Spanish Enigma: A History of the Enigma in Spain

by

José Ramón Soler Fuensanta, Francisco Javier López-Brea Espiau, and Frode Weierud

The definitive version was published in Cryptologia, Volume 34, Issue 4, October 2010.

DOI:10.1080/01611194.2010.485414 (http://dx.doi.org/10.1080/01611194.2010.485414).

To cite this article: Fuensanta, José Ramón Soler, Espiau, Francisco Javier López-Brea and Weierud, Frode (2010) 'Spanish Enigma: A History of the Enigma in Spain', Cryptologia, 34: 4, 301−328.

Page intentionally blank.

Spanish Enigma: A History of the Enigma in Spain

José Ramón Soler Fuensanta[1], Francisco Javier López-Brea Espiau[2], Frode Weierud[3]

ADDRESS:
(1) C/ Aragón 100, 07800 Ibiza (Balearic Islands), Spain. Email: j.ramon.soler@terra.es
(2) C/ Vitruvio 1, 28006 Madrid, Spain. Email: jlopezbrea@oc.mde.es.
(3) Le Pre Vert, 1041 Rte de Mategnin, F-01280 Prevessin-Moens, France. Email: frode.weierud@cern.ch, WWW: http://cryptocellar.org/

ABSTRACT: The presentation of a brief study of the use of Enigma Machines in Spain, during the Spanish Civil War (1936-1939) and later, until their final replacement.

KEYWORDS: Enigma machine, Spanish Civil War, Spain.

1. Introduction

The birth and commercialization of cipher machines represented a revolution in the history of cryptography. These machines provided greater security and strength to encryption systems, and at the same time avoided one of the main problems of manual ciphers, continuous errors in the process of encryption and decryption. Amongst these, the Enigma machine, which made its public appearance in 1923 [1], was particularly relevant. One of its most notable features was the reversibility of the cipher produced; the same machine was capable of ciphering and deciphering, all that was required was the correct setting up of the machine.

We know the history of the Enigma from the early models [30;17] until the end of its life span. Many of the models are well documented, however from time to time information appears in the archives about one particular model with no apparent success in the commercial or military markets, but nevertheless interesting from the point of view of the machine's evolution. For example, this is the case of the model Z discovered by professor Quirantes in the Archive of the Spanish Ministry of Foreign Affairs [22]. Two models of this machine were manufactured; one with pawl drive and the other with cog-wheel drive. Only a small number of these machines were sold, mainly to Sweden and Chile.[1]

The history of the Enigmas in Spain dates back to 1931 when the Spanish Ministry of State, the equivalent of today's Ministry of Foreign Affairs, made a request to the Spanish Embassy in Berlin with regards to the cipher machines used in Germany. However, we have to wait until 1936, when General Franco bought ten Enigma machines to protect nationalist military and diplomatic communications, before the first machines arrived in Spain [25]. Eventually the machines were all transferred to the military forces because the diplomats were more familiar with their codebooks [27].[2]

The nationalist forces in the Spanish Civil War used commercial Enigma machines with serial numbers in the A and K series; surprisingly, the rotors from some of the first ten machines acquired are labelled with the numbers of all the machines, not

[1] "Enigma Machines in Foreign Countries," TICOM translation of a German document addressed to OKH/Chef H Rüst u. BdE/AHA/In 7 IV and dated Berlin, 3 Sept. 1943; TICOM/DF-190-AM. The document is part of [13] that was released under a NSA FOIA request.

[2] As a curious note, the staff of the Secretariat of State transferred their Enigma to the General Staff's Cipher Department each month to have the internal settings of the machine changed.

only with the number of the machine itself .[3] There are a small number of military Enigmas with plugboard (*Steckerbrett*) in Spain,[4] presently we don't know the exact moment when they arrived but the serial numbers indicate that it must have been in or after 1943.

2. The patents

Searching for information about the Enigma in the Spanish Patent Office we find three patents related to the machine:[5]

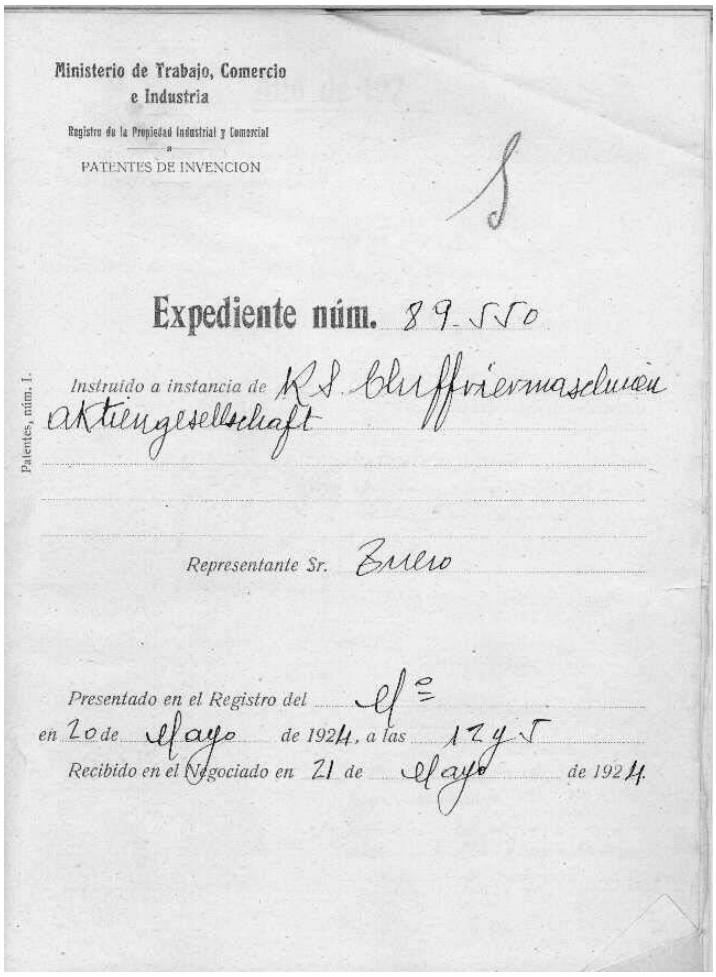
- The patent no. 89546 registered on 19 May 1924 by Mr. Bueno in the name of Naamlooze Vennootschap Ingenieursbureau "Securitas". This is the same patent as the one registered in Great Britain in 1923 under the number 193035.
- The patent no. 89550 registered on 20 May 1924 by Mr. Bueno in the name of Chiffriermaschinen Aktiengesellschaft.[6]
- The patent no. 89611 registered on 24 May 1924 by Mr. Bueno in the name of Naamlooze Vennootschap Ingenieursbureau "Securitas". This one looks like the Enigma A model.

[3] In [27] we can see one photograph of some rotors labelled "A 1232–1235, K 203–K 208", the numbers of the first ten machines purchased by the nationalist forces. The rotors were in the K 296 machine. The mix of rotors is frequent in the Spanish Enigmas. Curiously, the A 1232 and the K 205 have their rotors labelled only with the number of the machine.

[4] There are some German military machines in Spain, the A 17314S, A 17315S, A 17316S and A 16101. These machines were perhaps used by the German/Spanish intelligence liaison or by the German intelligence in Spain. The existence of the G 316, an *Abwehr* machine, seems to confirm this hypothesis. At the end of the war all the German institutions in Spain were registered by FBI personnel [21, p. 57]. At least two Enigma machines were recovered by the Americans [21, p. 341]. The same day the war in Europe was over, 7 April 1945, the Ministry of Foreign Affairs received a note from the United States embassy in Madrid. The note requested that all German official buildings and dependencies be closed and kept under surveillance. The German personnel were kept under surveillance too. The seals were officially in place on May 8 and the official handover to the Allies took place on the twelfth of the next month. The Spanish authorities did not maintain a strict control and much documentation and material disappeared. In some cases the Spanish authorities broke the seals and seized material and documents. At least some material was removed from the Nazi Party press office, the offices of the paymaster of the *División Azul* (DA – The Blue Division), the official German news agency – *Deutsches Nachrichtenbüro* (DNB) and the German consulates in Vigo and Bilbao.

[5] There is a fourth Spanish patent from Scherbius & Ritter, number 89432, which is for an electrical typewriter machine but not a cipher machine.

[6] The patent number 89550 has a German patent application dated 17 January 1924. The German patent number is 407804. The German Patent Office shows that the application for patent 407804 was registered on 18 January 1924 and published on 22 August 1925. This information is also given in Siegfried Türkel's book [30].



Ministerio de Trabajo, Comercio e Industria

Registro de la Propiedad Industrial y Comercial

PATENTES DE INVENCION

Expediente núm. 89.550

Patentes, núm. I.

Instruido a instancia de K.S. Chiffriermaschinen aktiengesellschaft

Representante Sr. Bueno

Presentado en el Registro del ...

en 20 de Mayo de 1924, a las 12 y 5

Recibido en el Negociado en 21 de Mayo de 1924.

Figure 1. The first page of the patent 89550. Source: Spanish Patent Office Archive.

The patent number 89550 is possibly a pre-Enigma model patented in Spain by the Chiffriermaschinen Aktiengesellschaft, but with only one function, either cipher or decipher. Consequently, to communicate two machines were necessary. This patent is identical to the patent described in Türkel's book [30, p. 94].

Figure 2 shows a schematic view of the machine obtained from the patent description. This model has some similarities to model C,[7] but from the figures shown in this document, we can see there are only two rotors labelled with the numbers 1 to 28.

[7] This model is a development that preceded the first *Enigma Glühlampen-Chiffriermaschine*. The need for two machines at both ends convinced the company that a turn-around switch was needed; this was solved by inventing the reflector.

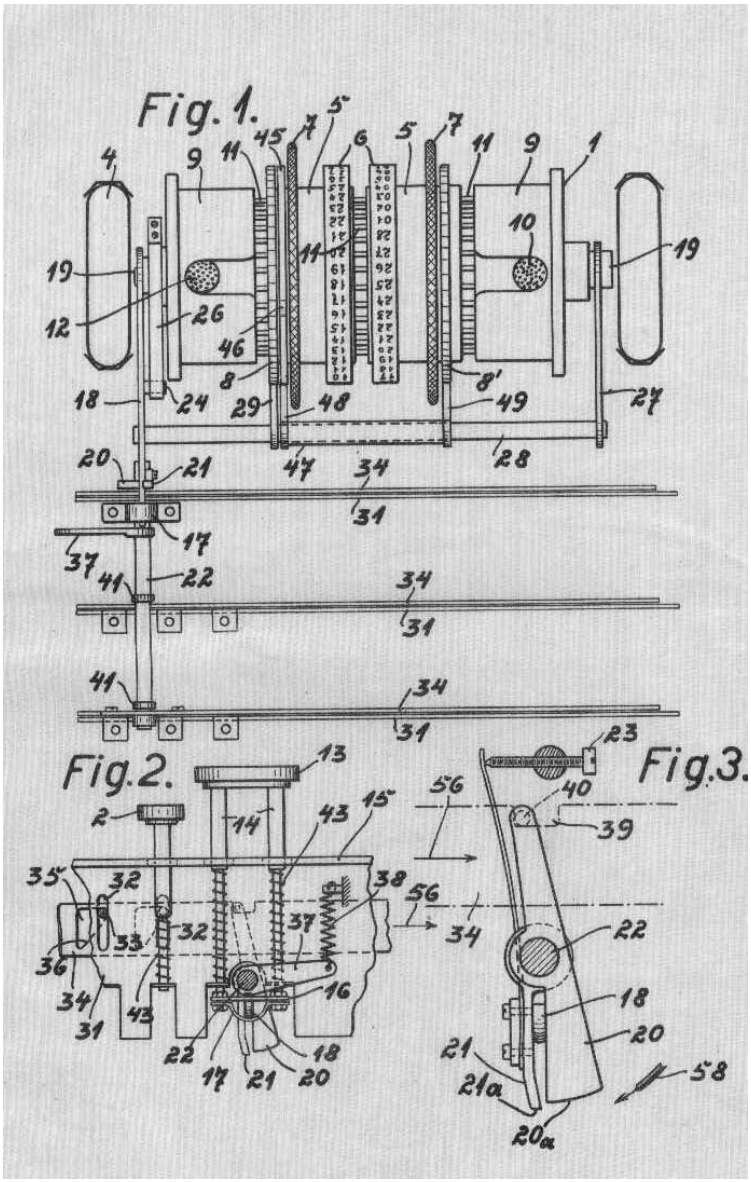


Figure 2. Detail of the machine. Source: Spanish Patent Office Archive.

The security offered by this model, a reduced Enigma machine, was inferior to that of the military and commercial Enigma because the period of the key was reduced to just 784. Not sufficient security for military and diplomatic applications, but perhaps enough for the commercial market and surely cheaper to purchase. We don't know if this machine was fabricated, but probably not. It was most likely a prototype destined for the commercial market that was never commercialised.

3. The military use of the machine

The Enigma was used by the Italian, German and nationalist forces in the Spanish Civil War from November 1936 until the end of the war [25]. When the civil war finished they continued to be used by the Spanish military forces until the mid 1940s, and by the military attachés in France, Rome and Berlin from 1941 onwards. At the end of the Second World War they were slowly replaced by Hagelin machines.

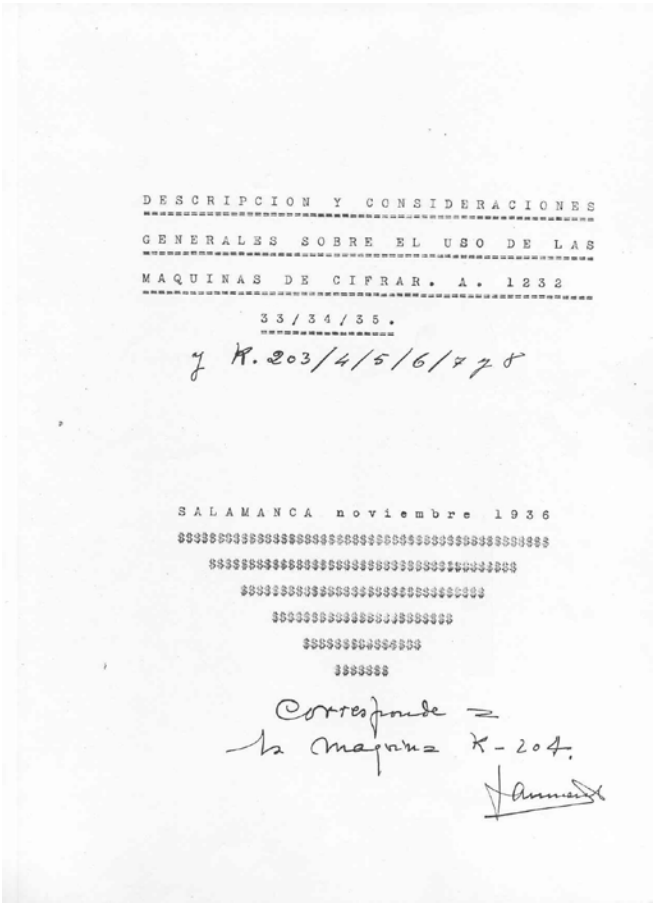


Figure 3. Front page from the Enigma Manual used by the nationalist forces.

The German, Italian and nationalist naval forces used the Enigma machines in combination with a codebook named DEI, an acronym of Deutschland, España, Italia (Germany, Spain and Italy). The Enigmas used by the Italian forces are shown in Figure 4 [4].

A 1236[8]	Italian Naval Ministry, Rome.
K 238	Italian Naval Ministry, Rome.
K 241	Ship docked in Palma in Mallorca. Later delivered to the ship commanding the naval group.
K 234	Italian Naval Mission in Cadiz, Cipher Department.
K 235	Italian Naval Mission in Burgos, Cipher Department.
A 1238	Italian Naval Mission in Palma of Mallorca, Cipher Department.
K 297[9]	Italian Naval Mission in Logroño, Cipher Department.
A 1250	Italian Naval Mission in Barcelona in 1939.

Figure 4. The Italian Enigma machines used in the Spanish Civil War.

[8] It is known that the three machines A 1236, A 1238 and A 1250 were wired with wiring D, Dora; see below. It is therefore likely that also the other machines in this group have the same wiring.

[9] The history of this machine is somewhat convoluted. The machine, which must have been on wiring D, was most likely Italian, but it could also have been a Spanish machine on loan to the Italians. As we will see later the machine turns up in the *Abwehr* communications and there it is said to have been returned to Berlin. Today there is no trace of this machine in Spain.

The Italians did not only use the Enigma machine, they used Hagelin machines as well, probably the model C38 [8]. When the Spanish Civil War was over they considered the purchase of Enigma machines because the agreement was to return all of the existing Enigma machines to Germany. However, the Communications Section of the Naval Ministry in Rome had a preference for the Hagelin machines and decided in their favour in spite of the fact they considered the Enigma machines more robust and superior from a cryptographic point of view.[10]

The nationalist naval forces received two Enigma machines on 28 January 1937 [14]; the only Spanish naval Enigma serial number we know is K 298 that was delivered to the Navy General Staff by the Italian Naval Mission [4]. The number of Enigma machines used by the naval forces is unknown at present, but probably it was very small, two or three machines at the most. The largest number of machines was assigned to the nationalist Army. The distribution of those machines on 30 November 1937 is shown in Figure 5 [2].

Destination
General Franco's Headquarters in Burgos
Headquarters in Salamanca
Operations in General Franco's Headquarters
Tenerife High Command
Majorca High Command
Armed Forces in Morocco
Madrid Army Corps
Galicia Army Corps
Navarre Army Corps
Morocco Army Corps
Castile Army Corps
Aragón Army Corps
6th Military Region
7th Military Region

Figure 5. Spanish forces equipped with Enigma machines on 30 November 1937.

A year later, in December 1938, the distribution was as shown in Figure 6 [27].

Destination	**Machine number**
Cipher Cabinet of General Franco's Headquarters	K 202[11]
General Franco's Headquarters	A 1235[12]
"Terminus"[13] Headquarters	K 204
North Army	A 1232
Centre Army	K 290
South Army	A 1234
East Army	K 207
Aragón Army Corps	K 291
Galicia Army Corps	K 208
Castile Army Corps	K 292
Navarre Army Corps	K 293

[10] Letter of 10 May 1939 sent from Rome to the Head of Service of the Italian Naval mission in Cadiz. Partially reproduced in [4].
[11] This machine has rotors with wiring F. These special wirings are described in detail below.
[12] A 1232, A 1233, A 1234 and A 1235 were all using wiring C.
[13] This was the name of General Franco's mobile Headquarters.

Morocco Army Corps	K 295
1st Army Corps	K 288
Head of Air Forces	K 287
Chief of the Armed Forces in Morocco	A 1233
General Command of the Balearic Islands	K 205
6th Military Region	K 296
7th Military Region	K 206
General Command of the Canary Islands	K 289
Reserve	K 294

Figure 6. Distribution of Enigma machines in December 1938.

Figure 7 shows the distribution of the Army machines in July 1939, a few months after the civil war was over.

Authority	**Destination**	**Machine number**
General Franco's Headquarters	Burgos	A 1235
General Franco's Headquarters	"Terminus"	K 204
Secretariat of the Minister of Defence	Burgos	A 1232
Staff 1st Military Region	Madrid	K 290
Staff 2nd Military Region	Seville	A 1234
Staff 3rd Military Region	Valencia	K 208
Staff 4th Military Region	Barcelona	K 207
Staff 5th Military Region	Zaragoza	K 291
Staff 6th Military Region	Burgos	K 296
Staff 7th Military Region	Valladolid	K 206
Staff 8th Military Region	La Coruña	K 293
Head of the Air Forces	Madrid	K 287
Chief of the Armed Forces in Morocco	Ceuta	A 1233
General Command of the Balearic Islands	Palma de Mallorca	K 205
General Command of the Canary Islands	Santa Cruz de Tenerife	K 289

Figure 7. Distribution of machines at the end of the civil war in July 1939.

It is possible that the number of machines acquired grew; at least we know that machines with different numbers were given to the Embassies. On 22 June 1940 the High Command delivered four machines to the Cipher Department of the Ministry of Foreign Affairs as shown in Figure 8.

Machine Number	**Destination**
K 202	Cipher Department of Ministry of Foreign Affairs
K 295	Spanish Embassy in France
A 1241[14]	Spanish Embassy in Rome
A 1242	Spanish Embassy in Berlin

Figure 8. Enigma machines used by the Spanish Ministry of Foreign Affairs.

Shortly thereafter the machines were sent to their respective destinations. On 2 July an order was given to send the machine to the Embassy in Berlin. Although normally under the responsibility of the military Attaché, the encryption was usually

[14] The machines A 1241, A 1242 and K 202 are known to have wiring F. It is therefore likely that K 295 also has wiring F.

performed by the Naval Attaché, Manuel Espinosa, and his deputy, Miralles de Imperial, the reason being that the Navy was in charge of the embassy radio station.

It is known that encrypted communications between the General Staff of the Army and the Spanish Volunteer Division, the Blue Division, were deciphered by the British, in particular by the Knox group [16;5]. In fact, it is not surprising since they decrypted virtually all communications enciphered with the commercial Enigma machines, greatly helped by the poor quality of the secret keys used by the Spaniards; names of provinces, Spanish rivers, and countries as we shall see later. The Spanish traffic was not of great interest to the British once they discarded the idea of a possible entry of Spain into the war; however it was important for keeping an eye on the considerable Spanish trade with Germany. In the Blue Division one Enigma machine was used to communicate between Berlin and Spain, but whether there existed a second machine to communicate directly with the Germans is not known. Communication with the Germans was more likely to have been made through the German liaison group, because there were very few Spaniards who spoke German. The Enigma used to communicate with the Germans was probably a German *Heeres* Enigma used and handled by them.

Figure 9. *Stecker* Enigma A 17316S and commercial Enigma A 1252 that are in the Spanish Army Museum in Toledo.

4. The rotor wirings

The internal wirings of the rotors and reflector were never changed during the Spanish Civil War, but, as we will see later, there were several different rotor wirings, some equivalent to the commercial Enigma wiring [24]. The reason for there being no change was probably due to the need for communications with the German and Italian forces. It also helped, no doubt, the blind belief in the invulnerability of the encryption produced by this machine.

Six different and special rotor wirings labelled A to F were used in the Enigma machines connected with Spain. The wirings A, C, D and F were used in the Spanish

machines. The wiring of the wheels of the two Enigma machines A 1252[15] and A 17316S[16] shown in Figure 9 are given in Appendix A together with other wheel wirings. Only a small number of the Spanish machines have been measured so far. We therefore do not have a full overview of all the different wirings. The wirings called D and F have been recovered as well as the wiring for the specially wired *Heeres* Enigma machines. Wiring D[17] has further been identified as the wiring used for the machine Bletchley Park (BP) called SNA, Spanish Naval Attaché. Wiring D was also used for the three first wheels, I, II and III, in the Italian Naval machines which BP called Italian K or Italian Naval. This machine had three extra wheels, IV, V and VI, on a special wiring called Ch 11 Tz 350a–c. The wiring designations are described in detail below. Recently one of the Italian Navy[18] machines, K 240, was discovered in Spain. The machine is in private hands since the early 1980s and as far as we can tell it has always been in Spain where it probably was used for communications between Spain and Rome. Another of these Italian machines is K 261, which belongs to the Spanish Ministry of Defence. They both have the same wiring as A 1252, wiring D.

5. Documentary Evidence

A large number of original documents from the manufacturers of the Enigma, *Chiffriermaschinen Aktiengesellschaft* (ChiMAG) and later *Chiffriermaschinen Gesellschaft Heimsoeth & Rinke* (H&R), have recently been discovered.[19] Unfortunately only in a few of these documents is there a direct reference to the sale or delivery of machines to Spain.

The Enigma machines delivered to Spain were of the commercial type that did not have a plugboard (*Steckerbrett*). Internally at H&R this machine was called A27 (*Glühlampen-Chiffriermaschine Modell A 1927*) or Ch 11b after the technical drawing designation for the machine. It was an adaption of the earlier model Enigma D, which they called A26 and Ch 8. The main cryptological difference between the two machines is that on the A26 the transport notches are located on the wheel cores while on the later version, A27, the notches are on the letter rings. In 1936, the A27 (Ch 11b) machines were given their own model series; it was named Enigma K as in K for *kommerziell* (commercial). The change was undoubtedly due to the confusion caused by having both the commercial machines A27 and the Army (*Heeres*) Enigma I, internally called Ch 11f, on the same A-series. The first machine in the new series was K 201.

When the machines were sold to commercial customers such as large companies, banks and to most foreign governments, the wheels were wired with the commercial wiring (*handelsübliche Schaltung*). This wiring, like all other wirings, was described in a

[15] This machine is one of the machines belonging to the group that Bletchley Park (BP) called the Spanish Naval Attaché machines. The wiring was called D, Dora, by the Germans and it is identical to the wiring used by the Italian Army and Navy Enigma machines.

[16] A17316S is a three wheel *Heeres* Enigma of the type used by the German Army and Air Force. However, this is one of the specially wired machines that probably were used by the German Military Attaché or the German *Abwehr*.

[17] Wiring D (*Schaltung D*) is a specific German wheel wiring and it should not be confused with UKW D, *Umkehrwalze* (reflector) D, which has variable wiring changeable by tiny plugs; for more details see [20].

[18] The Italian Army also used Enigma machines with wiring D. It is therefore impossible to say if the Italian machines found in Spain were used by the Army or the Navy; however the majority of the users were naval.

[19] 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 ChiMAG and H&R. The collections are in the *Politisches Archiv des Auswärtigen Amts, Berlin* [28]. Copies of some of these documents will be available at: www.cryptocellar.org/Enigma/EnigmaInSpain.html.

wiring drawing that carried a technical drawing number and which also became the internal H&R designation for a given wiring. The commercial wheel wiring was designated Ch 11 Tz 87a–c[20] for the three cipher wheels and Ch 11 Tz 86 for the reflector (*Umkehrwalze – UKW*). The drawings were dated 27 July 1927, which fits well with the date for the introduction of the machine A27. The commercial UKW wiring seems to have had a variant of some sort since a drawing existed that was labelled Ch 11 Tz 86a and which was dated 18 February 1936. What the differences are is not known as H&R destroyed all wiring diagrams when the Russians entered Berlin in April 1945.

However, some customers requested special wheel wirings (*Sonderschaltungen*). Usually the wirings were only changed for the three cipher wheels while the reflector (UKW) in most cases was left with the commercial wiring Ch 11 Tz 86. These special wirings were normally devised by H&R but they were always reported to the *Reichwehr* cipher office (*Chiffrierstelle*), later *Wehrmacht/Chi*. For special customers, such as the Italians and the Spanish, a special set of wirings labelled from A to F were in use. Who invented these wiring, the *Reichswehr* or H&R, is not known but both used the same terminology and referred to these wirings in the same way, such as *Schaltung D* or *Schaltung Dora*. Figure 10 gives an overview of these special wirings and the wiring Ch 11 Tz 183a–d which was used for the extra wheels IV and V on two series of machines.

Wiring	Wheel drawing	Date
A	Ch 11 Tz ??	21.4.1936
B	Ch 11 Tz 171a–c	Sept. 1936
C	Ch 11 Tz 172a–c	Sept. 1936
D	Ch 11 Tz 173a–c	09.09.1936
E	Ch 11 Tz 175a–c	11.11.1936
F	Ch 11 Tz 174a–c	Sept. 1936
–	Ch 11 Tz 183a–d	01.03.1937

Figure 10. Special wheel wirings (*Sonderschaltungen*).[21]

On most of the machines that used these special wirings the UKW had the normal commercial wiring Ch 11 Tz 86. The first machines that went to Spain seem to have been the machines that were prepared for the Condor Legion.[22] On 2 October 1936 H&R sent a letter to the *Reichskriegsministerium, Chiffrierstelle*[23] with 15 enclosures concerning two orders for cipher machines. The enclosures consisted of the drawings for the special wheel wirings for two sets of machines that had already been delivered. The first order was for 5 *Zählwerksmaschinen*, Enigma G, which probably were intended for the German military intelligence service, *Abwehr*.

However, the second order, Nr. 12360/36, for 22 Enigma machines of the type A27 or Enigma K is strongly suspected to be identical with the 22 *Chiffriermaschinen* (Enigma) that appear on an ordnance list of telephone and radio equipment intended for

[20] Ch most likely stands for *Chiffriermaschinen* in the form of the company name. Ch 11 is their eleventh cipher machine or device while Tz 87a–c is *Technische Zeichnungen*, technical drawings, number 87 a to c.

[21] Based on information in two letters from H&R to *Reichskriegsministerium, Chiffrierstelle* dated 2 October 1936 and 2 March 1937.

[22] The Condor Legion was a military unit of "volunteers" from the German Air Force and German Army that was part of the German military aid to the Spanish Nationalist forces.

[23] On 21 May 1935 the *Reichswehrministerium* was transformed to the *Reichskriegsministerium*, which on 4 February 1938 was changed into *Oberkommando der Wehrmacht*.

the Condor Legion.[24] The machines had the following serial numbers: A 1216, A 1226 – A 1239, A 1241 – A 1242, A 1250 – A 1252, and K 201 – K 202. Many of these machines are among those found in Spain. However, the 22 machines were not all wired the same way. Figure 11 shows a table with the machines that from documentary evidence are known to be on the different wirings.

Wiring	Machine Serial Numbers
A	A 1243, A 1244, A 1245, A 1246
B	A 1226, A 1227, A 1228, A 1229, A 1230, A 1231
C	A 1232, A 1233, A 1234, A 1235
D	A 1216, A 1236, A 1237, A 1238, A 1239, A 1250, A 1251, A 1252
E	K 209, K 210, K 211, K 212
F	A 1241, A 1242, K 201, K 202

Figure 11. Machines wired on the special wirings A–F. The machines found in Spain are underlined.

If we look at the machines suspected to have been delivered to the Condor Legion we see that they are on the four different wirings B, C, D and F. The machine A 1246 on wiring A was not among the 22 Condor machines. Another equipment list for the Condor Legion shows another five machines but unfortunately nothing is known about their identities. It is possible that A 1246 does not belong to the machines delivered to the Condor Legion or to the Spanish Nationalist forces but that it rather is one of the A27 machines that were used by the *Abwehr* in Spain. The question arises as to why the Condor Legion would be equipped with machines with different wirings. The answer is most likely that from very early on it was clear that the German forces would have to communicate among themselves, but they also needed to communicate with Berlin, with Mussolini's Italian "volunteers," and with General Franco's forces. Being careful, the Germans obviously decided to keep these communications well separated and on different cipher networks. Wiring D is the wiring that was used for the machines delivered to the Italian Army and Navy. Wiring B was probably the one used for communication with Berlin or for internal Condor Legion communications. None of these machines have been found in Spain. They were obviously brought back to Germany where in November 1943 A 1226 – A 1229 and A 1231 were rewired for use by the General Staff of the Croatian Home Defence Forces (*Kroatischen Landwehr – Hrvatsko Domobranstvo*). The UKW remained on the commercial wiring Ch 11 Tz 86 but the three cipher wheels were wired after the new wiring Ch 11 Tz 364 a–c.

Another indication that wiring B was not used by Spain is an order sent in May 1941 by WFSt/Stb WNV/Fu II[25] to OKH Chef H Rüst u. BdE/In 7,[26] with a copy to H&R, concerning Enigma machines with special wiring. They ask for the six machines K 739 – K 744 to be wired after Ch 11 Tz 171a–c (wiring B) for the three wheels I–III. The machines would exceptionally be equipped with two extra wheels, IV and V, wired

[24] The 22 machines for the *Luftwaffe* unit and the five for the *Heeres* unit appear in the ordnance lists of *Sonderstab W*. The documents are in the Archivo del Ministerio de Asuntos Exteriores, archive signature: R-2065, 13 and have been reproduced in [10]. On 27 July 1936, on direct orders from Hermann Göring, General Erhard Milch instructed General Helmuth Wilberg to set up *Sonderstab W*. The decision was made during a meeting at the Reich's Air Ministry (RLM) in the presence of General Albert Kesselring and Hans-Jürgen Stumpf. *Sonderstab W* was in charge of organizing the German help to General Franco, an operation code named "Magic Fire" (*Unternehmen Feuerzauber*). During the same meeting the decision to create HISMA was made.

[25] WFSt/Stb WNV/Fu II (*Wehrmacht Führungsstab/Stab Wehrmacht Nachrichten Verbindungen/Funk II*) was the department responsible for supplying the *Abwehr* with communication equipment.

[26] Chef H Rüst u. BdE = *Chef der Heeresrüstung und Befehlshaber des Ersatzheeres*.

after Ch 11 Tz 183a–b, while the UKW would remain on the commercial wiring Ch 11 Tz 86. By this time the Condor Legion, which returned to Germany in April 1939, had long since been abolished. For what purpose these machines were intended is not known but in November 1943 the three machines K 739, K 741 and K 743 were no longer needed. They were then, like the machines A 1226 – A 1229 and A 1231, rewired for use by the Croatian Home Defence Forces. On the order for the rewiring of A 1226 – A 1229 there is a note that the wheels IV and V should be destroyed. This indicates that some of the machines on wiring B had five wheels; but they were not the only ones. The machines K 209 – K 212 on wiring E also had the extra wheels IV and V; however the wiring was not the same as the extra wheels for wiring B. Wheels IV and V for K 209 – K 212 were wired respectively after Ch 11 Tz 183c–d. None of these machines have been found in Spain which strongly indicates that either they were not among the Condor Legion machines or that they were also brought back to Germany. However, it is likely that the machines K 209 – K 212 on wiring E are somehow connected with Spain because they are mentioned together with the machines A 1226 – A 1229 on wiring B in a letter from H&R to *Reichskriegsministerium* In 7 V dated 1 March 1937. Also the fact that the wirings for the extra wheels IV and V for these two groups of machines are described on the same drawing Ch 11 Tz 183a–d indicate a strong affinity between these machines.

One would now expect the Spanish machines to have sufficient variety in their wirings to amply divide and protect the traffic on the different cipher networks, but suddenly some of the reflectors were to be rewired. On 3 December 1936 Chief Engineer Willi Korn[27] signed for the reception of the four reflectors (UKW) A 1241, A 1242, K 201 and K 202 which he had received from In 7 V for rewiring. On which wiring they were to be rewired the note does not say, but it is known that reflectors were only rewired on machines that were to be used for extra secret communications. However, the UKW rewiring order is strange in more than one respect. The four machines A 1241, A 1242, K 201 and K 202 were delivered to the *Reichswehr* sometime in the period from 2 October to 12 November 1936. There is no indication that the machines were delivered with specially wired reflectors. One therefore is tempted to believe that the machines a month after their delivery would get new and special reflector wirings; but this seems not to have been the case. Two of the machines, A 1241 and A 1242, have recently been inspected and the wheels measured electrically; the wirings are shown in Figure 18 in Appendix A. Both machines are equipped with reflectors with the commercial wiring Ch 11 Tz 86. The most likely explanation for this discrepancy is that the reflectors of the four machines were wrongly wired. Either they were wired using the wrong wiring diagram or there was simply an error made during rewiring.

Four three-wheel *Heeres* Enigma machines, A 16101, A 17314S, A 17315S and A 17316S, each equipped with a plugboard (*Steckerbrett*), are among the machines discovered in Spain. These machines belong to a small group of machines of this type that were rewired for special, unknown purposes. It is known that no *Heeres* Enigma machines were delivered to Spain. It is therefore likely that these machines were used by German representatives in Spain, possibly by the German *Abwehr*, or that they were used for intelligence liaison with Spain. A 16101 belongs to a group of machines that were called the Delta machines. On 15 May 1943 H&R received two letters dated 13 May 1943 from OKW WFSt/Ag WNV/Fu IIb and addressed to Chef H Rüst u. BdE

[27] Chief Engineer (*Oberingenieur*) Willi Korn was the chief technical officer of H&R.

AHA/In 7 and H&R. The first letter asked for two *Heeres* cipher machines Enigma to be wired according to the special wiring shown in Figure 12.

Wheel	Wheel Drawing
I – III	Ch 11 Tz 408 a–c
IV – V	Ch 11 Tz 408 d–e
UKW	Ch 11 Tz 409

Figure 12. Wirings for the special *Heeres* Alpha machines.

The letter B on the reflector (UKW) was to be removed and replaced with the Greek letter Alpha (α) and each of the five cipher wheels were also to be marked with the Greek letter α. The two machines that were wired this way were: A 16079 and A 16080. Only one Alpha machine has indirectly been discovered. The two wheels II and III of the machine A 16749, both wheels marked Alpha (α), were captured in Italy at the end of the war [13]. Their wiring is known.

The second letter also asked for specially wired *Heeres* Enigma machines, but this time the order was for 30 machines with the special wiring shown in Figure 13.

Wheel	Wheel Drawing
I – III	Ch 11 Tz 409 a–c
IV – V	Ch 11 Tz 409 d–e
UKW	Ch 11 Tz 410

Figure 13. Wirings for the special *Heeres* Delta machines.

The wheels and the reflector were marked as described above but now with the Greek letter Delta (δ). The 30 Enigma machines with the Delta wiring were: A 16081 – A 16110. The Spanish machine A 16101 belongs to this Delta group. In July 1945 the TICOM Unit of the SSA[28] reported the discovery of a Delta machine, A 16081, which had been used by the German Military Attaché in Zagreb [13]. The machine came equipped with five wheels with the transport notches in the standard positions and with the wheels and reflector marked as described above. The wiring was measured and is shown in Appendix A. This might indicate that perhaps the Spanish Delta machine was being used by the German Military Attaché in Madrid.

Very little is known about the *Heeres* Enigma machines marked with the letter S after the serial number. It is possible the S stands for *Sonderschaltung* and that the machines were marked this way to avoid possible confusion with the normal *Heeres* Enigma. What is known is that they probably all had special wirings. A few other such machines have been discovered but the wiring is only known for one other machine, A17245S, which is described in [13]. The wiring is given for three of the wheels but it differs from the wiring of the wheels in the Spanish S-machines. The fact that the three Spanish S-machines have the same wiring as the Delta machine A 16101 should indicate that the Spanish S-machines are using the wiring given in Figure 13. The problem with this assumption is that the wirings of the two known Delta machines, A16081 and A 16101, are different even if they originally belonged to the same group of machines. Which of the two machines was rewired is not known, but sources in the

[28] The TICOM Unit of the SSA (Signal Security Agency) was the unit processing TICOM information in the USA. The British/American TICOM Teams were controlled and coordinated from GC&CS at Bletchley Park in the UK, where recovered equipment and original documents were also being kept. Microfilmed copies and duplicate equipment were sent to the TICOM Unit at SSA.

Spanish cipher department state that none of these machines were used by Spain after the war and that a post-war rewiring can be excluded. Until a third Delta machine of this group appears this is likely to remain a mystery.

Not all of the Enigma K machines in Spain were used by the Spanish authorities. As mentioned previously some of these machines were used by the *Abwehr*. Some K-machines were used on a network located at Algeciras, Tetuan, Tangier and Ceuta. The network, which was called GGG or GISK2 by the British and that appeared for the first time in June 1941, was servicing the *Abwehr* operation "Bodden" that reported on shipping in the Straits of Gibraltar [9]. These and other Enigma K machines resurfaced in the mid- and late 1944 when BP cryptographers intercepted several messages about Enigma K machines with rewired, multi-notched[29] wheels and equipped with UKW D[30], the so-called KD machine that was going to replace *Abwehr's* Enigma G.[31] The initial idea was to equip the existing machines with new wheels without sending the machines themselves to Berlin, but for various reasons this seemed difficult. In the end, in November 1944, Berlin sent seven new machines with the new wheels to the main Iberian *Abwehr* stations, four to Madrid and three to Lisbon. As was often the case confusion reigned at *Abwehr* headquarters in Berlin. On 17 June Berlin asks if one of the nine K machines in the Madrid area is unusable. On 23 June Berlin fires off yet another question: "How many K-machines do you have in the Madrid area? Reply urgently." This seemingly wakes up the Madrid end who replies on the same day: "Eight K-machines." During this period Berlin tries to take stock of the Enigma K machines but yet again there is more confusion. Berlin seems not to know that they have got K 297 and Madrid is vague as to how it was returned. Apparently also the wheels became detached from the parent machine. On 28 November there is reference to yet another K machine. Madrid asks Berlin to return wheel IV of K 688, which had been sent back to Berlin for repairs. Berlin replies on 1 December 1944, two days before the UKW D measure came into effect, saying that the wheel for K 688 will be dispatched shortly. The codebreakers at BP's ISK[32] section, Illicit Services Knox, followed the Enigma KD development with more than a little worry. Initially they considered the KD traffic intractable, but eventually and yet again they got their break. In January 1945 they succeeded in recovering the first wheel wiring and by 28 January all six wheels had been recovered; a remarkable accomplishment.

6. British Attacks on the Spanish Machines

Germany had serious doubts about Italian crypto security and it is very likely that they had similar reservations about Spanish cryptography. Before the war Germany supplied only commercial Enigma machines to the Italian armed forces, but when Italy became a German ally both the *Heeres* Enigma with plugboard (*Stecker*), Ch 11f, and the Enigma G (*Zählwerksmaschine – Ch 15a*) were supplied for special German/Italian intercommunications. The machines were used mainly for intelligence and cryptanalytic liaison between the two countries. The other belligerent nations among the Axis powers,

[29] The wheels have nine notches at A, C, G, I, M, P, T, V, and Y.
[30] For further details about *Umkehrwalze* D see Philip Marks' detailed description in [20].
[31] "Review of material relating to the K-machine plus 'D'." ISOS Section notes and reports on *Abwehr* cypher usage, TNA PRO HW19/314. We are grateful to Ralph Erskine, who supplied a copy of this document.
[32] The ISK Section was also sometimes referred to as Intelligence Services Knox. The section deciphered German intelligence traffic enciphered with the Enigma machines.

Bulgaria, Hungary, Romania and Slovakia, also received the *Heeres* Enigma, Ch 11f.[33] Spain, not being a part of the Axis, never received the more secure versions of the Enigma machines. Italy received their first commercial Enigma machines of the type A27 in 1932. The three machines, A 1213, A 1214 and A 1215, were probably delivered with the normal commercial wiring; wiring D was first created in September 1936. The next delivery, which took place in September 1936, was for 50 Enigma K machines, K 233 – K 282.[34] They all had the new wiring D and they were probably delivered to the Italian Army and Navy, but we cannot exclude the possibility that some of the machines were intended for the Spanish Nationalist Forces. Some of these machines were being used by Mussolini's Italian "volunteers" during their Spanish campaign. While the Italian Army and Navy used machines with the special wiring D the Italian Air Force seemingly used Enigma machines with the normal commercial wiring. In mid-September 1937 the Italian Air Ministry received 10 Enigma K machines, K 302 – K 311 with the commercial wiring, Ch 11 Tz 87a–c.

The increased Italian traffic was quickly noticed by the British cryptanalysts at GC&CS.[35] The codebreaker who initially attacked the Italian Enigma traffic and discovered the new wheel wirings with his "buttoning-up" method was the famous Dillwyn (Dilly) Knox [5]. The Italian traffic was received by two intercept stations situated at Fort Bridgewoods, outside Chatham, and at Flowerdown, the Admiralty station at Littleton near Winchester [31]. To deal with the Italian Naval and Air Force traffic Britain entered into collaboration with the French who operated an intercept station at Pointe de la Croisette at Cannes [7]. The breakthrough for Dilly Knox came in April 1937 when 20 Italian naval messages were enciphered on the same Enigma setting. This blunder, breaking the most basic of all cryptographic rules, allowed Knox to find the wiring of all the three wheels on wiring D. It was soon discovered that the Spanish Enigma machines[36] used the same wheel wirings so that they could communicate with the Italian machines. Wilfred Bodsworth, a Spanish expert and a member of Dilly's team of codebreakers, took over the Spanish traffic.

After the Spanish Civil War the Spanish machines were used for communication with their Naval Attachés, while some of the Italian machines were sent to their stations in the colonies: Asmara, Rhodes, Tripoli, Benghazi, Leros and Tobruk. Machines were also deployed at Hyères on the south-eastern coast of France, at Pula on the Istrian peninsula in Croatia, at the base Marisudest at Pireaus in Greece and at BETASOM[37], the Italian submarine base at Bordeaux in France. Furthermore, the Italian Enigma K machines were used by their Naval Attachés in Tokyo and Berlin.[38] As we have seen the Italian cipher clerks initially made stupid errors, probably due to being badly instructed and perhaps also to some degree of laziness, but finally their cipher officers

---

[33] "Enigma Machines in Foreign Countries," TICOM translation of German document addressed to OKH/Chef H Rüst u. BdE/AHA/In 7 IV and dated Berlin, 3 Sept. 1943; TICOM/DF-190-AM. The document is part of [13] that was released under a NSA FOIA request.

[34] The September 1936 delivery of 50 Enigma K machines with wiring D is mentioned in a letter dated 12 September 1940 from *Oberkommando des Heeres, Generalstab des Heeres / Chef HNW IV / 78 g S Nr. 4987/40 geheim* and addressed to H&R.

[35] GC&CS – Government Code and Cypher School, the British codebreaking and cipher security organization, was then situated at Broadway Buildings in Westminster, London.

[36] The BP codebreakers seem not to have discovered or identified traffic enciphered on the machines with the other wheel wirings used in Spain.

[37] BETASOM is an Italian acronym for *B Sommergibile* (B submarine) referring to submarine base B (Bordeaux).

[38] From "Communications Organization of the Italian S.I.S.", Appendix 4. The US National Archives and Records Administration (NARA), College Park, RG 457, Historic Cryptographic Collection, Box 1386, NR 4421, ZEMA 193. We are grateful to Ralph Erskine and Philip Marks for copies of this document.

seem to have understood how to secure the Enigma traffic. The indicator system they devised, which took the form of three letters and two numbers, i.e. WTY47, and that probably came from a book, was never broken by GC&CS. Because the indicator system was not broken the wheel turnovers were never known. This meant that every message had to be broken separately [6].[39] In December 1943 Dilly Knox's section ISK received accumulated traffic between the Spanish Military Attaché in Berlin and Spanish Army Headquarters in Madrid. Nothing was known about the cipher; except that it appeared to be a machine cipher and that it used a peculiar indicator system. The indicator consisted of eight letters made up of the first and last letters of the cipher groups 2, 3, 4 and 5. The indicator system was easily broken because a rather simple substitution system was used and the result was of the form ROSA SPTB; the machine setting followed by a garble check.

At first this problem seemed insoluble because there were no good cribs (probable words) available and the volume of traffic was low, rarely more than five or six messages a day. Fortunately it was discovered that occasionally the Military Attaché would send his messages on the Naval Attaché's cipher, which was then being read currently. When the Naval Attaché messages were inspected it appeared that often a short message of constant text was transmitted: DIVISION NO HA DADO HOY PARTE NOVEDADES. It had already been noticed that frequently short messages of eleven or twelve groups were transmitted on the Military Attaché cipher and it was therefore supposed that they were reporting that the "Blue Division",[40] which was then on the eastern front, had nothing to report. Thirty-seven such short messages were collected and as suspected the given crib did fit these messages with very few "crashes."[41] This showed that the suspected crib was correct and that the messages had been enciphered on an Enigma machine. The ISK section already knew that the wiring was different from the machine used by the Spanish Naval Attaché. However, it was natural to suspect that the Military Attaché would also be using a commercial Enigma but with differently wired wheels. The question was how to recover the wheel wiring from thirty-seven different encipherments of the same plaintext. The recovery of the wheel wiring is too elaborate to be given here, but a short description of the problem is very educational. Due to the already recovered indicator system the BP codebreakers suspected that the Spaniards would use the machine in an ingenious manner. They therefore thought the setting of the *Ringstellung*, similar to the setting of the message key, would be based on pronounceable words with a high preponderance of vowels in the fourth place. With vowels being used for both the *Ringstellung* and the message key setting for the fourth wheel – the fast, right-hand wheel – many of the messages would likely have been enciphered at the same right-hand wheel rod (i.e. core) position. This hypothesis resulted in six messages initially being selected as likely to have been enciphered in the same rod position, but after some work they were reduced to only two messages. After buttoning up these messages with the suspected plaintext and testing the various hypotheses that resulted, the wiring of the fast wheel was recovered. It was then relatively straightforward to recover the other wheel and the reflector wirings. It then turned out that the recovered wiring for the fast wheel was indeed the wiring of the

[39] The document in [6], which is covered by Crown Copyright, has been released in part (pages 5, 84–92, 174–175, 178) as a discretionary release by the Director of Government Communications Headquarters (GCHQ), UK. We are very grateful to GCHQ for their cooperation with our research.

[40] The Blue Division or the German Army 250th Infantry Division was a unit of Spanish volunteers who served in the German Army on the Eastern Front. They entered the Russian front in August 1941 and were on active duty until at least October 1943.

[41] A "crash" was a BP term for a letter that enciphered to itself; something impossible for the Enigma machine.

fast wheel for all of the thirty-seven messages. As the messages covered almost a complete year it was naturally assumed that the wheel order never changed. By the normal Saga methods that are described in Alan Turing's "The Profs Book" [29][42] first the middle wheel was recovered and finally the left-hand wheel and the reflector. The report [6] is rather severe in its criticism: "As expected, the Spanish used the Enigma in a childishly incompetent fashion. The wheel order never changed, and the keys were constructed to last for a hundred days, a *Ringstellung* lasted ten days and the indicator substitution a hundred days."

Because the wheel wirings had been recovered cryptanalytically they would have the normal offsets and twists with respect to the real wheels and the *Ringstellung* would therefore be unknown. However, because the wheel order was constant the effect of the offsets and twists was nothing more than a constant substitution applied to each of the four *Ringstellung* letters. It was obvious that the *Ringstellung* letters were part of words and by discovering which letters in each *Ringstellung* were vowels the codebreakers succeeded in recovering the true *Ringstellung*. It turned out that when the set of *Ringstellung* for a hundred-day period was put together they formed the words from a certain topic. One set was a tour of the Spanish coast as shown in Figure 14.

1	2	3	4	5	6	7	8	9	10
BARC	ELON	ATOR	TOSA	VINA	ROZS	AGUN	TOGA	NDIA	VERA

Figure 14. Hundred-day *Ringstellung* key table for the Spanish Military Attaché machine.

Another set of *Ringstellung* keys consisted of a set of barber's shops after which the keys switched to appliances used in a metal foundry. The persons responsible for generating keys for the Military Attaché machines seem not to have understood the seriousness of the task and instead they looked upon the work as some kind of intellectual game. However, as we know they were not alone in this regard. The German key management people were often equally incompetent. There was also a Spanish Military Attaché in Rome who used the same machine for his communications with the Military Headquarters in Madrid. However, he used a different key and even a different wheel order. This presented a new problem for the ISK codebreakers but it was not very difficult as he always enciphered his "situation reports" on the setting SITU. The Enigma keys were constructed on the same system as already described but the two attachés always used different sets of *Ringstellung* keys. While the Berlin attaché toured the Spanish coast from the north-east, his Roman colleague started from the north-west such that they nearly met at Gibraltar. During the time of the Allied advance in Italy in 1944 the Attaché in Rome did not receive his keys. To repeat the keys would obviously have been insecure, so instead he decided to use the reverse *Ringstellungen* of the immediately preceding period. That the ISK codebreakers enjoyed solving the Spanish problem is shown by their final words of this chapter: "The problem of the Spanish Attachés was highly entertaining throughout, providing an excellent example of how a cypher machine should not be used."

7. The keys

The cipher using Enigma machines was named "mechanical key" during the Spanish Civil War. Initially this hampered our search in the archives because there is no reference to the Enigma machines in the archive search engines. Unfortunately the only

[42] Wheel recovery and the Saga method are described in Chapter 3 which is available online from: http://www.cryptocellar.org/Turing/

list of daily keys used in the civil war we know is one from the Condor Legion reproduced in David Kahn's book "Seizing the Enigma" [15, p. 289]. The first time we saw a description of an Enigma key procedure was in a paper written by Antonio Sarmiento, head of communications of General Franco's forces, entitled "Description of and general information about the use of the cipher machines: A 1232/33/34/35 and K 203/4/5/6/7/8" [25]. The procedure was divided into three steps named first, second and third operation in this little manual; these operations are:

- First operation. Set the rotor order. The rotors are labelled I, II and III and the reflector, logically never changed, was named rotor 0.
- Second operation. Set the alphabet rings (*Ringstellung*).
- Third operation. Set the start or initial position of the rotors, the message key. The message key has two parts, the four letters of the key and the position where the key is dissimulated in the message

The internal settings (the first and second operations) were always sent with an order to destroy the message with the new settings after the machines had been set. Initially the key in the third operation, the message key, was set daily. In the manual this is the indicated periodicity — "the quaternary combination agrees; for each day …" and later in the same text there are two references to "set one key for each day of the month". Later, the message key was freely chosen, and indicated twice in the message, probably due to German influence.

The message key was normally hidden in the message but there were some variations. In telegraphic communications to foreign countries the procedure is described in a document entitled: "Particular instructions for the use of A and K series mechanical ciphers by Overseas Commissions for communications with the Office of the Secretary of State".[43] Because of the rules and limitations of some foreign telegraph offices these messages always used five-letter cipher groups. The document calls for the message key to be dissimulated in the third and last five-letter groups of the message. The three first letters of the key are in alternate positions in the third group, the first, third and last letters of the group, while the second and fourth letters are nulls. The last group contains the last three letters of the key in reverse order with nulls for the second and fourth letter. For example, if the key was FOUR then in the third group we find FbOdU and in the last RxUcO, where b, d, x, c are the null letters. If the foreign telegraph office obliged the user to indicate the code being used in the first group, the word COLOC was written here and hence the fourth group was used for the message key instead of the third.

In military use and when the telegraph offices allowed groups of four letters, the standard for Spanish military use, the third and last groups were used for the message key. In a message dated 9 December1936[44] we find the message key in the third and last groups, the latter in reverse order.

We have no indication about the frequency of the rotor order change (the first operation), but it seems the *Ringstellung* (the second operation) changed every ten days. The order for the destruction of the documents containing the setting for the internal keys makes it extremely difficult to obtain information about how often these changes occurred. Some of the documents saved from destruction give us only a fragmentary idea of these changes. A telegram dated 31 December 1938 changes the rotor order and the procedure for the message key operation. The rotor order (first operation) changed

[43] "*Overseas Commissions"* refers to the diplomatic legations in foreign counties. The "*Office of the Secretary of State"* is equivalent to the Ministry of Foreign Affairs.
[44] Reproduced in [27], page 139.

to I, II, III and the position of the key in the telegram also changed. The message key was now hidden in the sixth group in normal order, while the last group, used as a garble check, was formed by adding one to each message key letter in the normal alphabetical sequence. For example, if the sixth group was FOUR then the last group was GPVS. Another document from 5 October 1941[45] is more informative. We see a change in the order of the rotors (first operation) to I-III-II, and new keys for the second operation (*Ringstellung*) for three months. A change in the third operation is also made. The message key is hidden in the two first positions in the second and third groups. The verification group is the penultimate one and is formed in the same way as above, taking the next letter in the normal alphabetical sequence. For example, if the second and third groups are ABrs and CDtv, with the message key in capital letters, the penultimate group will be BCDE. One important thing about this document is the recipients, the High Command, the General Staff of the Army, the Command of the Spanish Blue Division and the Military Attaché in Berlin. From the recipients of this document we can deduce that the Military Attachés were on separate cipher networks with their own Enigma keys, otherwise the document would have been addressed to all the Military Attachés in foreign countries. This confirms the observation made by the British that the Spanish attaché in Rome used a different key from the attaché in Berlin.

13/04/39	No dates indicated							
TRIA	NGUL	OROM	ABER	LINT	OKIO			
Corresponding to: TRIANGULO ROMA BERLIN TOKIO [3]								
30/10/40	10/11/40	20/11/40	30/11/40	10/12/40	20/12/40	30/12/40		
ECUA	DORN	ICAR	AGUA	HOLA	NDAJ	APON		
Corresponding to the nations: ECUADOR, NICARAGUA, HOLANDA, JAPÓN [23]								
05/10/41	15/10/41	25/10/41	05/11/41	15/11/41	25/11/41	05/12/41	15/12/41	25/12/41
NALO	NNAR	CEAS	ELLA	NAVI	ASIL	MIER	APAS	ORIA
Corresponding to the Spanish rivers NALON, NARCEA, SELLA, NAVIA, SIL, MIERA, PASORIA. Rotor order: I, III, II. [26]								
05/03/41	15/03/41	25/03/41	05/04/41	15/04/41	25/04/41			
SEVI	LLAC	ORDO	BAJA	ENHU	ELVA			
It corresponds to the Spanish provinces: SEVILLA, CORDOBA, JAÉN, HUELVA [23]								
10/01/41	20/01/41	30/01/41	10/02/41	20/02/41	30/02/41	10/03/41	20/03/41	
LOPE	DEVE	GACA	LDER	ONDE	LABA	RCAD	ARIO	
Corresponding to the Spanish writers: LOPE DE VEGA, CALDERON DE LA BARCA, DARIO [23]								

Figure 15. Examples Enigma keys used after the Spanish Civil War.

The *Ringstellung* keys shown in Figure 15 are typical of the keys from the 1940s, not very original and highly insecure, generally formed using geographical names or the names of well-known Spanish authors.

8. How the machines arrived in Spain

An interesting aspect of the Spanish Enigma history is how the machines were acquired and how they arrived in Spain. In September 1943 H&R prepared an overview for the *Wehrmacht* that showed which foreign countries had bought or received Enigma machines. Apart from three machines delivered to Spanish Morocco via the German

[45] Reproduced in [26], page 157.

telecommunication manufacturer Lorenz, no other Spanish machines are mentioned. At first this seems rather odd but on second thoughts it is perhaps not so strange. If the orders for weapons, telecommunication and cipher equipment for the Spanish campaign went through official or semi-official German channels, then it is normal that these orders would not have been regarded as commercial sales by H&R. Hence they would not appear on the list of commercial orders. The machines that were prepared for the Condor Legion were ordered by the *Reichskriegsministerium* and also delivered to them; but what about the machines that were bought by Spain and delivered to the Nationalist forces? It is doubtful if H&R knew that the first machines were destined for the Condor Legion, but perhaps they had their suspicions or they were unofficially informed by their good contacts in the *Chiffrierstelle*. It is possible that in the very beginning the machines for Franco's forces were ordered and delivered through the *Reichskriegsministerium*, however later H&R probably dealt directly with Spanish representatives. The intermediary here was the German end of the HISMA / ROWAK[46] Corporation. ROWAK, which was founded on 2 October 1936 on direct orders from Hermann Göring, should be seen as a company controlled by the German state. On 9 November the Reich Economics Ministry (RWM) published an administrative order that prohibited private German companies from trading directly with Spain [18;19]. All trade had to go through ROWAK. In January 1938 an engineer with the name Karl Devantier, who had business interests in Spain, wanted to represent H&R there but this was rejected by the *Reichskriegsministerium* for the following reason: "The delivery of cipher machines for the national Spain takes place – as you know – through ROWAK under precise control of the receiver. OKH is unfortunately therefore not in a position to give you permission to open business connections with Karl Devantier."[47]

The only direct contact between H&R and ROWAK that has been discovered so far is via the Berlin firm Helmut Schröder. In January 1941 H&R was in contact with Mr. J.O. Wehn, the representative of one of ROWAK's German companies, Helmut Schröder, Import – Export with an address at Kochstrassse 18, Berlin SW 68. Their letterhead says they are the purchasing house of the firm H. & O. Wilmer, Sucesores de H. Tönnies, Tetuan – Madrid. In Christian Leitz's articles on the foundation of HISMA/ROWAK we are told that the German intervention in Spain more or less started with a meeting between Johannes E. F. Bernhardt and General Francisco Franco on 21 July 1936 [18;19]. Johannes E. F. Bernhardt was the sales director of the company H. & O. Wilmer, Sucesores de H. Tönnies.[48] This shows that the company Helmut Schröder was probably one of the core German representatives of HISMA/ROWAK. Only part of the correspondence with Helmut Schröder is available but what has been found shows that it concerns an order for 100 Enigma machines for the Spanish Gendarmerie. A letter from the Dirección General De La Guardia Civil[49] in Madrid dated 14 January 1941 and signed by Antonio Torres Bestard, Coronel Jefe de Estado Mayor, is addressed to H&R. The letter explains that the chief administration of the Gendarmerie wants to equip their units with cipher machines to encipher their communications and that they have had the opportunity to test the Enigma machines that H&R had already delivered to other Spanish state organizations. Mr. Torres Bestard explains that the total

[46] HISMA stands for *Hispano-Marroquí de Transportes, Sociedad Limitada.* ROWAK, the German branch, stands for *Rohstoff- und Waren-Kompensation Handelsgesellschaft AG.*

[47] The quote is from a letter in German sent by *Oberkommando des Heeres* to H&R on 27 January 1938.

[48] Bernhardt was on very familiar terms with the top Spanish military officers in Morocco. These military offices knew Bernhardt by his more informal name, Tónie. Bernhardt became a member of the *Auslands-organisation* (AO) on 1 April 1933 [11].

[49] Guardia Civil is the Spanish Gendarmerie, a police force with military status in charge of public safety and other civilian police duties. It resembles closely the French Gendarmerie Nationale.

order will not be under 100 machines and on the top of the page a delivery schedule dated 20 March 1941 has been added in pencil. It shows a delivery of 10 machines in September with a further 10 machines in November and December and the remaining 50–70 machines delivered in April 1942. The business card of Mr. J.O. Wehn is attached to the letter, but it ends with Mr. Torres Bestard asking H&R if they by any chance would have a representative in Madrid or at least a Spanish representative who could make direct contact and pay the Gendarmerie a visit. One therefore gets the feeling that it was H&R who then established contact with the company Helmut Schröder, the ROWAK representative.

On 12 February 1941 H&R receives a letter from the *Oberkommando der Wehrmacht* (OKW) dated the day before. The letter explains that OKW has no reservations against a sale of commercial Enigma machines to the Spanish Gendarmerie under the conditions that this contract will not delay the delivery of Enigma machines for the *Wehrmacht*. They further say that as soon as the contract with the Spanish Gendarmerie has been signed and the delivery made, OKW wants to be informed about the serial numbers of the machines and their rotor wirings.

On 25 March 1941 a letter from Helmut Schröder, dated 24 March 1941 and signed by Wehn, Export Division, arrived at H&R. Helmut Schröder's reference is ES 930[50] and the subject is "Spanish export; cipher machines for the Dirección General De La Guardia Civil, Madrid. Discussions with you." The letter refers to the discussion the undersigned (Wehn) had with Mrs. Rinke[51] and Mr. Korn and their agreement about the contract for the Guardia Civil. The letter further says that unfortunately Mr. Herbert Wilmer of the firm H. & O. Wilmer, Madrid, cannot meet with them as he has already flown back to Madrid. Wehn explains that they (Helmut Schröder) or their Spanish company (H. & O. Wilmer) will work as a representative for the company Heimsoeth & Rinke and that they will present an offer to the Guardia Civil for 100 Enigma cipher machines with the following delivery schedule:

1. 10 machines September 1941
2. 10 machines October 1941
3. 10 machines November 1941
4. 10 machines December 1941
5. Delivery of the outstanding up through April 1942

The quoted price for the firm Helmut Schröder was 800 RM minus 10% rebate per machine. He also states that the firm H. & O. Wilmer is justified in adding an additional sum on top of the machine price of 800 RM because the Spanish company needs to take special considerations, which frankly sounds like some form of corruption. He closes by saying that Mr. Wilmer has taken the offer with him to Madrid and that they hope soon to be able to give a brief situation report.

But there the matter stops. There are no further documents relating to this case and as there are no sales to Spanish customers mentioned in the 1943 overview of Enigma sales to foreign customers it is most likely that the whole thing foundered. Perhaps the Guardia Civil found the machines were too expensive or perhaps things went wrong when the right officials had to be paid their "commission". A former member of the Spanish cipher department has confirmed that the Guardia Civil never received any Enigma machines. However, as mentioned previously, one sale of a more

[50] ES 930 probably stands for *Export Spanien* (Spanish export) reference no. 930. A similar reference, ES-1060 has been found in the Spanish archives. It is dated mid October 1938 and it concerns the acquisition of eight *Kryha* machines.

[51] Mrs. Elsbeth Rinke was the managing director of H&R.

commercial character took place via the German firm Lorenz. On 9 January 1939 H&R sent a letter addressed to *Oberkommando des Heeres* In 7 V informing them that three commercial Enigma machines with the serial numbers K 356 – K 358 have been delivered to Spanish Morocco. They were delivered by the firm C. Lorenz AG, Lorenzweg, Berlin-Tempelhof to the *Batallón de Transmisiones de Marruecos*, Ceuta. All the wheels and the reflector were wired with the normal commercial wiring.

9. How many Enigmas are there in Spain?

It's very difficult to know at this moment how many Enigmas were being used in Spain. The Spanish military has very strict rules concerning cryptology, and the machines should all have been destroyed. Luckily some were saved, forgotten in a warehouse, such as the machines that recently appeared in the Army Headquarters. It is also possible some were saved from destruction and are in private hands. At the moment we know there are several machines in the Army Museum, the National Centre of Intelligence (CNI), the Army Headquarters and other military establishments. Figure 16 gives an overview of the machines that are known to have been used in Spain and those machines that are still in existence today and with their known locations.

#	Serial number	Date acquired	Source/Notes
1	A 1216	2002[52]	National Intelligence Centre
2	A 1232	November 1936	*Description of and general information about the use of the cipher machines: A 1232/33/34/35 and K 203/4/5/6/7/8.*
3	A 1233	November 1936	*Description of and general information about the use of the cipher machines: A 1232/33/34/35 and K 203/4/5/6/7/8.*
4	A 1234	November 1936	*Description of and general information about the use of the cipher machines: A 1232/33/34/35 and K 203/4/5/6/7/8.*
5	A 1235	November 1936	*Description of and general information about the use of the cipher machines: A 1232/33/34/35 and K 203/4/5/6/7/8.*
6	A 1241		Spanish Ministry of Defence
7	A 1242		Foreign Ministry Archive. Army Headquarters.
8	A 1246[53]		Army Headquarters
9	A 1252		Army Museum
10	A 17314S		Spanish Ministry of Defence
11	A 17315S		Spanish Ministry of Defence
12	A 17316S		Army Museum
13	A 16101[54]		Private collection
14	K 202	November 1936	*Description of and general information about the use of the cipher machine "ENIGMA": K 202.*
15	K 203	November 1936	*Description of and general information about the use of the cipher machines: A 1232/33/34/35 and K 203/4/5/6/7/8.* Lost or stolen in 1937 [26]
16	K 204	November 1936	*Description of and general information about the use of the cipher machines: A 1232/33/34/35 and K 203/4/5/6/7/8.*

[52] In 2002 the machine A 1216 was donated by the National Intelligence Centre (*Centro Nacional de Inteligencia* – CNI) to the Army Museum.

[53] On 21 February 1934 *Chiffriermaschinen AG* delivered to the *Reichswehr* four machines with special wiring, A1243 to A1246. On the delivery slip it is noted in pencil: (A1245 – A1246 Japan), however it is doubtful that any of these machines went to Japan. We now know that A1246 is in Spain and that it has wiring A.

[54] This machine belongs to a group of machine with special wheels wirings and which were called Delta machines. All the rotors were marked with the Greek letter Delta as well as their wheel number and serial number.

#	Serial number	Date acquired	Source/Notes
17	K 205	November 1936	*Description of and general information about the use of the cipher machines: A 1232/33/34/35 and K 203/4/5/6/7/8.* Now in the Army Museum.
18	K 206	November 1936	*Description of and general information about the use of the cipher machines: A 1232/33/34/35 and K 203/4/5/6/7/8.*
19	K 207	November 1936	*Description of and general information about the use of the cipher machines: A 1232/33/34/35 and K 203/4/5/6/7/8.*
20	K 208	November 1936	*Description of and general information about the use of the cipher machines: A 1232/33/34/35 and K 203/4/5/6/7/8.*
21	K 225	1937	[14]
22	K 226	1937	[14]
23	K 240		Private collection
24	K 256		Army Headquarters
25	K 261		Spanish Ministry of Defence
26	K 287	1937	[14], confirmed existence by Army Headquarters
27	K 288	1937	[14], confirmed existence by Army Headquarters
28	K 289	1937	[14], confirmed existence by Army Headquarters. Now in the Army Museum.
29	K 290	1937	[14], confirmed existence by Army Headquarters
30	K 291	1937	[14], confirmed existence by Army Headquarters
31	K 292	1937	[14], confirmed existence by Army Headquarters
32	K 293	1937	[14], confirmed existence by Army Headquarters
33	K 294	1937	[14], confirmed existence by Army Headquarters
34	K 295		Army Headquarters
35	K 296		Army Headquarters
36	K 298		[4]
37	K 356[55]	January 1939	Army Headquarters
38	K 357	January 1939	Army Headquarters
39	K 358	January 1939	Army Headquarters
40	K 693		Army Headquarters
41	K 694		Army Headquarters
42	K 723		Army Headquarters
43	K 726		Army Headquarters
44	G 316		Spanish Ministry of Defence

Figure 16. Overview of known and existing Spanish Enigma machines[56].

[55] The machines K 356, K 357 and K 358 are known to have been delivered to Spanish Morocco via a contract with the German firm Lorenz. The machines were delivered in January 1939 to the Batallón de Transmisiones de Marruecos, Ceuta. All of the machines were delivered with commercial wirings.

[56] The "source" is not an indication of where the machines are located. In some cases "source" shows the ownership but sometimes the machines might be on loan to other institutions such as museums and schools.

Appendix A: Wheel Wirings

Wheel	Wheel Wiring ABCDEFGHIJKLMNOPQRSTUVWXYZ	Notch	Window
I	CIAHFQOYBXNUWJLVGEMSZKPDTR	G	Y
II	KEDXVBSQHNCZTRUFLOAYWIPMJG	M	E
III	NUJPHWFMGDOBAVZQTXECLKYSIR	V	N
UKW	IMETCGFRAYSQBZXWLHKDVUPOJN		
ETW	QWERTZUIOASDFGHJKPYXCVBNML		

Figure 17. Wheel wiring for A 1252, K 240 and K 261. This is wiring D that was used in the Spanish Naval Attaché (SNA) machine and in the Italian Naval Enigma.[57]

Wheel	Wheel Wiring ABCDEFGHIJKLMNOPQRSTUVWXYZ	Notch	Window
I	HFOTWPDURMCGXJLQEIVZSKBNAY	G	Y
II	MUHTASIPJYNCVKLOXFDZEGQBWR	M	E
III	DKWOJVUNGLFTZCSYIBEARHXQPM	V	N
UKW	IMETCGFRAYSQBZXWLHKDVUPOJN		
ETW	QWERTZUIOASDFGHJKPYXCVBNML		

Figure 18. Wheel wiring for A 1241, A 1242, K 205 and K 289; wiring F.

Wheel	Wheel Wiring ABCDEFGHIJKLMNOPQRSTUVWXYZ	Notch	Window
I	OCHQZMJPFIWEXTYLGVBKDNURAS	Y	Q
II	HWBEOSZFQMTXRKIGVJYPUCLNAD	M	E
III	XTKFJRMLGYVQWUBIEHANPDSOZC	D	V
IV	IGTCNQWJMHXFEZVSYBLPROKDAU	R	J
V	NXEKUZMQLVCTIRJYHSDGAFBPWO	H	Z
UKW	YIOGTXDKBSHVWRCQPNJEZLMFAU		
ETW	ABCDEFGHIJKLMNOPQRSTUVWXYZ		

Figure 19. Wheel wiring for A 16101, A 17314S, A 17315S and A 17316S.

Wheel	Wheel Wiring ABCDEFGHIJKLMNOPQRSTUVWXYZ	Notch	Window
I	CVFWJOBXANQTDZUMEYRPSKGILH	Y	Q
II	XJGURHZMYDLATWKSEPNCQFOIBV	M	E
III	SYIGXELDUKBVOAWTZHQNFCRMJP	D	V
IV	HKTZDSRFWPCQJIYXNVMUGELAOB	R	J
V	WMGRKEJUAZFTOXINDYBQVHLCPS	H	Z
UKW	DONAJUXTQELKSCBZIVMHFRYGWP		
ETW	ABCDEFGHIJKLMNOPQRSTUVWXYZ		

Figure 20. Wheel wiring for the Zagreb Delta machine A 16081.

[57] The Italian Naval Enigma has a total six wheels but we have so far only found the three first wheels. All the wheels were recovered cryptanalytically by GC&CS at Bletchley Park, but with the normal twists and offsets. Also their wheel numbering was off; wheel I BP called Green (III), wheel II was labelled Red (I) and wheel III was Blue (II).

Wheel	Wheel Wiring	Notch	Window
	ABCDEFGHIJKLMNOPQRSTUVWXYZ		
I	DMTWSILRUYQNKFEJCAZBPGXOHV	ACDEHIJKMNOQSTWXY	SUVWZABCEFGIKLOPQ
II	HQZGPJTMOBLNCIFDYAWVEUSRKX	ABDGHIKLNOPSUVY	STVYZACDFGHKMNQ
III	UQNTLSZFMREHDPXKIBVYGJCWOA	CEFIMNPSUVZ	UWXAEFHKMNR
UKW	RULQMZJSYGOCETKWDAHNBXPVIF		
ETW	QWERTZUIOASDFGHJKPYXCVBNML		

Figure 21. Wheel wiring for Enigma *Zählwerksmaschine* G 316.[58]

[58] G 316 has identical wheel wirings to the famous Bletchley Park *Abwehr* Enigma G 312 that was described in great detail by David Hamer in [12].

Acknowledgements

We would like to thank Mr. Ángel Sarmiento, who recently died, for his invaluable help; Mr. Arturo Quirantes for the copies sent to us concerning the delivery of the Enigma machine to the Embassy in Berlin; Mr. Manuel Espinosa de la Garza for the information about communications in the Berlin Embassy; Mr. Carlos Caballero Jurado for his help with the Blue Division organization; Mr. Walter Austin Edler for assisting us with the English translation and edition of this article, and the editors for their assistance. The third author, who is presently engaged in a major research on Enigma history, should like to express his gratitude to a number of people who have been of most invaluable help. First of all he should like to thank Dr. Heinz Ulbricht who graciously shared his detailed knowledge of the TICOM collection in Berlin [28] and who arranged for the author to get special access to the collection in the very early days. Further thanks go to Dr. Peter Grupp, Dr. Martin Kröger, Mrs. Sabine Schafferdt and Mrs. Birgit Kmezik of the *Politisches Archiv des Auswärtigen Amts* in Berlin whose arrangements and friendly help made this first visit a great success. The author should furthermore like to thank his wife Kayoko for her help with photographing thousands of documents. Special thanks also go to the Departmental Historian of GCHQ and indirectly the Director for agreeing to discretionary disclosure of still classified information. We are most grateful. Thanks are also addressed to the NSA's FOIA and MDR offices and their staff who have generally been very helpful even if the present declassification rules make requests for 60 year old cryptographic material a time-consuming struggle. We also thank Ralph Erskine and Philip Marks for their help with documents and Philip Marks for his thorough review.

About the Authors

José Ramón Soler Fuensanta gained his degree in sciences at the University of Barcelona. He received his PhD in engineering from the Universidad Nacional de Educación a Distancia (UNED). Now he's a teacher in the Escuela de Turismo del Consell Insular de Ibiza (Spain). His interest in cryptology began years ago and since then he has been a dedicated collector of studies on the subject. His main interest is in the field of Spanish cryptology and especially the Spanish cryptology of the 20th century.

Francisco Javier Lopez-Brea Espiau is Lieutenant-Colonel in the Spanish Army and specialist in cryptology in the Ministry of Defence. His main interest is in the field of Spanish cryptology and especially cryptographic devices and military cryptography.

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

References

1. Anon. 2001. "From the Archives. The Glow-Lamp Ciphering and Deciphering Machine: Enigma," *Cryptologia*, 25(3):161-173.
2. Anon. 1937. "Telegram from HQ General Franco to Fifth Army Corps." Archivo General Militar de Ávila. Ávila. Archive Signature: C.1302,7,1/4.
3. Anon. 1939. "Telegram from HQ General Franco to Fifth Army Corps." Archivo General Militar de Ávila. Ávila. Archive Signature: C.1308,30,1/1.

4. Bargoni, F. 1995. *Participación naval italiana en la Guerra civil española 1936–1939*. Madrid: Instituto de Historia y Cultura Naval.
5. Batey, M. 2009. *Dilly: The Man Who Broke Enigmas*. London: Dialogue, Biteback Publishing.
6. Batey, J. K., Batey, M. E., Rock, M., and Twinn, R. F.G. 1945. "A History of the Solution of Unsteckered Enigmas and Abwehr Machine Cyphers 1941–1945." GC&CS Secret Service Sigint Volume II: Cryptographic Systems and their Solutions. I: Machine Cyphers, The British National Archives. Kew, London. TNA PRO HW 43/7, Document retained by GCHQ under Section 3.4 of the Public Records Act.
7. Bertrand, G. 1973. *ENIGMA ou la plus grande énigme de la guerre 1939–1945*. Paris: Librairie Plon.
8. Bloch, G. 2001. "Chiffrement, décryptement et intoxication durant la seconde guerre mondiale." In *"Le chiffre, le renseignement et la guerre", Actes du colloque de l'Historial de la Grande Guerre*, Peronne.
9. Erskine, R. 1997. "Eavesdropping on 'Bodden': ISOS v. the Abwehr in the Straits of Gibraltar," *Intelligence and National Security*, 12(3):110-129.
10. Franco, L. M. and García, J. M.M. 2001. *Legión Cóndor: La historia olvidada*. Valladolid, Spain: Quiron Ediciones.
11. González Álvarez, M. 2005. *Operación 'Fuego Mágico'*. Valladolid, Spain: AF Editores.
12. Hamer, D. H. 2000. "G-312: An Abwehr Enigma," *Cryptologia*, 24(1):41-54.
13. Hammarborg, A. 1954. "Catalog of Enigma Cipher Machine Wirings." Technical Information Division, Bibliographic Research Branch, June 1954. Top Secret FROTH. Released under FOIA., National Security Agency. Washington.
14. Heiberg, M. and Ros Agudo, M. 2006. *La trama oculta de la guerra civil*. Barcelona, Spain: Editorial Critica.
15. Kahn, D. 1992. *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943*. London: Souvenir Press Ltd.
16. Kozaczuk, W. 1984. *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two*. London: Arms and Armour Press.
17. Kruh, L. and Deavours, C. 2002. "The Commercial Enigma: Beginnings of Machine Cryptography," *Cryptologia*, 26(1):1-16.
18. Leitz, C. 1996. *Economic relations between Nazi Germany and Franco's Spain: 1936-1945*. Oxford: Oxford University Press.
19. Leitz, C. 1996. Nazi Germany's Intervention in the Spanish Civil War and the Foundation of HISMA/ROWAK. In *The Republic Besieged: Civil War in Spain 1936–1939*, edited by Paul Preston and Ann L. Mackenzie. Edinburgh: Edinburgh University Press.
20. Marks, P. 2001. "Umkehrwalze D: Enigma's Rewirable Reflector - Part I," *Cryptologia*, 25(2):101-141.
21. Martin de Pozuelo Dauner, E. 2007. *Los secretos del franquismo*. Barcelona, Spain: La Vanguardia Ediciones S.A.
22. Quirantes, A. 2004. "Model Z: A Numbers-Only Enigma Version," *Cryptologia*, 28(2):153-156.

23. Quirantes, A. 2003. Taller de Criptografía. [Online]. http://www.cripto.es/enigma/boletin_enigma_15.htm#5. Last visited: 01/02/2010.
24. Quirantes, A. 2009. Taller de Criptografía. [Online]. http://www.cripto.es/museo/rotor.htm. Last visited: 01/02/2010.
25. Soler Fuensanta, J. R. 2004. "Mechanical Cipher Systems in the Spanish Civil War," *Cryptologia*, 28(3):265-276.
26. Soler Fuensanta, J. R. 2004. *Missatges secrets*. Ibiza, Spain: Editorial Mediterrània-Eivissa.
27. Soler Fuensanta, J. R. and López-Brea Espiau, F. J. 2008. *Soldados sin rostro. Los servicios de información, espionaje y criptografía en la guerra civil española*. Barcelona, Spain: Inédita Editores S. L.
28. TICOM. 1945. "ENIGMA Documents from Heimsoeth & Rinke." Bestand Rückgabe TICOM, Politisches Archiv des Auswärtigen Amts. Berlin. Archive Signature: T 1715, T1716, T1717 and T1718.
29. Turing, A. M. 1939–42. "Turing's Treatise on the ENIGMA (The Prof's Book)." Government Code and Cypher School: Cryptographic Studies, The British National Archives. Kew, London. TNA PRO HW 25/3.
30. Türkel, S. C. 1927. *Chiffrieren mit Geräten und Maschinen*. Graz: Ulrich Mosers Buchhandlung (J. Meyerhoff).
31. West, N. 1986. *GCHQ: The Secret Wireless War 1900–86*. London: Weidenfeld & Nicolson.