (T) and O (15) − P (16) = −1 (B) is calculated, which results in ring setting NTB. The Beaufort table Deavours and Kruh provided in their article on the Turing bombe [5, p. 335] represents an equivalent of this procedure.

Wheel order	*Bomba stop and output*	*Ring setting* (AAA – stop + BOP)
123	**OVO** OVR XMY XMB VKC VKF → RREEZZ	**NTB**
132	**MQU** MQX VHE VHH TFI TFL → VVCCFF	**PYV**
	UFH UFK DWR DWU BUV BUY → DDXXZZ	**HJI**
213	**CSM** CSP LJW LJZ JHA JHD → NNJJII	**ZWD**
231	**WVQ** WVT FMA FMD DKE DKH → CCTTJJ	**FTZ**
312	**GJE** GJH PAO PAR NYS NYV → CCFFSS	**VFL**
321	%	%

Figure 4. Bomba results and corresponding ring settings.

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**
0	25	24	23	22	21	20	19	18	17	16	15	14	13	12
0	-1	-2	-3	-4	-5	-6	-7	-8	-9	-10	-11	-12	-13	-14

16	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**
P	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
11	10	9	8	7	6	5	4	3	2	1
-15	-16	-17	-18	-19	-20	-21	-22	-23	-24	-25

Figure 5. Table for the conversion of indicators to ring settings.

Now the message keys of the three segments of the cryptogram (FRX HCALNU, FRX ZZWTVS, FRX DHHAOF) will be deciphered with the different wheel orders and ring settings obtained.[12] By counting how many females arise, it can be determined which of the above alternatives is the most probable one:

	W123, NTB=14,20,2	W132, PYV=16,25,22	W132, HJI=8,10,9	W213, ZWD=26,23,4	W231, FTZ=6,20,26	W312, VFL=22,6,12
FRX HCA LNU	BOV KQO	ALK XRZ	KLY SJS	A**G**U M**G**I	NWK FUY	PLG NRK
FRX ZZW TVS	AJO RMR	ID**R** HL**R**	YFJ RIU	LDF YWZ	PSB OCM	NBC RFW
FRX DHH AOF	JXU BFW	WFL CXK	MIG KUB	**BIN BDN**	JES YSX	FPR DKH
	0	1	0	**3**	0	0

Figure 6. Experimental decipherment of message keys with solutions obtained.

The fourth ring setting and rotor sequence bring forth significantly more letter doublings than the others, which suggests they are the ones sought-after. If needed, more indicators can be included into the test.

[12]Here and in the following I relied on Dirk Rijmenants' excellent Enigma simulator (http://users.telenet.be/d.rijmenants/en/enigmasim.htm) for manual ciphering.

6. Deriving Steckers

Since it is known that the clear text of the key was "something of the form XYZXYZ", the Stecker connections can now be derived by decrypting the indicators received with the ring setting and wheel order just determined. For every sign that does not repeat on positions 1–4, 2–5 and 3–6, there exist two cross-pluggings that establish identity. The input letter that produced the difference needs to be connected to another one that converts to the desired output symbol, equal to the one at the other place. Without plugs, **H**CA**L**NU decrypts to **A**GU**M**GI in Grundstellung FRX. Taking positions 1–4 as example, either H needs to be cabled to U, which produces M in setting FRX (the indicator the machine is at when permuting the first sign), and then **H**CA**L**NU deciphers to **M**GU**M**GI; or L needs to be connected to B, which converts to A in setting FRA (the indicator at the fourth letter), then **H**CA**L**NU decrypts to **A**GU**A**GI. To decide which of the two Stecker connections to plug, we derive the alternatives for all differing symbols in the keys that were received (Figure 7). Due to the reciprocity of Enigma, this can simply be achieved by typing the target letter at corresponding indicators, i.e., by setting the machine to FRX and typing **M**XX**A**XX, resulting in **U**XX**B**XX for the above example.

Basic setting and encrypted message key	*Decrypted message key*	*Plug alternatives*	*Resulting plug*
1.FRX HCA LNU	A**G**U M**G**I	1-4: H-U v L-B	
		3-6: A-E v **U-I**	
2.FRX ZZW TVS	LDF YWZ	1-4: Z-E v T-M	
		2-5: Z-R v V-O	
		3-6: W-R v S-N	
3.FRX DHH AOF	**B**I**N** **B**D**N**	2-5: H-Z v O-J	
4.BOP ADD AKS	**NWO NWO**	%	
5.KFY IAQ HAU	F**J**W V**J**O	1-4: **I-U** v H-I	**I-U**

Figure 7. Deduction of plug alternatives from decryption of message keys.

We find that plug I–U should be set, because it appears twice. The Stecker alternatives converge. Repeating the procedure with the letters exchanged reveals one more junction:[13]

Basic setting and encrypted message key	*Decrypted message key*	*Plug alternatives*	*Resulting plug*
1.FRX HCA LNU	A**GI** M**GI**	1-4: H-I v L-B	
2.FRX ZZW TVS	LDF YWZ	1-4: Z-E v T-M	
		2-5: Z-R v V-O	
		3-6: W-R v S-N	
3.FRX DHH AOF	**B**U**N** **B**D**N**	2-5: H-Z v **O-J**	
5.KFY IAQ HAU	**VJW VJW**	%	
6.IDB PNA OUA	H**ZU** S**ZU**	1-4: P-K v O-X	
7.AAA QZM OMS	PKY YCE	1-4: Q-E v **O-J**	**J-O**

Figure 8. Further deduction of plugs from decryption of message keys.

[13]Here and subsequently, message keys that already decrypt to a repeated identical sequence have been omitted.

We continue the process with Steckers I–U and J–O plugged, realising each connection that appears twice.

Basic setting and encrypted message key	*Decrypted message key*	*Plug alternatives*	*Resulting plug*
1.FRX HCA LNU	AGI MGI	1–4: H–I v L–B	
2.FRX ZZW TVS	LDF YWZ	1–4: Z–E v T–M	
		2–5: Z–R v V–J	
		3–6: **W–R** v S–N	
3.FRX DHH AOF	**BUN BUN**	%	
6.IDB PNA OUA	H**ZU** Q**ZU**	1–4: P–X v O–X	
7.AAA QZM OMS	**P**KY **P**CE	2–5: Z–L v M–N	
		3–6: M–V v S–I	
8.ABC RQB KQR	H**S**S A**S**V	1–4: **R–W** v K–M	**R–W**
Cycle IV.			
1.FRX HCA LNU	AGI MGI	1–4: H–I v L–B	
2.FRX ZZW TVS	LD**Z** YR**Z**	1–4: Z–E v T–M	
		2–5: Z–W v V–J	
6.IDB PNA OUA	H**ZU** Q**ZU**	1–4: P–X v O–X	
7.AAA QZM OMS	**P**KY **P**CE	2–5: Z–L v M–N	
		3–6: **M–V** v S–I	
8.ABC RQB KQR	**AS** **AS**D	3–6: B–L v R–E	
9.OKW OQE UMA	**L**RL**L**LD	2–5: Q–G v **M–V**	**M–V**
Cycle V.			
1.FRX HCA LNU	AGI V**GI**	1–4: H–I v L–B	
2.FRX ZZW TVS	LD**Z** YL**Z**	1–4: **Z–E** v T–V	
		2–5: **Z–E** v V–J	**E–Z**
Cycle VI.			
1.FRX HCA LNU	AGI V**GI**	1–4: H–I v **L–B**	
2.FRX ZZW TVS	**YLE YLE**	%	
6.IDB PNA OUA	H**EU** Q**EU**	1–4: P–X v O–X	
7.AAA QZM OMS	**PYZ PYZ**	%	
8.ABC RQB KQR	**AS** **AS**D	3–6: **B–L** v R–Z	**B–L**
Cycle VII.			
1.FRX HCA LNU	**AGI AGI**	%	
6.IDB PNA OUA	H**EU** Q**EU**	1–4: **P–X** v O–X	
8.ABC RQB KQR	**ASD ASD**	%	
12.KFZ XOH YST	S**AM** I**AM**	1–4: **X–P** v Y–Z	**P–X**
Cycle VIII.			
1.FRX HCA LNU	**AGI AGI**	%	
2.FRX ZZW TVS	**YBE YBE**	%	
3.FRX DHH AOF	**LUN LUN**	%	
4.BOP ADD AKS	**NRJ NRJ**	%	
5.KFY IAQ HAU	**MOR MOR**	%	
6.IDB PNA OUA	**QEU QEU**	%	
7.AAA QZM OMS	**XYZ XYZ**	%	
8.ABC RQB KQR	**ASD ASD**	%	
9.OKW OQE UMA	**BRD BRD**	%	
10.REX VSE RNC	**DUM DUM**	%	
11.NAX DJW LOO	**SPD SPD**	%	
12.KFZ XOH YST	**IAM IAM**	%	

Figure 9. Further deduction of plugs.

At this point, all sequences decrypt to doubled indicators in clear, all Stecker connections are found, and in combination with the rotor sequence and the ring settings already obtained, all dispatches of the day can be deciphered. The message keys of the three segments of the cryptogram, HCA LNU, ZZW TVS and DHH AOF, now decode to AGI AGI, YBE YBE and LUN LUN, and when the machine is set to AGI, the letters that follow the key,

QKRQ WUQTZ KFXZO MJFOY RHYZW VBXYS IWMMV WBLEB DMWUW BTVHM RFLKS DCCEX IYPAH RMPZI OVBBR VLNHZ UPOSY EIPWJ TUGYO SLAOX RHKVC HQOSV DTRBP DJEUK SBBXH TYGVH GFICA CVGUV OQFAQ WBKXZ JSQJF ZPEVJ RO,

are transformed to readable German:

AUFBE FEHLD ESOBE RSTEN BEFEH LSHAB ERSSI NDIMF ALLEX ZXZTX UNWAH RSCHE INLIC HENXF RANZO ESISQ ENANG RIFFS DIEWE STBEF ESTIG UNGEN JEDER ZAHLE NMAES SIGEN UEBER LEGEN HEITZ UMTRO TZZUH ALTEN X.

The same is true of the other parts of the message, which decrypt to

FUEHR UNGUN DTRUP PEMUE SSENV ONDIE SEREH RENPF LIQTD URQDR UNGEN SEINX ABSXD EMGEM AESSB EHALT EIQMI RDIEE RMAEQ TIGUN GZURP UFGAB EDERB EFEST IGUNG ENODE RAUQV ONTEI LENAU SDRUE CKLIQ

and

PERSO ENLIQ VORXA BSXAE NDERU NGDER ANWEI SUNGX OKHXG ENXST XDXHX ERSTE ABTXN RXDRE IDREI ZWOEI NSXDR EIAQT GXKDO SXVOM JULIE INSNE UNDRE IAQTB LEIBT VORBE HALTE NXDER OBERB EFEHL SHABE RDESH EERES,

respectively, and this results in the following text in clear:

Fernschreiben H.F.M.No. 563
+HRKM 13617 1807−
AN HEERESGRUPPENKOMMANDO 2=
2109 −1750
Auf Befehl des Obersten Befehlshabers sind im Falle z. Zt. unwahrscheinlichen französischen Angriffs die Westbefestigungen jeder zahlenmäßigen Überlegenheit zum Trotz zu halten.
Führung und Truppe müssen von dieser Ehrenpflicht durchdrungen sein.
Demgemäß behalte ich mir die Ermächtigung zur Aufgabe der Befestigungen oder auch von Teilen ausdrücklich persönlich vor.
Änderung der Anweisung OKH/Gen/St/D/H Erste Abt. Nr. 3321/38 G KDos vom Juli 1938 bleibt vorbehalten. Der Oberbefehlshaber des Heeres.
=1 ABT GEN ST D H NR. 2050/38 G KDOS +[14]

[14]Translation: The Commander-in-Chief orders as follows: In the case of French attacks on the Western fortifications, although unlikely at this moment, those fortifications must be held at all costs, even against numerically superior forces. Commanders and troops must be imbued with the honor of this duty. Accordingly, I emphasize that I alone have the right to authorize the fortifications to be abandoned in whole or part. I reserve the right to make changes to order OKH/Gen/St/D/H 1. Abt. Nr. 3321/38 G KDos of July 1938. The Commander-in-Chief of the Army.

Content and style of this message are quite unexpected, as it was issued well before the war, when the fortification of the Siegfried line was still under construction and no imminent threat had to be expected from the French army. On the very same day though, the delegates of England and France had declared in Prague that if the Czechoslovaks continued to refuse ceding the Sudetenland to Germany, they would be responsible for a war in which the western countries would not participate, forcing president Eduard Benesch to comply with Hitler's demands. The German High Command might have suspected this was a ruse.

The event is documented in the papers of Sir Eric Phipps, the British ambassador in Paris: "Phipps tel., 21 September 1938, 5.5 p.m. The Czechoslovak Government replied on 21 September that, 'under the pressure of urgent insistence culminating in (the) British communications of 21 September', they 'sadly accept(ed) the French & British proposals'." [6, p. 218, n. 52] The Enigma message was transmitted 45 minutes later.

7. Examples by Rejewski

Using the same procedure, the earliest example by Rejewski mentioned above will be investigated to find out if it is authentic, that is, was produced on a replica Enigma. It provides the following females

1. GKD **W**AV **W**HA
2. JOT I**W**A B**W**N
3. MDO OT**W** YZ**W**

and these further keys:

4. KTL WOC DRB
5. SVW KKM IYS
6. EDC DSP LJC
7. BWK **T**CA **T**OC
8. GRA FDR YWD
9. KJC B**S**W R**S**E
10. SGF TEY ASR
11. AGH MD**F** RL**F**
12. JBR WLT SOQ.

The bomby are set up with the following offsets

I. GKD – II. GKG
III. JOU – IV. JOX
V. MDQ – VI. MDT,

and letter W is continuously input while rotating through all possible positions. They stop at the following wheel orders and indicators, resulting in ring settings:

Wheel order	*Bomba stop and output*	*Ring setting* (AAA – stop + BOP)
123	**QBG** QBJ TFX TFA WUT WUW → RRHHMM	**QJX**
132	**OUV** OUY RYM RYP UNI UNL → IIKKYY	**SQI**
213	%	
231	**RED** REG UIU UIX XXQ XXT → LLRRDD	**PGA**
312	**IDG** IDJ LHX LHA OWT OWW → AAAALL	**YHX**
	IQS IQV LUJ LUM OJF OJI → UUMMJJ	**YUL**
	AUY AUB DYP DYS GNL GNO → RRSSSS	**GQF**
321	%	

Figure 10. Bomba results with corresponding ring settings for Rejewski example.

Decrypting the message keys suggests the first rotor sequence and ring setting should be further investigated:

	W123, QJX=17,10,24	W132, SQI=19,17,9	W231, PGA=16,7,1	W312, YHX=25,8,24	W312, YUL=25,21,12	W312, GQF=7,17,6
KTL WOC DRB	LT**S** BA**S**	SJB ATQ	PWO SPS	NLV CSH	GFR WLP	DUG THF
SVW KKM IYS	SZH NUJ	GAT VBK	WPV CWH	PI**K** HW**K**	RCK HJH	BIF DOC
EDC DSP LJC	UVB JHV	GCK HHD	BPD IRO	KEA JNI	YDG EVF	CAD THM
GRA FDR YWD	JLY LZB	MXQ VKE	EPO OKQ	ZPE DNR	SNU DLC	NVH ORN
SGF TEY ASR	**M**WU **M**XB	GJU WIW	ZCU XBA	KUP JXQ	BUV ITO	WIP RKO
JBR WLT SOQ	HGL OND	LFA EKO	CID OQI	REO ALE	TVX JND	VJV BGT
BWK TCA TOC	WHZ HBP	HBX VHJ	WBU HML	JPJ LQL	CLJ HPS	LNE XQL
KJC BSW RSE	SQI XNQ	GRG JQV	VTH SHR	NPI YDB	QZG MRH	GZZ BWD
AGH MDF RLF	E**I**J G**I**X	XRS BTQ	OAP JMT	UU**S** DR**S**	Z**W**J Y**W**H	YSU WCK
	3	0	0	2	1	0

Figure 11. Experimental decipherment of message keys with solutions obtained.

But the deduction of Stecker alternatives does not converge:

Basic setting and encrypted message key	*Decrypted message key*	*Plug alternatives*	*Resulting plug*
1.GKD **W**AV **W**HA	**R**IO **R**NB	2-5: A-V v H-B	
		3-6: V-F v A-H	
2.JOT I**W**A B**W**N	ZHS TAH	1-4: **I-A** v B-Y	
		2-5: W-F v W-G	
		3-6: A-N v N-M	
3.MDO OT**W** YZ**W**	WI**M** AV**M**	1-4: O-B v Y-D	
		2-5: T-B v Z-G	
7.BWK **T**CA **T**OC	WHZ HBP	1-4: T-P v T-U	
		2-5: C-Y v O-Z	
		3-6: **A-I** v C-J	**A-I**
Cycle II			
1.GKD **W**AV **W**HA	**R**IO **R**NN	2-5: A-V v **H-R**	
		3-6: V-Z v A-H	
2.JOT I**W**A B**W**N	**T**HO **T**IH	2-5: W-F v W-G	
		3-6: A-N v N-F	
3.MDO OT**W** YZ**W**	WA**M** IV**M**	1-4: O-B v Y-D	
		2-5: T-B v Z-G	
7.BWK **T**CA **T**OC	WH**P** HB**P**	1-4: T-P v T-U	
		2-5: C-Y v O-Z	
9.KJC B**S**W R**S**E	SQA XNQ	1-4: B-M v R-Q	
		2-5: S-V v S-T	
		3-6: W-T v E-Z	
11.AGH MD**F** RL**F**	E**A**J G**A**X	1-4: M-X v **R-H**	**H-R**

Figure 12. Deduction of plug alternatives from decryption of message keys.

Cycle III			
1.GKD **W**AV **W**HA	**HI**O **HI**N	3-6: V-Z v A-R	
2.JOT I**W**A B**W**N	**T**RO **T**IR	2-5: W-F v W-G	
		3-6: A-N v N-F	
3.MDO OT**W** YZ**W**	WA**M** IV**M**	1-4: O-B v Y-D	
		2-5: T-B v Z-G	
7.BWK **T**CA **T**OC	WR**P** RB**P**	1-4: T-P v T-U	
		2-5: C-Y v O-Z	
9.KJC B**S**W R**S**E	SQA TNQ	1-4: B-U v R-Q	
		2-5: S-V v S-T	
		3-6: W-T v E-Z	
11.AGH MD**F** RL**F**	**EA**J **EA**X	3-6: F-I v F-I	
4.KTL WOC DRB	LT**S** BU**S**	1-4: W-A v D-R	
		2-5: O-G v R-J	**?**

Figure 12. Continued.

Rejewski obviously created a fictitious example as a mere illustration of the decoding process.[15]

8. Hardware

Concerning the hardware of the device, among others, one inconsistency stands out: if the same letter was input into each of the three pairs of Enigmas that made up the machine, why are there three columns of switches on the outside, each representing a full alphabet (cf. Fig. 1)? They would have permitted to enter different characters into each couple. Perhaps Rejewski planned a more general procedure that worked with all females, no matter which letter repeated, like the sheet method invented by Zygalski [15, p. 287ff].[16] He might only have realised in practical experiment with the machine that the same sign needed to be entered, because it was less probable that a single symbol was changed on the plug board. And even if he was not sure that the procedure would work, the bomby could be tried in case only females with different letters had been received, with a slight chance that they would produce the right ring setting. Designing the artefact more general than necessary could have permitted to counter the next change of procedure by the Germans without having to build new hardware. When Alan Turing devised the British version of the device in 1940, the ''bombe'', he successfully followed the same principle, anticipating that the doubling of the message keys on which all Polish methods relied would be given up shortly after [19, p. 81].

The diagram in Figure 13 tentatively depicts the circuitry within the bomba. For the sake of simplicity, it has been reduced to only four letters. The motor at the bottom of the picture drives the six Enigmas on top via a planetary gear (not shown). As in the encryption device, closing the manual switches mechanically disconnects the corresponding contact of the rotor from the relay below, preventing it to be activated immediately.

[15]I have also tried to solve the example with reflectors A and C, with the same result. Also the second set of message keys Rejewski provided has been investigated and found not to be authentic. The full report is located on the author's website, http://alpha60.de/research/bomba_krypt/.

[16]Tony Sale has published a working simulator of the sheets method online, cf. [16].

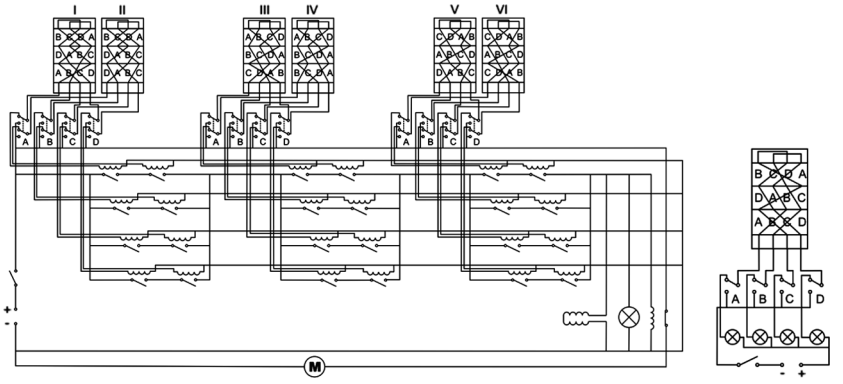

Figure 13. Circuitry of a reduced version of the bomba in comparison with a reduced version of Enigma.

The couples of Enigmas in the simplified bomba are set up with an offset of three:

```
I.   BDA – II. BDD
III. ABC – IV. ABB
V.   CAD – VI. CAC.
```

This setup could be based on the following females (3-letter Grundstellung and 6 letters encrypted message keys):

1. BDA **B**AD**B**CA
2. ABB A**B**DC**B**A
3. CAB AD**B**CA**B**.

The repeating letter in the females, B, is switched on in all three couples. In the first rotor position, the following relays close (cf. Figure 14):

```
I/II   : A–D
III/IV: D–C
V/VI   : C–D.
```

Nothing further happens. If, however, each of the three couples of Enigmas produces two identical letters, the circuit closes. This activates the horseshoe magnet, lights the lamp and opens the relay at the bottom right, disconnecting the motor from current. If the on/off switch at the bottom left is toggled, all relays in the middle are released and the system returns to its initial state.

The mysterious double solenoid visible in Rejewski's sketch close to the main axle shaft has been included into the circuitry, even though its function remains mysterious. It might have been part of a clutch mechanism to disengage the motor, or part of a system that produced the end result of the operation – the ring setting sought-after. A hardware equivalent of the above calculation would be a simple three-wheel counter stepping backwards from AAA each time the rotors of the apparatus moved forward. This complement would reinforce the device's similarity to a time bomb, which also counts down.

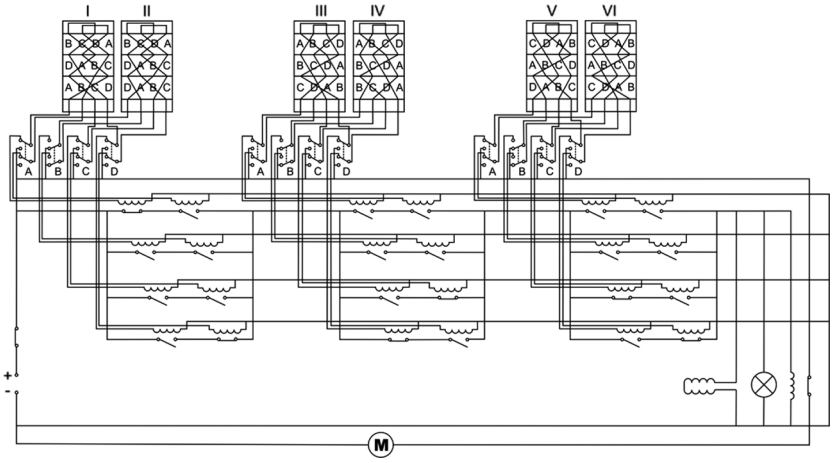

Figure 14. Reduced version of the bomba with current applied.

Acknowledgments

The author is indebted to Ralph Erskine and John Gallehawk for providing scans of the Zyklometer schematic, to David Hamer for sharing his photos of the Polish Enigma double, to John Harper for a hands-on introduction into the stopping mechanism of the Turing bombe, to Klaas Henschel for help on technical details, to Anna Ucher for translating relevant parts of Rejewski's accounts from Polish, and to Frode Weierud and an anonymous reviewer for most helpful criticism and suggestions on an earlier version of this article.

About the Author

David Link is a machine theorist, artist and programmer based in Cologne, Germany. In 2004, he took his PhD in philosophy at Humboldt-University, Berlin, and the Academy of Arts and the Media, Cologne, with a thesis on text generating algorithms in the early years of computer development (''Poetry Machines/Machine Poetry''). His current research focuses on the convergence of mathematics and engineering in the early 20th century. He recently reconstructed Christopher Strachey's ''Loveletters'' algorithm from 1952, by writing an emulator of the Ferranti Mark 1. His work ''Poetry Machine'' (2001), an interactive text generator based on semantic networks, is part of the permanent collection at the Centre for Art and Media Technology ZKM, Karlsruhe. More information can be found on his website, http://alpha60.de.

References

1. Anonymous (Commander Howard T. Engstrom?). 11 October 1943. Note on Early Bombe History, ed. Frode Weierud. National Archives and Records Administration, RG 457, NSA Historical Collection, Nr. 1736, CBLH17, Box 705. http://frode.home.cern.ch/frode/crypto/Enigma/BombeHistNote.pdf (accessed March 5, 2009).
2. Bauer, Friedrich L. 2000. *Decrypted Secrets. Methods and Maxims of Cryptology*. Berlin: Springer.

3. Carter, Frank. July 1999. The First Breaking of Enigma. Some of the Pioneering Techniques Developed by the Polish Cipher Bureau. Bletchley Park Report No. 10. Milton Keynes: Bletchley Park Trust.
4. Copeland, B. Jack. 2004. Enigma. In *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life*, edited by B. J. Copeland, Oxford: University Press, pp. 217–264.
5. Deavours, Cipher A. and Kruh, Louis. 1990. "The Turing Bombe: Was It Enough?", *Cryptologia*, 14(4):331–349.
6. Herman, John. 1998. *The Paris Embassy of Sir Eric Phipps: Anglo–French Relations and the Foreign Office 1937–1939*. Sussex: Academic Press.
7. Johnson, Brian. 1978. *The Secret War*. London: BBC.
8. Kozaczuk, Władysław. 1984. *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two*, C. Kasparek, trans., Frederick, MD: University Publications of America.
9. Lisicki, Tadeusz. 1979. Appendix. In *Intercept. The Enigma War edited by Józef Gárlinski*, London: Dent, pp. 192–204.
10. Oberkommando der Wehrmacht (OKW). 13 January 1940. *Schlüsselanleitung zur Schlüsselmaschine Enigma*, H.Dv.g. 14. http://www.ilord.com/enigma-manual1940-german.pdf (accessed March 5, 2009).
11. Rejewski, Marian. ~1940. Enigma 1930–1940. Metoda i historia rozwiązania niemieckiego szyfru maszynowego (w zarysie) ("Enigma 1930–1940. Method and history of the solution of the German cipher machine (in outline)"). Thirty-two page typescript, in Polish. http://www.spybooks.pl/en/enigma.html (accessed March 5, 2009). The material on this website originates from the private files of Col. Władysław Kozaczuk (Rafal Brzeski, personal communication, 3 April 2007).
12. Rejewski, Marian. 1979. Matematyczne podstawy konstrukcji bomb kryptologicznych oraz uwagi o ich wykorzystaniu w Polsce i w Wielkiej Brytanii. Informacje o pierwszym komputerze na świecie ("The mathematical foundation of the construction of the cryptologic bombs and notes on their employment in Poland and England. Informations on the first computer of the world"). Two-page typescript, in Polish, probably in preparation for Kozaczuk's book [8]. http://www.spybooks.pl/en/enigma.html.
13. Rejewski, Marian. 1980. "Jak matematycy polscy rozszyfrowali Enigmę" ("How Polish mathematicians broke the Enigma cipher"), *Wiadomości Matematyczne*, 23(1):1–28. In Polish. English translation: How the Polish Mathematicians Broke Enigma, Appendix D. In [8], 246–271.
14. Rejewski, Marian. 1982. "Remarks on Appendix 1 to British Intelligence in the Second World War by F. H. Hinsley", *Cryptologia*, 6(1):75–83. The Polish original, Uwagi do Appendix 1: The Polish, French and British Contributions to the Breaking of the Enigma książki: British Intelligence in the Second World War prof. F.H. Hinsley'a [*sic*], can be found at http://www.spybooks.pl/en/enigma.html.
15. Rejewski, Marian. 1984. "The Mathematical Solution of the Enigma Cipher". Appendix E. In [8], 272–291.
16. Sale, Anthony. "Virtual Bletchley Park", http://www.codesandciphers.org.uk/virtualbp/poles/poles.htm (accessed March 5, 2009).
17. Ulbricht, Heinz. 2005. Chiffriermaschine Enigma. Trügerische Sicherheit. Ein Beitrag zur Geschichte der Nachrichtendienste. Ph.D. diss., Technical University Braunschweig. http://www.digibib.tu-bs.de/?docid=00001705 (accessed March 5, 2009).
18. Weierud, Frode. 1998. German Army Enigma Message. http://frode.home.cern.ch/frode/crypto/Enigma/tbombe.html (accessed March 5, 2009).
19. Welchman, Gordon. 1982. *The Hut Six Story. Breaking the Enigma Codes*. New York: McGraw-Hill.