received: 2021-06-23 DOI 10.19233/ASHS.2023.01

ENIGMA M4 CIPHER MACHINE FROM THE WRECK OF THE GERMAN MINESWEEPER R 15 NEAR UMAG

Andrej GASPARI
University of Ljubljana, Faculty of Arts, Department of Archaeology, Aškerčeva 2, 1000 Ljubljana, Slovenia
e-mail: andrej.gaspari@ff.uni-lj.si

Danijel GERMEK
Navtika Water Sports Association, Obala 125, Lucija, 6320 Portorož, Slovenia
e-mail: d.vodnihsportov@gmail.com

Aleš JELINČIČ
National Museum of Contemporary History of Slovenia, depot Pivka, Kolodvorska cesta 51, 6257 Pivka, Slovenia
e-mail: ales.jelincic@muzej-nz.si

Miha HREN
Slovenian National Building and Civil Engineering Institute, Dimičeva ulica 12, 1000 Ljubljana, Slovenia
e-mail: miha.hren@zag.si

Lidija KORAT
Slovenian National Building and Civil Engineering Institute, Dimičeva ulica 12, 1000 Ljubljana, Slovenia
e-mail: lidija.korat@zag.si

Danijel FRKA
Sušilo 13, 51262 Kraljevica, Croatia
e-mail: danijel.frka@gmail.com

ABSTRACT

In 1984–1986, Zvonimir Kralj, diver and keeper of the Piran Aquarium, recovered the Enigma cipher machine with codebook and several other items from the wreck of the German minesweeper R 15 sunk off the west coast of Istria between Savudrija and Umag. The article describes and defines the device and outlines the technical characteristics of the minesweeper of the 6th Minesweeper Flotilla (6. Räumbootsflottille) of the German Kriegsmarine, which was hit by the British torpedo boat MTB 409 on the night of April 16–17 1945, and sank about 3 nautical miles northwest of Umag. An examination of the preserved parts of the cipher machine revealed that it was a naval Enigma M4 with four rotors and a reflector C. An X-ray microtomography showed the serial number of the machine M 15648 and the last configuration, left to right: C/γ (Gamma), III, VI, IV. The external position of the Gamma rotor (»P«) indicates that the Enigma was not set in a mode compatible with the M3 model, which corresponds to the cipher keys for the last two months of the war.

Keywords: Adriatic, Istria, Second World War, Kriegsmarine, Minesweeper R 15, 6. Räumbootsflotille, Cipher machine, Enigma M4, Archaeological remains

LA MACCHINA CRITTOGRAFICA ENIGMA M4 RECUPERATA DAL RELITTO DEL DRAGAMINE TEDESCO R 15 PRESSO UMAGO

SINTESI

Negli anni 1984–1986, Zvonimir Kralj, sommozzatore e custode dell'acquario di Pirano, recuperò una macchina crittografica Enigma con un cifrario e pochi altri oggetti dal relitto del dragamine costiero tedesco R 15, che affondò al largo della costa occidentale dell'Istria fra Salvore e Umago. L'articolo fornisce una descrizione

del dispositivo e un schema delle caratteristiche tecniche del dragamine appartenente all 6. flottiglia dragamine (6. Räumbootsflottille) della Kriegsmarine tedesca. Il R 15 fu colpito dalla torpediniera britannica MTB 409 nella notte tra il 16 e il 17 aprile 1945 e affondò a circa 3 miglia nautiche a nord-ovest di Umago. Un esame dei resti della macchina crittografica ha rivelato che si trattava di un modello della marina, l'Enigma M4, con quattro rotori e una bobina di rinculo di tipo C. L'esame microtomografico computerizzato a raggi X ha rivelato il numero di serie della macchina M 15648 e l'ultima impostazione, vista da sinistra a destra: C/γ (gamma), III, VI, IV. La posizione esterna del rotore gamma (»P«) indica che l'Enigma non è stato impostato in modo da consentirgli di scambiare messaggi con la macchina a tre rotori (M3), il che corrisponde alle chiavi in uso negli ultimi due mesi della guerra.

Parole chiave: Adriatico, Istria, seconda guerra mondiale, marina tedesca, dragamine costiero R 15, 6. Räumbootsflotille, macchina crittografica, Enigma M4, resti archeologici

INTRODUCTION

Through the intervention of Danijel Germek, The Park of Military History Pivka received a precious museum exhibit at the end of 2020 – a German cipher machine Enigma M4, which was found in the mid-1980s by a well-known Piran diver Zvonimir Kralj amongst the wreckage of the minesweeper R 15 sunk along the west coast of Istria between Savudrija and Umag. This study expands upon the data from the initial online posts and media reports with a more complete description and identification of the machine and an outline of the technical characteristics and history of the minesweeper R15 of the 6th Minesweeper Flotilla (6. Räumbootsflottille) of the German Kriegsmarine, which operated in the second half of the war off the coasts of Dalmatia, Kvarner and Istria. In order to provide context, the study concisely presents the military and historical circumstances of naval warfare in the central and northern Adriatic following the capitulation of Italy, focusing on the operations of the German Navy.

SUMMARY OF THE NAVAL ACTIVITY IN THE ADRIATIC FROM SEPTEMBER 1943 TO MAY 1945

Following the capitulation of Italy on 8 September 1943, most of the Italian fleet set off from Taranto towards Malta where it joined the Allies. The Germans managed to disarm Italian forces in Rijeka, two divisions in northern and central Dalmatia and all of their forces in southern Dalmatia and Herzegovina, while the rest surrendered to the Partisans. This resulted in large numbers of Italian arms and equipment ending up in the hands of the Partisans. After the Yugoslav National Liberation Army linked up with the Allies, a base for the British Coastal Forces was established in Komiža on Vis Island in the beginning of January 1944. Allied presence on this island reached almost 2000 soldiers in the first half of 1944 (Vasiljević, 1972).

At the time of the capitulation of Italy, the German Navy (Deutsches Kriegsmarine – DKM), did not have any significant naval units in the Adriatic. The Germans found a large number of Italian warships and support vessels in Italian ports. They captured one cruiser, one support cruiser, 4 torpedo boats, 6 escort boats, 1 submarine chaser, 2 commando submarines, 2 minelayers and 6 support vessels. Apart from the transfer of their naval forces from the Mediterranean, the Germans also organized land transport of smaller vessels (motor torpedo boats and motor minesweepers) from the Ligurian Sea to the Adriatic. The lack of professional naval personnel was a serious concern, so the Germans transferred some of their units from Norway and southern France, while they also used personnel from the navy of the Independent State of Croatia. The Germans divided the Adriatic into four operating districts, of which the northern Adriatic, Dalmatia and the southern Adriatic were under the Commanding Admiral Adriatic (Kommandierender Admiral Adria). He ordered the formation of the 11th Security Division which included all of the captured Italian torpedo boats and destroyers as well as some armed steamboats. From October 1943 onwards, the Adriatic was the theatre of operation for the 1st Motor Torpedo Boat Division (1. Schnellbootdivision) and the 3rd S-Flotilla (initially 4, later 8 torpedo boats), with 8 small ships of the 7th S-Flotilla set to join them. The German 24th S-Flotilla received the former Italian motor torpedo boats (MS), but was disbanded in October 1944 with the 3rd S-Flotilla obtaining the remaining boats. February 1944 saw the formation of the 11th Security Division based in Trieste which operated in coordination with the 1st Motor Torpedo Boat Division. It consisted of the 1st and 2nd Escort Flotillas (Geleitflotille), the 2nd Submarine Chaser Flotilla (U-Jagdflotille) and the 6th Minesweeper Flotilla. The division was added the 6th Transport Flotilla (Transportflotille) and the 10th Landing Craft Flotilla (Landungsflotille). After the 1943/1944 winter operations, the Germans controlled the entire coastal belt and all the islands except for Vis and Lastovo. The key task for the Germans was the defence of their maritime traffic, and the defence of the coast and islands from a potential Allied landing (Freivogel & Rastelli, 2014).

For the Partisans, the main concern was the immediate danger of a German raid on Vis Island, the last base of the combined forces of the Yugoslav National Liberation Army and the Allies. The light coastal forces of the British Royal Navy in Komiža had at their disposal a squadron of motor torpedo boats and motor gunboats as well as patrol boats and coast guard boats. As a base and port of departure for British motor torpedo boats and motor gunboats, Komiža represented the ideal base for offensive operations against German maritime traffic in the corridors between the islands of central and southern Dalmatia. Their operation was initially extremely aggressive and resulted in successes which importantly endangered German maritime communications in the Adriatic. Since January 1944, the combined Allied and Partisan forces carried out raids on German garrisons on the islands of Korčula, Šolta, Hvar, Mljet and Brač, and drew a large number of German forces from the interior to the coast (Freivogel & Rastelli, 2014).

For the Germans, maintaining maritime transport along the eastern coast of the Adriatic was an absolute priority. Despite the constant British night attacks on their convoys, the Germans managed to maintain maritime connections between their ports up until October and November 1944 when they evacuated their forces from southern and central Dalmatia. During the year of 1944, German naval

forces suffered heavy losses. In a firefight on the night of 29 February 1944, French light cruisers Le Terrible and Le Malin sank the corvette UJ 201 Egeria and a large transport vessel, and inflicted heavy damage on a torpedo boat. In the evening hours of 18 March, the torpedo boat TA 36 Stella Polare hit a mine off the eastern coast of Istria and sank. Later in the month on 27 March, the corvette UJ 205 was sunk during a British fighter-bomber raid on the Port of Split and, on the same day, 14 British fighter-bombers attacked and sunk minesweepers R 188 and R 189 in the Port of Povlja on Brač Island, two assault boats on Korčula Island and two in Dubrovnik. Over the course of the next few days, Allied aircraft sank another 5 assault boats and a twin-hull landing ship in the waters of Brač and Hvar islands. In the Allied bombings of the Breda Shipyard in Mestre in February and March 1944, the corvette UJ 207 was destroyed and UJ 206 was heavily damaged which left the 11th Security Division with only the torpedo boat TA 20 in combat-ready condition. The situation with its motor torpedo boats was no better (Freivogel & Rastelli, 2014).

On 27 April 1944, partisans captured a special anti-partisan ship (later part of the Yugoslav National Liberation Army's Navy with the designation NB 11 Crvena zvijezda). In order to clear the islands of partisan activity, the Germans went ahead with operation Wikinger-Feuerzange and landed on Dugi otok on 31 May; escort was provided by the 11th Security Division. As a result of the German airborne and ground assault named Operation Roesselsprung (knight's move) – an attempt to destroy the supreme command of the Yugoslav National Liberation Army and Marshall Tito in Drvar on 25 May, which pulled German forces towards the coast, a joint partisan and Allied assault on Brač Island was launched from Vis Island. The period between June and August 1944 saw the beginning of the German retreat from all battlefields. At this time, with the addition of the newly constructed vessels and the transfer of a large number of landing ships to the Adriatic, the German Navy in the Adriatic was at the peak of its strength. In the second half of July, British motor torpedo boats and motor gunboats launched a few consecutive night attacks on several German convoys in the Mljet Canal and the waters around Korčula Island, sinking several boats, but suffering considerable losses themselves. British attacks continued in August when on the night of 10-11 August near Vir Island, British boats sank a landing vessel and heavily damaged a second one. On the night of 17-18 August, they sank a German assault boat, two escort boats and a small tanker in the Mljet Canal, while the motor torpedo boat S 57 was sunk the following night. On 17 August, torpedo boat TA 35 Giuseppe Dezza hit a mine near the Brijuni Islands and sank. The final three months of 1944 saw further German retreats and the liberation of a large part of Dalmatia. In the period from September to November 1944, British Coastal Forces launched attacks on German convoys that participated in the evacuation of German forces from around Šibenik and Zadar, and also acted as support vessels for the landing of partisan forces on the coast and islands of southern and central Dalmatia. From their base in Ancona, vessels of the Coastal Forces could operate all the way to Venice and Trieste. Following the liberation of Zadar, the British established a new major base of the Coastal Forces there. The Germans began laying mines on all sea access routes leading to crucial ports. The 11th Security Division was dealt its biggest blow on the night of 1 November 1944 when two British destroyers together with 7 boats of the Coastal Forces sunk German corvettes UJ 202 Melpomene and UJ 208 Spingarda and the torpedo boat TA 20 Audace near the island of Škrda (Operation Exterminate). In just one night, the Germans thus lost three irreplaceable military vessels and nearly 300 crew members. In the Allied bombing of Rijeka on 5 November 1944, the minelayer Kiebitz was sunk along with the torpedo boat TA 21 Indidioso, patrol boat G 104 of the Independent State of Croatia's Navy and a rescue boat Arpione. The 2nd Escort Flotilla was down to the torpedo boat TA 48, which was constantly in for repairs, corvette UJ 205, which was still being outfitted, and the old minelayer Fasana (Freivogel & Rastelli, 2014).

In the following months, the Germans focused on commando operations with explosive boats and folding kayaks, the base for which was in the Čikat Bay near Mali Lošinj. The Allies launched several combined airborne and naval attacks on the base in Čikat (18/19 November, 2 December, 17 December and 22/23 December 1944), but did not manage to destroy the base or stop the German commando activities. It was the Allies who suffered the biggest loss when the British destroyer HMS Aldenham hit a mine near Škrda Island on 14 December, broke in half and sank (Mason, 1988). The most significant German naval commando attack came on 12 February 1945 when three explosive boats attacked the Port in Split where they managed to inflict heavy damage upon the British cruiser HMS Delhi (Freivogel & Rastelli, 2014).

On the night of 12-13 April 1945, British motor torpedo boats sank the torpedo boat TA 45 Spica near Novi Vinodolski and on 16 April 1945, Allied motor torpedo boats and motor gunboats used a torpedo to sink the minesweeper R 15 near Umag, which practically ended any combat activity of the 6th Minesweeper Flotilla (Pope, 1998). Rijeka was liberated on 3 May and a day earlier, on 2 May 1945, the Yugoslav Army launched an attack on the fortified base in Pula, from where all the remaining seaworthy motor torpedo boats of the 3rd S-Flotilla of the 1st Motor Torpedo Boat Division set off for Ancona where

they surrender to the Allies. On 1 May 1945, surrounded by the Yugoslav Army in Trieste, the Germans scuttled the TA 40 and TA 43, and then proceeded to evacuate their naval forces along with the remaining support vessels and strand them at the mouth of the Tagliamento River where they surrendered to the Allies. This was the final action of the German Navy in the Adriatic (Birnbau & Vorsteher, 1987, 339–342).

CHARACTERISTICS OF THE GERMAN NAVY'S OPERATION IN THE ADRIATIC

The German Navy began its combat activities in the Adriatic exclusively with the captured military vessels and equipment of the former Italian Navy and operated out of the former Yugoslav and Italian ports. It took great effort and transferring small units by sea and land to the Adriatic, but by the middle of 1944, its power had been constantly increasing, although it did suffer heavy losses due to the Allied superiority in the air and, eventually, on the sea. A critical strategic mistake was abandoning the plans to take Vis Island. Contemporary former Italian Arieleclass torpedo boats were the strongest boats in the Kriegsmarine in the Adriatic, but their numbers were insufficient to maintain German sea superiority in the region. German motor torpedo boats were one of the main combat units which, despite not having specific objectives, bore the brunt of the combat activities. Their diesel fuel was less dangerous than the petrol used by British boats, but due to their light armament, they were no match for British boats in gun combat. The small R-class motor minesweepers were successful in battles against small partisan ships and corvettes – Italian Gabbiano-class submarine chasers, were serious adversaries to the British motor torpedo boats and motor gunboats, but there were too few of them and their numbers kept dwindling as a result of Allied activities. If the crews were aggressive enough, then the well-armed German landing vessels and assault boats could go toe to toe with British and partisan boats, but they were vulnerable due to their lack of armour and slow speed. The greatest threat to transport vessels and one that was difficult to hide from and defend against was the Allied Air Force which operated in the entire area of the Adriatic from the end of 1943 till the end of the war.

Since the large German submarines of the 29th Submarine Flotilla did not have a permanent base on the western coast of the Adriatic and only occasionally used the Port of Pula as an auxiliary base, mainly for repairs, their presence in the Adriatic was barely felt at all. However, in the final phase of the war, after losing the majority of the surface military vessels, the Germans resorted to commando warfare. They introduced navy commandos and explosive boats into the fight and were also planning to implement commando submarines, but they eventually ran out of time. Especially effective was the German mine warfare. Minelaying duties were performed by purpose-built minelayers, but also by merchant ships (e.g. the motor boat Kiebitz), tank carriers, motor torpedo boats and even torpedo boats, which laid several thousand mines of different types in 1944 and 1945. Mines were responsible for sinking a great number of Allied (but also German) ships and their presence was still felt years after the end of the war when many merchant ships sank in uncleared mine fields (Freivogel & Rastelli, 2014).

OUTLINE OF THE CHARACTERISTICS OF GERMAN LIGHT MINESWEEPERS OF THE FIRST SERIES

The light minesweepers (Ger. Minen-Räumboote or Räumboote; also R-Boote) belonged to the coastal vessels of the German Kriegsmarine and their development goes back to the time of the First World War. The prototype of the first series of minesweepers, to which the R 15 belonged, was designed by the Lürrsen shipyard in 1931, while the manufacture of the majority of this series of vessels and the adjustment of their dimensions deriving from the tests at sea was taken over in 1932–1934 by the companies Abeking & Rasmussen (R 2–R 7 and R 9–R 14) and Schlichting-Werft (R 15 and R 16). The vessels of the first generation were 24.5–27.8 m long, had a beam of 4.38–4.5 m, while their side height was 1.95–2.35 m. They had 1.12–1.58 m of draught and a displacement between 43.5 and 52.5 tonnes (Jung, Maass & Gröner, 1999, 190–191; Historisches Marinearchiv, 2022).

R-Boote of the first generation were envisioned exclusively as minesweepers in coastal waters, especially near river mouths and ports (Breyer, 1994, 90). The main requirement during the design process was that the vessels are as non-magnetic as possible, very manoeuvrable and not too large, but the minesweepers of the first series turned out to be too small. The slender, low-profile vessels were made in a composite technique with a framework of transverse and longitudinal steel and lightweight metal joints, and diagonally overlapping double planking of mahogany (»Quer- und Längsspant-Stahl-Leichtmetall-Mahagoni-Doppeldiagonalkraweel-Kompositbau«). Minesweepers of the first series had a raised forecastle, which makes them easily distinguishable from the later R-Boote variants with a more flush-decked appearance. The Lürrsen Company was the main manufacturer of fast torpedo boats (ger. Schnellboote; also S-Boote), which is where the similarity of the light minesweepers and the S-Boote comes from. Due to their lightweight construction, these minesweepers were known to shake heavily while firing its guns. They had five watertight bulkheads, the first one also being reinforced against collision damage. Explosive

charges for scuttling were placed in the engine room, radio room, crew room in the stern and one in the NCO room at the beginning of the bow of the vessel (Williamson, 2009, 15–16; Paterson, 2017).

Light minesweepers were powered by two four-stroke 6-cylinder diesel engines MWM (Motoren-Werke Mannheim) RS-127-SU with a combined output of 770 HP.[1] Two 0.85-m propellers enabled a top speed of 19.85 knots and provided enough power for towing minesweeping devices even in rough seas with a wave height of 6 according to the Beaufort scale. The minesweeper R 8 was a bit wider than the rest of the first series and was equipped at Lürrsen with new Voith-Schneider 1.5-m propellers (with blades that rotate around a vertical axis and are fitted to the circular rotor at a 90-degree angle), which generated thrust in all directions, combining propulsion and steering into a single unit. Due to the exceptional manoeuvrability afforded by this new type of propeller, they were installed on most of the minesweepers from the R 17 onwards. During the war, the displacement of the minesweepers kept gradually increasing from series to series and finally reached approximately 160 tonnes, however, the basic construction never changed. This is why the R-Boote were all very similar and were difficult to distinguish based on their series (Breyer, 1994, 91).

The crew of the R-class light minesweepers, which at first numbered 15 to 18 men and later more than 20, was typically comprised of the engine room crew (an NCO – Maat and three sailors – Matrosen per shift), each at their post below deck, and 6 men per shift on deck – an NCO on the front 20-mm gun, a sailor on the 20-mm gun on the stern (if mounted, otherwise the space was occupied by two lookouts, each responsible for covering around a 100-degree angle on each side), two sailors-lookouts on the bridge for the left and the right side (with two searchlights), a sailor-helmsman and a sailor-telegrapher. The captain of the vessel, usually a company-grade officer or an NCO, was constantly present on the bridge.

Minesweepers operated in pairs – Rotte, which was led by the command ship and its senior officer or pair commander (Rottenführer) while the commander of the second vessel – Rottenboot was usually an Obersteuermann (ObStrm). Apart from minesweeping, the R-Boote were also used for mine laying, to which end they were fitted with a total of 6 and later 12 mines at the sides of the stern. They would occasionally also carry depth charges, which were simply rolled overboard. All vessels were equipped with a device for reducing the magnetic signature of the ship (Mineneigenschutzgerät). R-Boote used three different towing devices for minesweeping. The first two: MPG – Motoren Pinass Gerät and KRG – Körb Räum Gerät, were composed of a long steel cable strung between two or more ships. MPG used guiding kites, whereas KRG used a form of iron basket for depth keeping. Both sweeps were armed with explosive cutters (ger. Sprenggreifer). The third method, SDG – Scheer Dracen Gerät, is a double sweep towed by one ship. It consists of two searching wires attached to a paravane (glider) and floats.

The armament of a light minesweeper initially consisted of one, and with later R-Boote variants up to four 20-mm anti-aircraft guns (FlaK 38). They were considered easy targets for Allied aircraft and were continuously being attacked, but still managed to inflict some losses, which is documented by the symbols and the dates of kills on the outside of the wheelhouse. In the latter part of the war, two 7.92-mm MG 34 machine guns were normally mounted on the bridge, while this increasingly hard-to-get weapon was replaced with other types of machine guns on other minesweepers. The crew's quarters usually contained up to four MP38/40 submachine guns. After initial combat experience, the wheelhouse and bridge, which is located on an elevated platform behind the wheelhouse, were fitted with armoured plating 10–12 mm thick. Shields of the same thickness were added to the guns as well.

Light minesweepers proved to be very robust and universally useful, which is why they were often used for other assignments, e.g. escorting convoys and submarines heading out or returning from battle, patrolling and sea rescue, unit transportation and, especially in the Adriatic, even anti-partisan warfare.

Out of the total of around 300 R-Boote, half were sunk for different war-related reasons, a few of them by their own crews after the cessation of hostilities, while 140 vessels were captured by the Allies. The Soviets kept them in service into the 1960s and some were returned by the USA to West Germany after joining NATO (Breyer, 1994, 104–105).

HISTORY OF THE R 15

The R 15 was launched in the Schlichting-Werft shipyard in Trävemunde on 3 May 1934 under the serial number (Bau-Nr.) 792 and was introduced to the 6th Flotilla in September 1941. Minesweepers of this flotilla arrived using continental waterways to Port Saint Louis at the mouth of the Rhone on the Mediterranean coast in February 1942. They were later moved to the harbour in La Spezia for overhaul and outfitting. From April 1942 onwards, they served along the Libyan coast as support and supply vessels for ground units. After the defeat of the German

1 A pair of engines of the same type (RS 127 S), combined with two electric motors, was installed in the Type II U-boats, produced between 1935 and 1940 (Rössler, 1999, 74).

Figure 1: German light minesweeper (Minen-Räumboot) R 15 on the North Sea on 5 November 1934. Length (LOA) 27.75 m; beam 4.38 m; depth 2.15 m; draught 1.36 m; displacement 52.5 t (Source: Sammlung Dressler, Württembergische Landesbibliothek, Stuttgart; Bildarchiv: 18-0701-a).

forces at El Alamein, the R 15 left Tobruk on 12 November 1942 as the last German ship and later took part in the unit supply in Tunisia. From the end of the African campaign until December 1943, the 6th Flotilla took part in escort and minesweeping tasks along the shores of the Tyrrhenian Sea and in January 1944 it was redeployed to the Adriatic. Together with torpedo boats, seven of the remaining minesweepers of the 6th Flotilla were transported by road from Genova to Piacenza and then along the Po River to Venice where they were assembled and outfitted in the local Arsenal between February and March 1944 (Räumboots-Flottillen, 2022; 6. Räumbootsflottille, 2022). From July 1943 onwards, the 6th Minesweeper Flotilla was commanded by Lieutenant Commander (Kapitänleutnant) Walter Klemm.

The 6th Minesweeper Flotilla was part of the 11th Security Division (11. Sicherungsdivision) under the higher Commanding Admiral Adriatic (Kommandierender Admiral Adria), which consisted of two Escort Flotillas (1. and 2. Geleitflottille) with torpedo boats or escort destroyers (TA-Torpedobootausland) and the 2nd Submarine Chaser Flotilla (2. Unterseebootjagdflottille). In the second half of 1944, they added the 6th Transport (6. Transportflottille) and the 10th Landing Craft Flotilla (10. Landungsflottille) with naval ferry barges/»F-lighters« (MFP), double hull barges, pontoons and tugboats. In the Adriatic, there were three other concurrently operating Torpedo Boat Flotillas (3., 7. and 24. Schnellbootflottille) as part of the 3rd Division, and a Minelayer Group (Freivogel & Rastelli, 2014, 165–170). The activity of German submarines in the Adriatic was negligible compared to the First World War. The port of Pula, which was one of the bases of the 29. Unterseebootsflottille, was in operation as a U-Stützpunkt until the end of July 1944. The scuttling of the last two submarines of the same flotilla that have already been badly damaged by air assaults (U-565 and U-596) in Scaramanga Bay in front of the base in Salamina in the Saronic Gulf in September of the same year signalled the end of the German submarine activity in the entire Mediterranean (Alman, 1985; Paterson, 2019, 280–282).

At the end of November 1944, the Commanding Admiral Adriatic was disbanded and the 11th Security Division was transferred to the Naval High Command South (Marineoberkommando Süd), which was responsible for the rest of Adriatic. From April 1944 onwards, minesweepers of the 6th Flotilla were carrying out missions along the Istrian and Dalmatian coast from their bases in Opatija and Pula. A military journal of

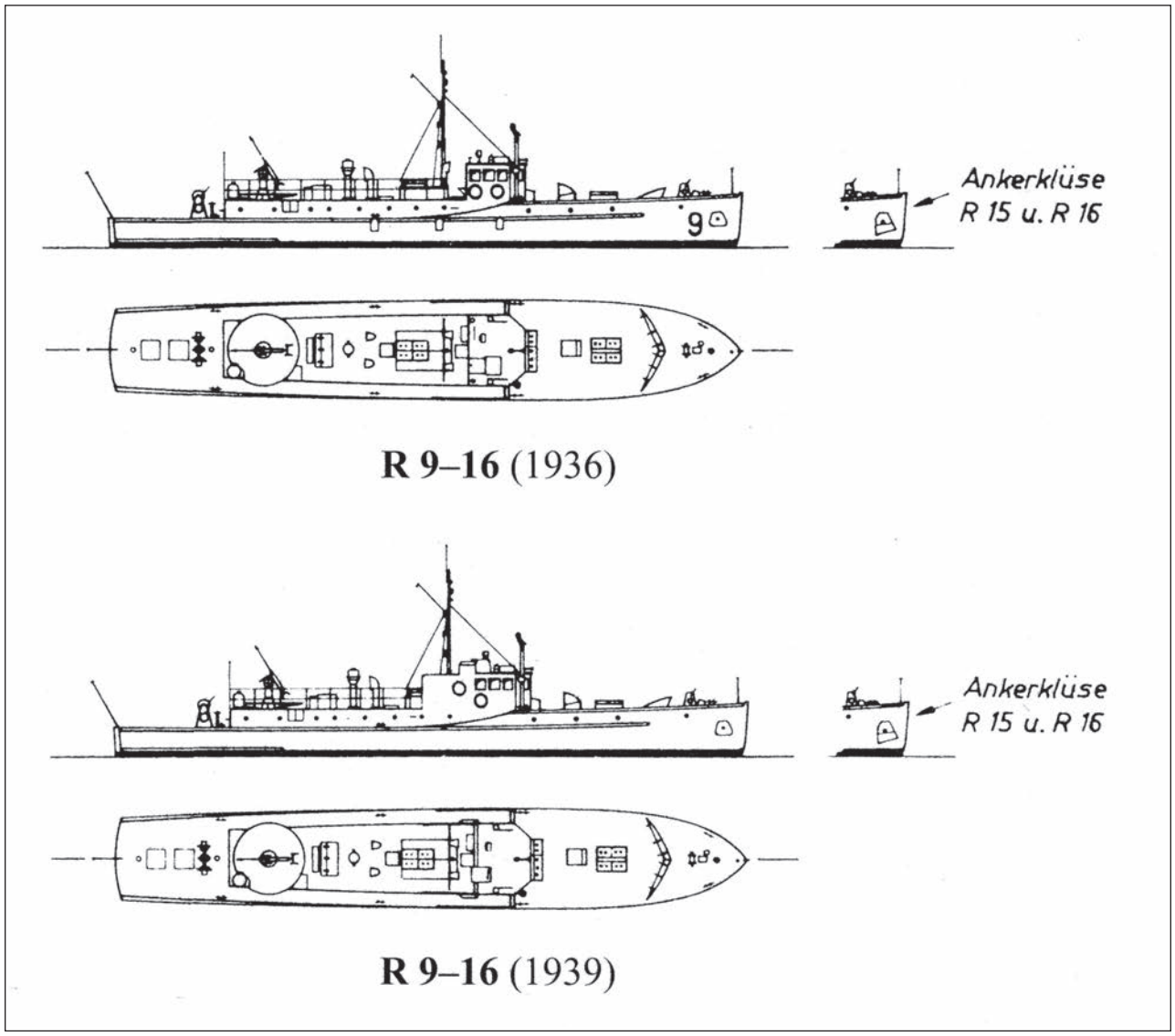


Figure 2: Groundplan and side view of the minesweepers R 9 to R 16 in their original form (1936) and after the refurbishment in 1939 (Drawing: Franz Mrva; Source: Dieter, Maass & Gröner, 1999, 193).

the unit[2] from 13 April[3] and 8 June 1944[4] reveals that the R 15 was additionally armed with an MG 15 (7.92 mm) and another 15-mm machine gun (perhaps an old version of the MG 151) instead of the more standard double MG 34, which were becoming very scarce at that point in the war. On the night of 5–6 August, the R 15 and R 16 got entangled into a battle with the partisan patrol boat PČ-22 Streljko in the Murter Channel.[5] A few days later, on 12 August, torpedo boat S 629 collided with the R 15 near Šibenik. The damage was quite extensive and the R 15 was leaking heavily and only returned to duty on 31 August after

2 The Croatian translation of the military journal belonging to the commander of the 6th Flotilla from 1 January to 15 September 1944 and from 31 January to 15 February 1945 was generously offered to us by Danijel Frka. It is one of the translations of military journals of the units of the Kriegsmarine in the Adriatic which are based on the material from NARA and used to be kept by the former Military and Maritime Museum (today Croatian Maritime Museum) in Split. Frka obtained the copies of the journals from the museum's former director, Vladimir Isaić.

3 NARA, PG 73451.

4 NARA, PG 73452.

5 NARA, PG 46525, p. 303.

more than two weeks of repairs in the base of Pula.[6] During this period, the R 15 was performing escort, casualty transport and patrol duties and was involved in anti-partisan activities on the islands.

Due to the increasingly frequent air attacks, German ships had to navigate mostly at night when they were harder to spot. Additionally, the Allies started laying mines of their own along German navigation routes. In the early morning of 5 September 1944, the R 15 and R 12 were on minesweeping duty near Lovrečica close to Umag when a mine detonation proved fatal for the R 12. When pulling out the sweeping device, a mine hit the stern and detonated, which resulted in the sinking of the minesweeper and the death of half of its 20-man crew.[7] In the morning of 23 September, the R 15 was hit several times by partisan machine gun fire while sailing through the Pašman Canal, but it did not sustain any serious damage or casualties.[8]

From October 1944 onwards, the operational area of the 6th Flotilla, which at the time numbered around 373 men, became increasingly focused on the territory between the Kvarner Gulf and Venice due to the partisan advancement in the coastal area of central Dalmatia. In the Allied air attack on the island of Rab on 5 November, the R 15 suffered several light hits and was kept in Pula for repairs until 22 November 1944.[9] During the second half of December 1944 and the middle of January 1945, the R 15 took part in two mine missions, »Alpha 1« and »Alpha 4 Ost«. On 20 January 1945, the R 15 and R 16 headed to Cres with the Chief of Staff MOK Süd. Winter conditions in the Kvarner Gulf took their toll on the R 15. In January 1945, windy conditions and rough seas caused damage and the R 15 took in a lot of water, which is why it was relegated to the Pula shipyard from the end of the month until 10 February. Between 11 and 15 February, when the military journal of the 6th Flotilla ends, the R 15 did not take part in any mission. During this time, the commander of the R 15 was Corvette Sub-Lieutenant (Leutnant zur See) Storb.[10]

The deteriorating position of the German forces meant that its units were no safer moored than out at sea, as proven by the case of the R 14 which suffered irreparable damage to its bow during an air attack on the Monfalcone Port on 16 March 1945. Poor prospects for the R 15 materialized on the night of 16–17 April when the minesweeper under the command of Sub-Lieutenant (LzS – Leutnant zur See) Frieß (Paterson, 2017) was navigating waters south of Savudrija. Around 11 PM, the English detected a convoy of eight vessels, consisting of three ships and five boats. They attacked with a motor torpedo boat (70-ft US Vosper) HM MTB 409 from the 28th MTB Flotilla (c.f. Reynolds & Cooper, 1999) under the command of Lieutenant Claude Holloway and two Higgins 78' class motor torpedo boats PT 207 and PT 217 of the Yugoslav Royal Navy in exile acting as escort.[11] Due to the apparent superiority of the German convoy, MTB 409 launched its torpedoes at the last ship in the convoy and immediately headed back towards base in order to avoid a battle. One torpedo hit its target and the R 15 sank. Only five crew members managed to save themselves and among the men killed was also 21-year-old Mechanic 1st Class (Machinenobergefreiter) Wilhelm Eickerman.[12] The remaining five vessels of the 6th Minesweeper Flotilla were run aground by their crews on 2 May 1945 at the mouth of the Tagliamento and set ablaze. After a breakdown in talks with the commander of the 57th Flotilla of motor gunboats and motor torpedo boats (MGB/MTB) of the British Coastal Forces, the minesweeper crews chose to surrender to the 2nd New Zealand Division, which was part of the British 8th Army (cf. Pope, 2014, 259–266).

6 NARA, PG 46525, p. 327.
7 NARA, PG 46527, p. 426.
8 NARA, PG 46527.
9 NARA, PG 46531.
10 The entries of the accessible military journals (KTB – *Kriegstagebuch*) of the 6th Minesweeper Flotilla end with 15 February 1945 while the journals of the command of *Marineoberkommando* (MOK) *Süd* from the last few months of the war were not available at the time of writing. Original *Marineoberkommando* (MOK) *Süd* (established on 1 January 1945) documents are kept by the *Bundesarhiv*, *Abt. Militärarchiv* in Freiburg (BArch RM 35-III) while the material on microfilm is kept by the National Archive and Records Administration (NARA) in College Park in Maryland (cf. Mulligan, 2005, 139, 143, 152–153, 157–158).
11 PT 207 and PT 217 were transferred to the Yugoslav Royal Navy in exile as part of Allied military aid in October 1944 on Malta, along with six boats of the same type and a Flower-class corvette (Freivogel & Rastelli, 2014, 473).
12 The loss of the R 15 in the northern Adriatic or »bei Kap Salvore« on 16 April 1945 is documented in German sources, the originals of which were not available at the time of writing. One exception is the encrypted message from MOK *Süd* with a situational report compiled on 17 April 1945 at 8 PM. The relevant part of the message, which was intercepted on 18 April by one of the British signals intelligence collection sites (Y-station) and deciphered in Bletchley Park, translates to: »Own R-boat sunk on the level of Umago after being torpedoed.« (TNA, DEFE 3/685, p. 363, p. 363: short situation report 2000/17/4). While Claude Holloway's published memoirs only recount that the attack on the convoy resulted in the sinking of one of the »German E-Boats« (MTB Flotilla, 2014), several other sources erroneously claim that the attack on the convoy, composed of »3 MFP and 5 leichtern«, resulted in the sinking of one of the naval ferry barges (MFP – *Marinefährpram*) (cf. Faggioni, 2013, 126).

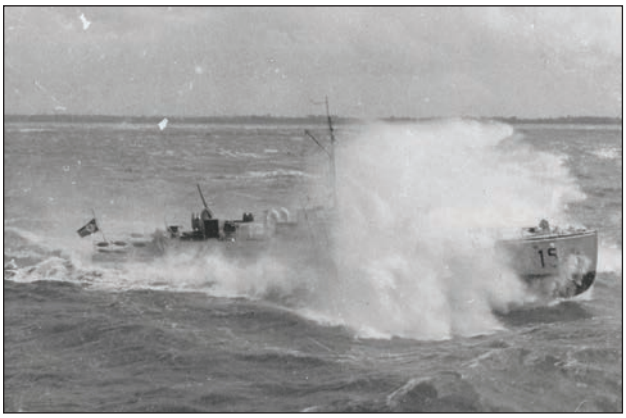


Figure 3: R 15 in rough seas (Source: Württembergische Landesbibliothek, Stuttgart).

Figure 4: The minesweeper photographed in the North African port of Derna in June 1942 could only be the R15 or R16, given the shape of the anchor hole. Since the R15 collided with MFP 149 near Ras al Hamama on 22 May and was under repair until 23 September, it is more likely to be the R16 (Source: Breyer, 1994, 90).

Figure 5: R 15 during a mission along the east coast of the Adriatic (Source: Württembergische Landesbibliothek, Stuttgart).

Figure 6: Among the remains of the wreck of the R 15 on the seabed south of Cape Savudrija is the diesel engine of the manufacturer Motoren-Werke Mannheim (Photo: D. Frka; October 2022). A pair of engines of the same type (RS 127 S), combined with two double-armature electric motors, was installed in the submarines of the type II in the years 1935–1940 (Rössler, 1999, 74).

THE FATE OF THE R 15 WRECK AND THE ITEMS SALVAGED IN THE 1980S

Some pieces of equipment from the minesweeper R 15 were salvaged immediately after the end of the war, which is possibly alluded to by the correspondence of the Port Authority Piran from 26 June 1945 (no. 73), which instructed Koper's Port Agency to salvage and dismantle »a wooden German minelayer«.[13] The wreck sitting at the depth of 25 m, approximately three nautical miles northwest of Umag, remained in a more or less integral condition all the way up to the 1980s when it was visited several times by diver Zvonimir Kralj, keeper of the Piran Aquarium. The wreck lay on the seafloor bottom side up and in the years 1984–1986, Kralj managed to salvage from it a flare gun and a backpack, which contained rusks, medical material and a bottle of water. On another occasion, he managed to salvage two MP 40 submachine guns and a case containing a device similar to a typewriter, which turned out to be the naval version of the electromechanical cipher machine Enigma M4. The Enigma was stored in a box along with a booklet (approx. 30 × 20 cm with black print), which soon disintegrated. The listed items were collected by Kralj

13 PAK PI 19.

from the inside of the hull in the middle section of the wreck where he also noticed plexi glass from the command bridge. Kralj stored the items from the R 15 along with the material from other sunken ships and airplanes in the Piran Aquarium and did his best to try and conserve them (Kralj, 2022).

Years ago, a porcelain saucer for a cup (Einsatztasse) with the markings of the manufacturer and the Kriegsmarine was also found inside the wreck of the R 15.[14] The sunken minesweeper is probably also where the 20-mm anti-aircraft gun (Flak 38) on a cone-shaped mount (Sockellefette C/30)[15] comes from. It was caught by Piran fishermen into a trawl net »south of Savudrija« in 1989 (Kralj, 2022) and is now exhibited in front of the Piran Aquarium (Fig. 7). Nowadays, only the right engine with the propeller axle, some electrical equipment and other remains can be seen on the seabed. Some time ago, the fishermen who named the wreck Ribaltada tied up the other axle and towed it, probably together with the left engine, to the shore in Umag.

Through the intervention of Danijel Germek, Kralj handed over the completely disintegrated submachine guns and Enigma remains to the Park of Military History in Pivka in 2020, which entrusted the items for conservation to Aleš Jelinčič, conservator with the Museum of Contemporary History of Slovenia. The Enigma, which was salvaged in a still integral state, has disintegrated in the three decades.

The examination of the preserved parts has revealed cracks on the edges of the plugboard, with a visible bend across the entire length of the board. All of the covers of the Bakelite switches are missing, which is odd. The same can be said for the broken axle shaft of the rotors and cipher wheels. This damage was definitely not caused after the salvage. It is almost certainly the result of a torpedo explosion as there was not enough time to sabotage the Enigma before the sinking of the minesweeper.

CONSERVATION FINDINGS AND PROCEDURES CARRIED OUT ON THE ENIGMA REMAINS

The device entered the conservation workshop completely fragmented and without its wooden box. The following parts were preserved: (1) wheel compartment with wheels and rotors and corresponding gears, (2) actuating mechanism, (3) top panel with rotor-setting windows, wheel cover lock, oval power socket and a station call window, (4) keyboard, (5) lamp panel with letters, (6) plugboard with sockets and plugs, (7) battery box, (8) parts of the case.

Figure 7: 20 mm anti-aircraft gun (Flak 38) recovered from the seafloor south of Cape Savudrija most likely originates from the minesweeper R 15 (Photo: A. Gaspari).

The conservation process began with the immersion of the preserved parts in a solvent. After the removal of the initial protective coating, the device was desalinated in distilled water for several months. Individual parts were then cleaned of sand, silt, shellfish and corrosion. The final conservation included the process of vacuum impregnation with a 20 % solution of tannin in 96% alcohol, and vacuum consolidation with a 7 % solution of Paraloid B72 in ethyl acetate. Non-metal parts were then coated with microcrystalline wax in pure gasoline.

Materials that the preserved parts were made of are listed below.

Case – sheet metal, 80–90% corroded.

Keyboard – base: sheet metal; front wall: Bakelite; keys: iron stem with spring; key cap: Bakelite with a letter made of white synthetic material; wiring: litz wire wrapped in green insulation; switch positions: brass coiled strips.

Console with light bulbs and illuminated letters – bottom wired plate: probably paper in melanite in 8 layers with a combined thickness of 1 mm (?); contacts: non-magnetic metal (brass, aluminium?); light

14 Underneath the marking of the manufacturer, the Wilhelm Jäger Porcelain Factory from Eisenberg in Thuringia, is the symbol of the *Kriegsmarine* eagle with its head turned to the left; the eagle is holding in its talons a stylized wreath, inside of which is a diagonally tilted swastika. Underneath the symbol is the letter M and the last number of the year 1941 (Porzellanfabrik, 2022).

15 The barrel jacket has the following markings (information in different lines is separated with a forward slash): »2cm Flak 38 MI / W 5319 / (?)ac / .43«, while the barrel itself has the following: »2cm Flak 38 MI / Nr 7512 / RohrNr. 1 / S / b(??)«. Different areas of the mount bear the serial number »1167« (cf.Stehr & Breyer, 1999, 3–5).

bulb base: galvanically-treated brass metal (chrome, nickel); glass bulb: flat-faced, the size of a pea; wiring: litz wire wrapped in green insulation; base mount: iron, riveted to the mount; illuminated panel with letters: black base with white letters probably applied onto a transparent synthetic panel through the process of screen printing, all together attached to the Bakelite base (with holes for the light bulbs).
Main wheel compartment with two wheels and rotors – mount: sheet metal; switchable rotors; Bakelite ring with accentuated white letters, attached to an aluminium wheel; drive gears from Bakelite (?); movable ring (one partially preserved): iron; leftmost and rightmost wheel: Bakelite.
Plugboard – base: Pertinax or Resopal (Paxolin); sockets: probably brass; pins probably brass integrated into a Bakelite body; wiring: litz wire cable wrapped in green insulation. Imprinted numbers from 1 to 26 near the contacts, accentuated with white colour.
Battery – battery inserts bound together in a box made from impregnated paper (pertinax?); paper sign of the manufacturer glued to the case (TANAX); signs visible, except for one illegible sign NR: 330 or 660 (?); insert slotted into the pertinax case (?); contacts are probably brass.

IDENTIFICATION OF THE DEVICE WITH THE DESCRIPTION OF THE LAST CONFIGURATION

The examination of the preserved parts confirmed the preliminary identification of the version of the cipher machine as the M4 model. This is evidenced by:

- wheel compartment with two wheels and four rotors; four blocking pins of the ratchet wheel; the wheel compartment cover has two preserved windows for the two wheels on the right; part of the panel just to the left is missing, but it is clear that it could accommodate two more windows);
- the upper panel has only one wheel cover lock (the M3 model had two);
- plugboard with numbered positions of pairs of sockets from 1 to 26 (with the M3 model, numbers come in combination with letters);
- the presence of single sockets for testing the 2-wire connecting cable for the plugs on the sides of the plugboard indicates that it is a cipher machine of a later make.

Only a fragment of the left edge and the attachment screws remain from the serial number plate which was attached in the middle of the bottom edge of the keyboard panel. The markings and serial numbers of the wheels and switchable rotors, which usually match the serial number of the machine, were checked using X-ray computed microtomography (microXCT) and 3D image analysis, which was carried out at the

Figure 8: The remains of the Enigma M4 from the minesweeper R 15 after conservation (Photo: A. Gaspari).

Slovenian National Building and Civil Engineering Institute. With direct observation and an xCT scan, it was possible to discern the following configuration and settings of the rotors from left to right:

- type-C reflector (UKW-c); label »C.«; serial number »M 15648«;
- so-called extra rotor (Zusatzwalze), Gamma version; label »γ«; serial number »M 15648«; external position – Grundstellung: P;
- rotor »III«; serial number »M 15648«; external position; F;
- rotor »VI«; serial number »M 15648«; external position; E;
- rotor »IV«; serial number »M 15648«; external position; Y;
- plugboard: at the time when it was last used, 10 of the 13 pairs of sockets were connected, but the cables have disintegrated, which is why the combinations of the occupied plugs could not be reconstructed. Out of the 26 sockets, 6 were unoccupied with plugs. These were: 1 (A), 5 (E), 7 (G), 9 (I), 19 (S), 26 (Z).

During the war, Naval Enigma machines were manufactured by Konsky & Krüger in Berlin and Geyr, Olympia in Erfurt, Ertel-Werk in Munich and Atlas-Werke in Bremen, all under license from Heimsoeth und Rinke. Serial numbers were assigned in blocks in the form of five-figure numbers preceded by the marking M (Marine; navy) and followed by the manufacturer's code (Heimsoeth und Rinke = jla; K&K Geyer = gvx; Olympia = aye; Ertel-Werk = bac) and

Figure 9: Enigma M4 from the minesweeper R 15; wheel compartment after conservation (Photo: A. Gaspari).

the abbreviated year of manufacturing (e.g. 44). The composite of microtomohraphic cross-sections of the reflector and the four rotors showed the serial number M 15648 in all cases. Serial numbers of machines, wheels and rotors of Naval Enigma machines usually match and the occurrence of rotors with different numbers is isolated to rare cases of completely preserved Enigma machines, where the swapping of the rotors probably happened after the war. With all that said, there is very little doubt that the Enigma recovered from the minesweeper R 15 also had the serial number M 15648. It is only a few positions older than the Enigma M4 with the marking »M15653/aye/44«, which is kept by the Royal Naval Flagship Museum in Portsmouth (Hamer, 2014). Preserved Naval Enigma machines (Hamer, 2022) from the serial number block M 15118/aye/43 to M 18428/aye/45 reveal that the Enigma M 15648 was most probably made by Olympia Büromaschinenwerke in 1944.

THE INTRODUCTION OF THE M4

The Enigma M4 was developed specifically for the submarine units of the German Navy, but the belief that it was used exclusively on submarines does not hold true and is the consequence of the flawed understanding of historical facts and the knowledge that the M4 model was the machine that brought the Allies' cryptographic war against the threat posed by German submarines in the Atlantic to a complete standstill (Weierud, 2022). Early in the Second World War, Karl Dönitz, the Supreme Commander of the German Navy's U-Boat Arm, was already concerned about the Allies' continued success against his submarines in the Battle of the Atlantic. Even though the Allies at that time were routinely reading messages encrypted with the early versions of the Enigma, the Germans were convinced that this was impossible and attributed the Allies' victories to espionage, radar detection or chance discoveries of their submarines. Despite this, Dönitz ordered the development of a special Enigma with four rotors, intended especially for submarines (U-Boote), submarine supply vessels and land bases offering support to submarine operations (Erskine & Weierud, 1987; Pröse, 2004, 42). Messages in »Triton« code (English designation »Shark«), which submarines in the Atlantic and the Mediterranean have been using since 5 October 1941, were being encrypted with Enigmas with three rotors (M3) until 1 February 1941, and after that with the new four-rotor version. The M4

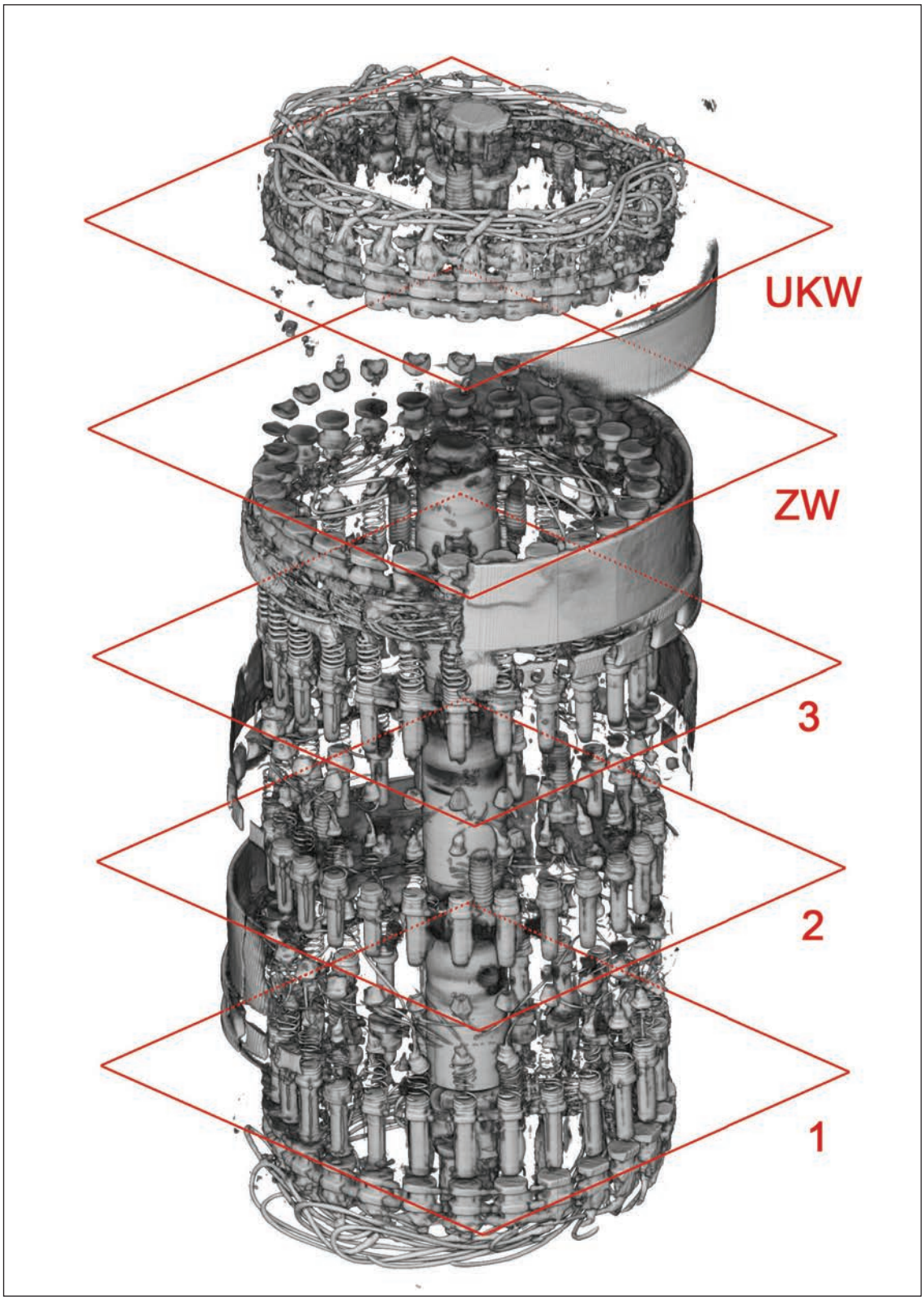


Figure 10: X-ray computed microtomography scan of the wheel block of the Enigma M4 from the minesweeper R 15, acquired with an x-ray microscope Zeiss XRadia Micro XCT-400 (3D render: Lidija Korat and Miha Hren, Slovenian National Building and Civil Engineering Institute).

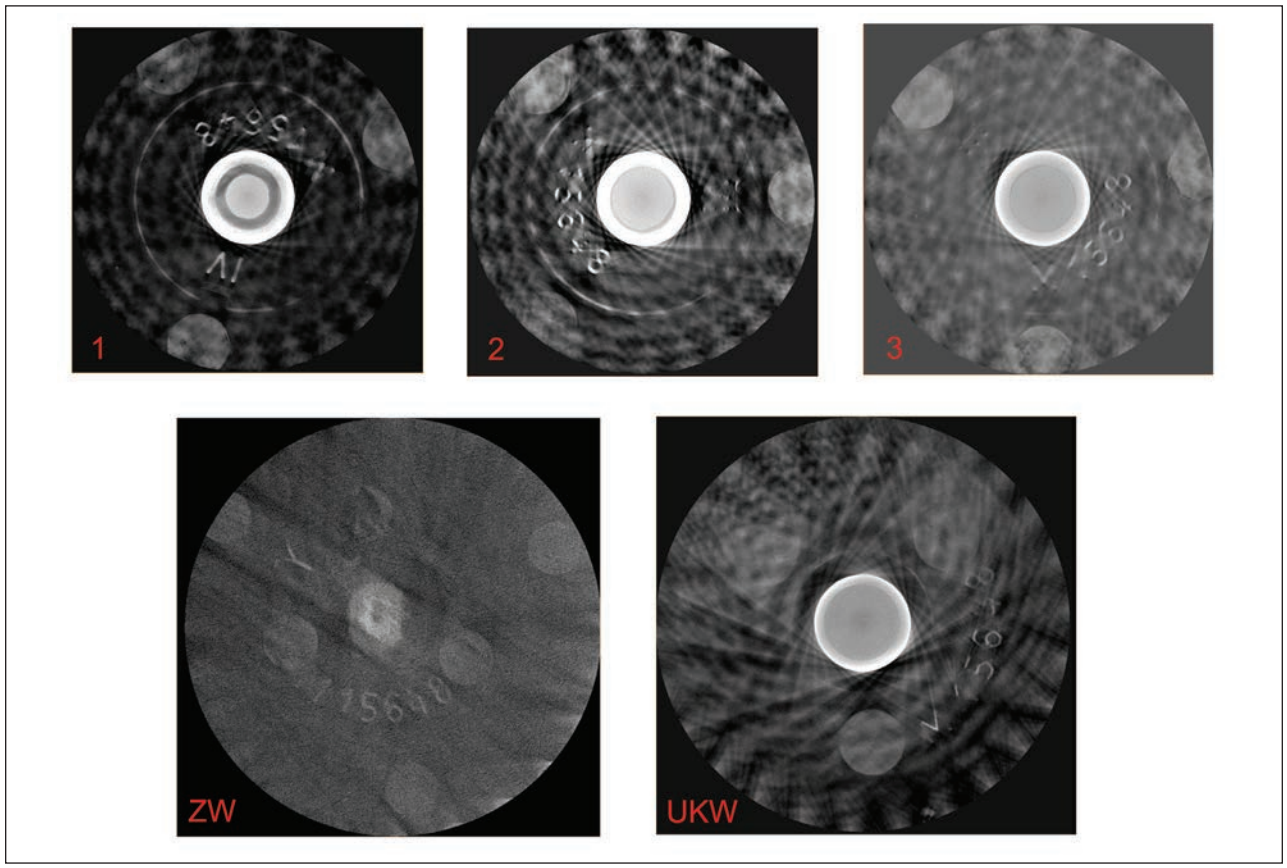


Figure 11: Cumulative X-ray computed microtomography cross-sections of the wheels and rotors with serial numbers and markings, shown from right to left (3D render: Lidija Korat and Miha Hren, Slovenian National Building and Civil Engineering Institute).

played a key role in the Battle of the Atlantic and its introduction caused a full intelligence blackout in the British Government Code and Cypher School (GC&CS) in Bletchley Park (Buckinghamshire). For the personnel of Hut 8, the introduction of the new Enigma model did not come as a surprise as the British already knew about the M4 early in 1941, but final confirmation came with the capture of the M4's top lid from submarine U-570, which surrendered on 28 August 1941 after an air attack south of Iceland (Erskine, 2011a).

Cryptanalysts needed a full 9 months to break the M4 key, a very long period for wartime. In order to decipher Kriegsmarine messages, Alan Turing and his colleagues designed an electromechanical code-breaking machine (rapid analytical machine – RAM), the so-called Bombe, as early as September 1939 on the basis of Polish decryption machines. However, after the introduction of the M4, the reliability of British Bombes was still unsatisfactory. The breakthrough came with the capture of the tables for the »Heimische Gewässer« code network and the key sheets for weather report signals (Wetterkurzschlüssel) from two German fishing boats (tugboats) converted for weather observation – Krebs near the Lofoten Islands on 4 March 1941, and München north of Iceland on 7 May 1941. Perhaps even more significant was the capture of books for short signals (Kurzsignale), special settings, a manual for so-called officer messages, and an Enigma machine from the U-110, which was damaged and captured during an attack on an Allied convoy near Greenland two days later. Short signals, which were used by the German Navy to shorten the transmission time of position, situation and observation reports, could already be deciphered with the standard Bombes and the deciphered short signals provided good starting settings for »Triton« key traffic. New success in this direction came with the operation of capturing the weather ship Lauenburg near Jan Mayen Island in the Arctic Ocean on 28 June 1941 as Bletchley Park knew that it was carrying monthly tables with Enigma settings (Sebag-Montefiore, 2004, 116–144, 147–150; cf. Paterson, 2007, 79–94; Conyers Nesbit, 2008; Erskine, 2008).

Figure 12: Enigma M4 electromechanical cipher machine was developed primarily for the U-Boot division of the German Kriegsmarine. The machine was housed in an oak carrying case (Source: Cryptomuseum, 2022).

New problems arose for GC&CS in March 1943 when a third edition of short signal books for weather reports was introduced, and on 1 July of the same year, when the Germans started using new versions of the extra rotor and reflector for the M4. The success of cryptanalysts from Bletchley Park in breaking the new system came in no small part to the capture of codebooks (Wetterkurzschlüssel and Kurzsignalheft) and maps as well as a completely preserved Enigma from a sinking submarine U-559, which was tracked down and critically damaged by Royal Navy destroyers on 30 October 1942, 60 miles off Port Said in Egypt (Sebag-Montefiore, 2004, 217–224; cf. Conyers Nesbit, 2008). Two of the three crew members who boarded U-559, Lieutenant Anthony Fasson and sailor Colin Grazier, drowned trying to recover the material. This event is even more tragic knowing that as early as the end of 1941, the personnel of Hut 8 were able to reconstruct the wiring of the Beta rotor and reflector B of the M4 (Erskine, 2008, 204–205), which is why obtaining the Enigma from U-559 was not of critical importance.

The agreement to share naval intelligence (naval SIGINT) signed in October 1942 was followed by the cooperation between GC&CS and OP-20-G (US Navy's Naval Enigma Section) in order to develop a more capable »analytical hardware«. By using American four-rotor Bombes, which were 34 times faster and were made in the US Naval Computing Machine Laboratory in Dayton (Ohio) led by Joseph Desch, the Allies were able to decipher most of the Enigma M4 messages from the second half of 1943 onwards. After September 1943, »Shark« code messages were usually deciphered within 24 hours and OP-20-G became entirely responsible for this task from the end of that year, having at its disposal approximately 75 Bombes. American success in deciphering enemy code was crucial in sinking multiple tankers (»Milchkuh«) and other ships that supplied the submarine fleet in the Atlantic in the middle of 1943. This meant that the submarines had to return to their bases on the west coast of France more frequently.

Further progress came with the American capture of U-505, which was forced to surface around 150 miles off the coast of Western Sahara after being hit by depth charges on 4 June 1944. The crew's attempt to scuttle the submarine failed as they were boarded in a daring manoeuvre by the men from USS Pillsbury (DE-133) who closed the valves and disarmed the scuttling charges. Apart from the intact Enigma, the captured material from U-505, which was later towed across the Atlantic to Bermuda (from 1954, the U-505 has been displayed in the Museum of Science and Industry in Chicago), also included books with officer and regular settings for June 1944, a valid codebook of short weather messages, new versions of bigram tables, a book of short signals and a book (Adressbuch) with quadrant marking codes on a grid map (cf. Ulbricht, 2005, 38–40). With the help of the latter, submarine tracking services in London and Washington were able to, for the first time, instantly identify positional references from deciphered messages (Sebag-Montefiore, 2004, 280–285).

Naval radio traffic, which was examined by the personnel of Hut 8 in Bletchley Park, was intercepted by 23 HF-DF (high-frequency direction-finding) stations on the Atlantic coast after May 1944, and the US Navy also had its own stations (Erskine, 2011a). The daily message traffic of the Kriegsmarine was constantly increasing during the war, going from around 300 in 1940 all the way to 1500–2000 in 1944–1945. Simultaneously, the number of keys was also increasing, from one main key in 1941 (»Heimische Gewässer«, later »Hydra«, Eng. »Dolphin«, and the corresponding officer's »Oyster«) to around 20 keys at the end of the war. After November 1944, the Kriegsmarine started issuing individual submarines so-called special keys (Sonderschlüssel), which were practically unbreakable (the first one was broken by OP-20-G as late as early April 1945), which prevented the Allies from accessing all the operational information on submarine activity in the last ten months of the war (Erskine, 2011a). Most of the other keys were usually broken by Allied analysts soon after their introduction, or they managed to decipher individual messages coded with those keys frequently enough to decide that they were not worth pursuing anymore (Alexander, 1945, 15–16). The Anglo-American cooperation was very successful thanks to the great relationship between Hut 8 and OP-20-G; out of 1,550,000 Naval Enigma's intercepted messages, Hut 8 managed to decipher 1,220,000 (Mahon, 1945). Out of those, only around 530,000 were forwarded to the Admiralty and the Operational Intelligence Centre (OIC) as many messages only included weather data and other operationally uninteresting information (Erskine, 2011a).

Information from the deciphered Enigma messages were given the highest security classification in Great Britain (»Ultra«) and remained limited to a very small circle of commanders and staff officers. Despite the warning signs that pointed towards their code being broken, Berlin never questioned the basic principles of communication security. Even the Supreme Commander of the German Navy's U-Boat Arm (Befehlshaber der U-Boote; BdU), Admiral Karl Dönitz, who did not completely trust the supposed security of the keys, refused to believe, even after the Bat-

Figure 13: Enigma M4. Machine parts (Source: Cryptomuseum, 2022).

tle of the Atlantic, that the Allies uncovered the positions and intentions of his submarines with cryptanalysis, and instead thought it came down to radar technology or radiogoniometry. Although the Abwehr received a clear message from an agent (»V-Mann«) within the US Department of the Navy that the Allies have been reading encrypted orders given to submarines for months, the Maritime Warfare Command (Seekriegsleitung; Skl) did not completely believe it, and the introduced improvements (e.g. double encryption) did not manage to stave off future naval and air attacks on rendezvous points of submarines and supply vessels for long. It was only after a succession of losses in February and March 1944 that the BdU and the commander of the Marinenachrichtendienst (MND; Naval Intelligence Agency) came to the conclusion that the enemy did not get the information on their rendezvous points from radiogoniometry, but by reading radio messages or treason. Even then, additional security measures could not stop the attacks for long, but the MND still unfalteringly trusted the Enigma. Such »strange coincidences« were interpreted as a consequence of the Allies capturing an intact machine together with that month's key, which would change anyway, and they dismissed the compromising of the entire coding system as impossible (Rahn, 2002).

The Allies also treated the success of deciphering Enigma messages as a secret that needed to be kept at all costs, which is reflected in the security and intelligence measures taken upon the capturing of codebooks, Enigma machines or submarines, including the immediate isolation and blindfolding of the rescued German crews. Among the high-risk

exploits that could have revealed to the Germans that their code had been compromised were especially attempts at rescuing submarines and the intent of their towing to the nearest ports as they could be observed by other submarines. Such cases include the aforementioned U-505 and U-205, the latter being severely damaged on 17 February 1943 during an attack on a convoy 80 miles northeast of Benghazi on the Libyan coast. After a risky boarding attempt performed by a group of sailors from the destroyer HMS Paladin (G69), which resulted in the capture of a Kenngruppenbuch (book with message indicators) and a Zuteilungsliste (allocation list), the corvette HMS Gloxinia (K22) attempted to tow the submarine into a nearby bay near Cape Ras el Hilal, but it sank about one kilometer off the coast to a depth of around 40 m (Sebag-Montefiore, 2004, 227–230; Conyers Nesbit, 2008). A special GC&CS committee, which believed that the submarine carried an Enigma as well as a new Gamma rotor and a corresponding reflector C (see below), even considered using deep-sea divers in order to extract them from the submarine, but it is not clear if such a dive was ever carried out (c.f. Erskine, 2008, 207). A similar decision for a rescue attempt of U-505 on 4 June 1944, two days before the invasion of Normandy, nearly got Captain Daniel Gallery, commander of an American naval squadron, court-martialed (Sebag-Montefiore, 2004, 284–285). An encrypted message of a captured officer from the end of 1944 stating that the enemy had captured an intact submarine along with its communication materials proves that such concerns were justified (Rahn, 2002, 151).

The success of Allied cryptanalysts and the heroics of the people who managed to capture intelligence material from sinking submarines became known to the public as late as the 1970s. Some of the information was only recently declassified (2016) while the majority of the captured codebooks with keys still lie in the vaults of the US National Security Agency and is inaccessible to the public.

FEATURES

The M4 cipher machine (»Schlüsselmaschine ENIGMA«, Funkschlüssel M Form M 4 or Schlüssel M4 for short) was developed as a more secure version of the Naval Enigma M3, which in turn was based on the Enigma I model used by the German Army and Air Force. The Enigma M3 had three switchable cipher rotors, a fixed reflector (Umkehrwalze) and a plugboard with sockets (Steckerbrett). It was equipped with eight different cipher rotors (I–VIII), with only three being in the machine at the same time. The first five rotors (I–V; the so-called Sigma rotors) were identical to those used by the German Army Enigmas (Heer), while three (VI–VIII; the-so called Delta rotors) were intended only for the Kriegsmarine. Unlike the Army, the Navy decided to use letters (A–Z) instead of numbers (01–26) on the rim of the rotors. Sigma (I–V) and Delta (VI–VIII) rotors had a movable ring which moved the contacts independently of the markings on the rotor and had to have been set (Ringstellung). Rotors I–V could be set via a spring-loaded pin, while the Naval rotors (VI–VIII) required two pawls to be pressed simultaneously. One of the rotors inside the machine had to be picked from one of the three Naval rotors and it could not be used in the same position on two successive days.

The M4 model had an extra rotor (Zusatzwalze; ZW) to the left of the three switchable rotors, which added another level to the coding algorithm. The installation of the fourth rotor demanded the thinning of the reflector and a reduced thickness of the extra rotor. The extra rotor in versions Beta (IX) and Gamma (X), hence also called the Griechenwalze, was fixed together with the thin reflector, which is why it did not move during the typing of the message and was not interchangeable with other rotors. In the internal settings (Innere Einstellung) of the key for an individual day of the month, the positions of the rotors (Walzenlage) were given in a sequence from left to right: reflector, fixed Zusatz- or Griechenwalze, then the left, i.e. slowly-rotating rotor, middle rotor, and finally, the right, quickly-rotating rotor.

The reflector B (»Bruno«) with the extra β-rotor entered into use in the area of the »Triton« or »Shark« key (submarines in the Atlantic and the Mediterranean) on 1 February 1942, and on 1 July 1943, the second version of the extra rotor (γ) was introduced with the corresponding reflector C (»Caesar«) (Hammarborg, 1954, 163–166; Ulbricht, 2005, 9–10). The Allies could not decipher messages encrypted with Gamma rotors until September 1943. Both extra rotors were switchable and were swapped on a monthly basis, whereas the initial setting of the extra rotor (Grundstellung) and the setting of its ring (Ringstellung) remained set to A until February 1945. The UKW as well as the extra (4th) rotor were wired in a way that allowed the Enigma M4 with this setting to be backwards compatible and could exchange messages with the M3 model (Hammarborg, 1954, 163–164; Rijmenants, 2004). In other words: the combination M4 UKW B + ZW Beta is identical to the M3 with a regular (wide) UKW type B while the combination M4 UKW C + ZW Gamma is identical to the M3 with a regular UKW type C. It is known that especially in home waters and

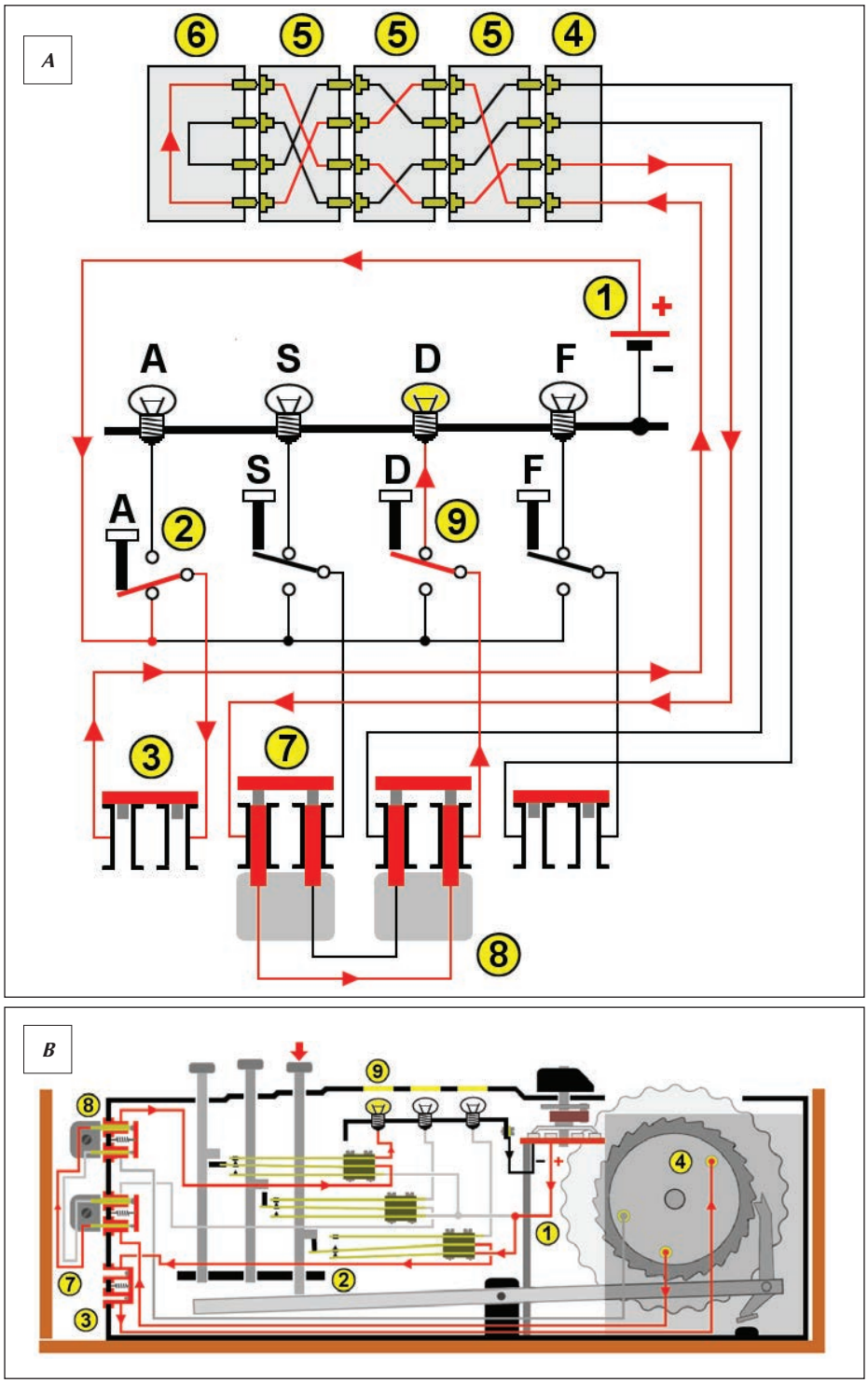


Figure 14: Wiring diagram (a) and side view of the mechanics and electric circuit of the Enigma. The current flows from the battery [1] through the depressed bi-directional letter-switch [2] to the plugboard [3]. The plugboard allows rewiring the connections between the keyboard [2] and the fixed entry wheel [4]. Next, the current proceeds through the unused, and therefore closed, socket [3] via the entry wheel [4] through the cross-wirings of the three (Wehrmacht Enigma) or four (Kriegsmarine M4) rotors [5] and enters the reflector [6]. The reflector returns the current, via a different path, back through the rotors [5] and entry wheel [4], and proceeds through the plugboard once again and through plug ‚S' connected with a cable [8] to plug ‚D', and through another bi-directional switch [9] to light-up the lamp (Made by: D. Rijmenants).

in the Mediterranean, Enigma M4 machines were used with settings that made them backwards compatible with the three-rotor model (M3), while during the last two months of the war, the setting of the extra rotor started being changed just like the other three rotors.

The design of the keyboard and the plate with illuminated letters uses the standard German layout (QWERTZ). When typing the messages, with each press of a key, the rightmost rotor would turn by one step (1/26), which caused a different connection in the internal wiring and, consequently, different encryption after each letter was typed. The turn of the rotor caused the same letter to be encrypted in a different way each time. The Enigma thus worked on the principle of polyalphabetic substitution. If the rotors had not been turning, it would classify as monoalphabetic substitution, which is much less secure.

In the set of 8 interchangeable rotors, five rotors (I–V) have a single notch on the rim, while three rotors (VI–VIII) have two notches positioned opposite each other. This meant that with each rotation of the right rotor, the other two rotors could also turn, but not always. Each new position would create an electric circuit. For additional encryption, the Enigma featured a plugboard at the front, which enabled the swapping of letters in pairs by using plugs, which connected the keyboard with the fixed entry wheel. Each machine was equipped with twelve 2-wire cables, approximately 20 cm in length, which had two Bakelite plugs with one thick (4 mm) and one thin (3 mm) pin that were cross-connected with single-wire cables. The pins fitted a socket with two holes of different diameters, which is why they could not be mistakenly swapped. The Bakelite casings of the plugs were not numbered or marked in any other way. This design enabled 0–13 contacts, which meant that anywhere between 0 and 13 pairs of letters could be swapped. As is evident from the M4 instruction manual, 10 cables were normally used during the war and two spare cables were stored underneath the lid of the box. Pressing one of the 26 keys created a connection with the plugboard, from where the current passed into the fixed entry wheel (Eintrittwalze) and from there to the rightmost rotor. This rotor transferred the current to other rotors on the left and to the reflector (Umkehrwalze). The latter sent the current in the opposite direction through the rotors back to the entry wheel and then back to the plugboard, and from there to the panel, where the appropriate letter was lit up. Once the key was lifted, the circuit was broken and the light bulb under the letter on the panel would go out. The machine was designed so that individual letters could not be encrypted to themselves. According to one of the calculations, the M4 model with the extra rotor allowed for 3.1×10^{25} different combinations or slightly fewer since the Navy was always using at least one of its three switchable rotors. The M4 provided a mathematical security almost 300 times greater than that of the Enigma used by the Army (Heer) (Rijmenants, 2004). All of the theoretically possible settings of the M4 amount to an astronomically high number of 2×10^{145} (Miller, 2019, 14).

OPERATING PROCEDURE

Before the encryption process began, the Enigma had to be set up in a way that was familiar to both sides of the communication. This included the selection, arrangement (Walzenlage) and starting position of each rotor (Grundstellung), and the setting of the ring with the indicator (Ringstellung). For the correct encryption and decryption of a message, the settings of the sender's and receiver's Enigma had to be identical. The operating procedure of the M4 machine, which was named after the version of the operating procedure and not the fourth wheel, started with the selection of the key from the codebooks and tables. Tables with keys for Naval Enigmas consisted of two parts: the first Schlüsseltafel M Allgemein – Innere Einstellung (internal settings) gave the choice of three rotors and their positions (Walzenlage), the settings of their rings (Ringstellung), the choice and setting of the thin Beta or Gamma rotor and the reflector, i.e. only for the odd days of the month. The second part Schlüsseltafel M Allgemein – Aussere Einstellung (external settings) contained the combinations of the pairs of sockets on the plugboard (Steckerverbindungen) and the settings of the four rotors (Grundstellung) for all days of the month (Rijmenants, 2010, 332).

The internal settings from a specific key were at first changed at midnight and the external settings at noon. After 1 July 1942, both the internal and external settings changed at noon D.G.Z. (Deutsche Gesetzliche Zeit), which meant early in the morning for German submarines that operated along the eastern coast of the US. The internal settings were supposed to be the responsibility of an officer, however, in practice, these were also normally set by the radio operator, usually the Funkmaat or Oberfunkmaat (Bauer, Erskine & Herold, 1997, 35).

In the case of Naval Kenngruppen, in order to determine the key used for an individual message, the radio operator had to choose two groups of three letters (Trigram) from a special book (Kenngruppenbuch) for a specific area of the key's validity (Schlüsselbereich), namely the Schlüsselkenngruppe for the identification of the key and the Verfahrenkenngruppe for the

acquisition of the message key (Spruchschlüssel). With the Enigma in the starting position, the operator first typed the Verfahrenkenngruppe trigram and received the key for the message, which gave him the starting settings of the rotors for the encryption of the message. Trigrams for the Schlüsselkenngruppe and the Verfahrenkenngruppe formed the indicator of the message (key for the message), which was additionally encrypted with the help of a table for the conversion of letter pairs – bigram (Doppelbuchstabentauschtafel) before it was sent together with the encrypted message. There were nine tables for the conversion of the letter pairs, labelled from A to J, which were chosen for any given day according to the calendar. With the three-rotor Enigma, both trigrams of message identifiers were written one under the other and were added a random letter to the beginning of the first one and the end of the second one. Vertical pairs of letters (bigrams) from both text indicators were then encrypted with the help of the tables. With the same table, the operator of the receiver of the message deciphered 8 letters of the message's indicator. The first trigram showed the appropriate key. Then, with the rotors in the starting positions, the second trigram was typed in. The obtained trigram gave the key of the message, on the basis of which the rotor's starting positions were set in order to decipher the rest of the message. With Enigmas with four rotors, instead of using three and one random letter, four letters were used (Rijmenants, 2010).

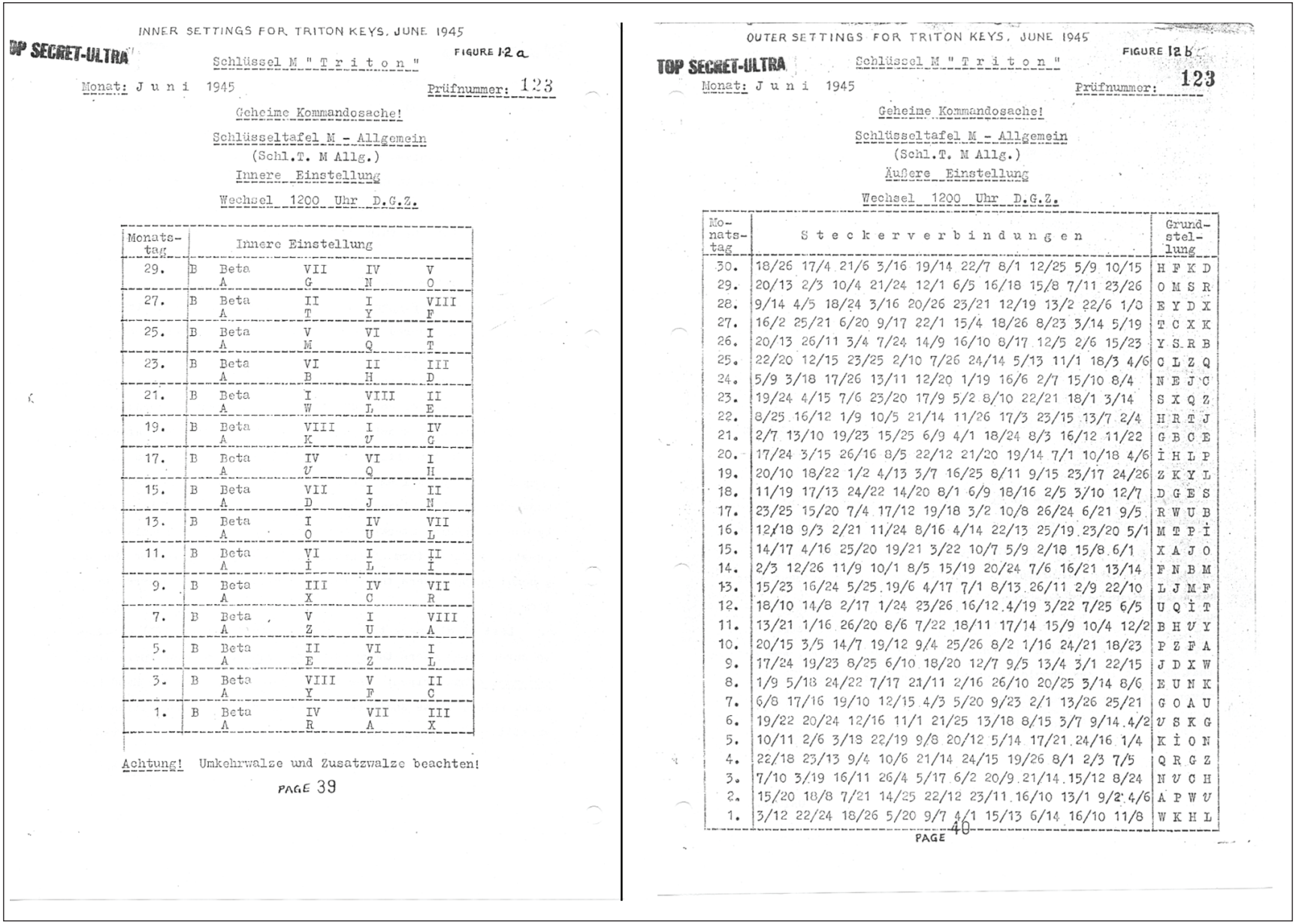
In the case of Naval Enigmas, the text of the message (Klarspruch) was divided into groups of four letters. At the beginning are two indicators with four letters each which are repeated at the end of the message, enabling the friendly and the enemy side to immediately recognize the signals of the Naval Enigma. The encrypted text was then sent via radio transmission, usually in Morse code, to the operator of the second Enigma. The operator typed the transcript of the encrypted text into the machine with the same daily settings. With the help of the bigram tables, he first deciphered both message indicators and thus obtained the coded key of the message. After typing it in and obtaining the deciphered key with the rotor settings, he then typed in the encrypted text of the message and wrote down the illuminated letters that gave the final text. According to one of the accounts, the encryption of a message with 40 groups (160 letters) took the operator and communications officer at least 5 minutes (Erskine, 2011b).

Initially, the German Navy only used a limited number of communication keys, i.e. radio communications with daily keys. Each area of operation had its own key and operating procedures. The three main areas or code networks were initially the »Heimische Gewässer« (from January 1943 »Hydra«, Allied designation »Dolphin«), »Auserheimische Gewässer« (from January 1943 »Ägir«; »Pike«) and »Süd« for the Mediterranean and the Black Sea area. They were used by submarines, most of the ships, coastal defence and other units. Before the encryption with the Enigma machine, some standard messages were encrypted with the short signal codebook (Kurzsignalheft) in order to shorten transmission time. At the start of October 1941, a new key »Front-U-Boote« was introduced for submarines in the Atlantic, which was officially called »Triton« (»Shark«) from February 1942 onwards, while warships were using the key »Kernflotte« (from January 1943 »Neptun«), which cryptanalysts from Bletchley Park were never able to break.

Submarines in the Mediterranean were using the »Süd« key only between November and December 1941, then switched to »Triton«, and in June 1943 to »Medusa« (»Turtle«), which was abandoned in August 1944. In October 1943, the code network »Süd« was split into keys »Hermes« (»Porpoise«) for the Mediterranean, »Poseidon« (»Grampus«) for the Black Sea and »Uranus« (»Trumpeter«) for the Balkans or the Oberkommando der Kriegsmarine (OKM) – Marineoberkommando (MOK) Süd/Südost (from October 1943, deciphered in April 1944). On 1 October 1944, the key »Hermes«, initially M »Süd«, was split into key M »Wotan« (»Bloater«) for the Mediterranean and M »Athen« (»Catfish«) for the Aegean Sea, while the designation »Porpoise« was kept for the communication key for Italy (German Naval Ciphers, 1944, 94–95, fig. 24b; Ulbricht, 2005, 28; Funkaufklärung, 2022). Upon its introduction, »Bloater« used the September keys of »Porpoise« and became an independent key on 15 November 1944. Due to the unavailability of the Bombe and the lack of interest in the messages it encrypted, the analytics personnel from Hut 8 in Bletchley Park did not break the »Bloater« key until 12 January 1945 when it once again merged with »Porpoise« (Alexander, 1945, 78; Mahon, 1945, 104). In February 1945, new independent keys were introduced for naval forces in the eastern Mediterranean, namely the »Albanien« for the south Adriatic and »Agäis« for the Aegean Sea (Rohwer, 2018). The »Hermes« key was in use all the way until May 1945 (Erskine, 1996, n. 8). Interestingly, one of the last deciphered messages, supposedly from the keys belonging to the code network »Süd«, was sent from Vižmarje near Ljubljana on 4 May 1945.[16]

The coding procedure described above was used only in the area of the main code networks. Instead of using the intricate message key selection with the help of the Kenngruppenbuch and the Doppelbuchstabentauschtafel, less important areas, such as the Black Sea, the Balkans, the Far East and the area of code network »Süd«, relied on a less secure method with double encryption

16 TNA, DEFE 3/685, p. 626.



INNER SETTINGS FOR TRITON KEYS, JUNE 1945

TOP SECRET-ULTRA

FIGURE 12 a

Schlüssel M "T r i t o n"

Monat: J u n i 1945 Prüfnummer: 123

Geheime Kommandosache!

Schlüsseltafel M - Allgemein

(Schl.T. M Allg.)

Innere Einstellung

Wechsel 1200 Uhr D.G.Z.

Monats-tag	Innere Einstellung				
29.	B	Beta A	VII G	IV N	V O
27.	B	Beta A	II T	I Y	VIII F
25.	B	Beta A	V M	VI Q	I T
23.	B	Beta A	VI B	II H	III D
21.	B	Beta A	I W	VIII L	II E
19.	B	Beta A	VIII K	I V	IV G
17.	B	Beta A	IV V	VI Q	I H
15.	B	Beta A	VII D	I J	II N
13.	B	Beta A	I O	IV U	VII L
11.	B	Beta A	VI I	I L	II I
9.	B	Beta A	III X	IV C	VII R
7.	B	Beta A	V Z	I U	VIII A
5.	B	Beta A	II E	VI Z	I L
3.	B	Beta A	VIII Y	V F	II C
1.	B	Beta A	IV R	VII A	III X

Achtung! Umkehrwalze und Zusatzwalze beachten!

PAGE 39

OUTER SETTINGS FOR TRITON KEYS, JUNE 1945

TOP SECRET-ULTRA

FIGURE 12 b

Schlüssel M "T r i t o n"

Monat: J u n i 1945 Prüfnummer: 123

Geheime Kommandosache!

Schlüsseltafel M - Allgemein

(Schl.T. M Allg.)

Äußere Einstellung

Wechsel 1200 Uhr D.G.Z.

Monats-tag	S t e c k e r v e r b i n d u n g e n	Grund-stel-lung
30.	18/26 17/4 21/6 3/16 19/14 22/7 8/1 12/25 5/9 10/15	H F K D
29.	20/13 2/3 10/4 21/24 12/1 6/5 16/18 15/8 7/11 23/26	O M S R
28.	9/14 4/5 18/24 3/16 20/26 23/21 12/19 13/2 22/6 1/0	E Y D X
27.	16/2 25/21 6/20 9/17 22/1 15/4 18/26 8/23 3/14 5/19	T C X K
26.	20/13 26/11 3/4 7/24 14/9 16/10 8/17 12/5 2/6 15/23	Y S R B
25.	22/20 12/15 23/25 2/10 7/26 24/14 5/13 11/1 18/3 4/6	C L Z Q
24.	5/9 3/18 17/26 13/11 12/20 1/19 16/6 2/7 15/10 8/4	N E J C
23.	19/24 4/15 7/6 23/20 17/9 5/2 8/10 22/21 18/1 3/14	S X Q Z
22.	8/25 16/12 1/9 10/5 21/14 11/26 17/3 23/15 13/7 2/4	H R T J
21.	2/7 13/10 19/23 15/25 6/9 4/1 18/24 8/3 16/12 11/22	G B C E
20.	17/24 3/15 26/16 8/5 22/12 21/20 19/14 7/1 10/18 4/6	I H L P
19.	20/10 18/22 1/2 4/13 3/7 16/25 8/11 9/15 23/17 24/26	Z K Y L
18.	11/19 17/13 24/22 14/20 8/1 6/9 18/16 2/5 3/10 12/7	D G E S
17.	23/25 15/20 7/4 17/12 19/18 3/2 10/8 26/24 6/21 9/5	R W U B
16.	12/18 9/3 2/21 11/24 8/16 4/14 22/13 25/19 23/20 5/1	M T P I
15.	14/17 4/16 25/20 19/21 3/22 10/7 5/9 2/18 15/8 6/1	X A J O
14.	2/3 12/26 11/9 10/1 8/5 15/19 20/24 7/6 16/21 13/14	F N B M
13.	15/23 16/24 5/25 19/6 4/17 7/1 8/13 26/11 2/9 22/10	L J M F
12.	18/10 14/8 2/17 1/24 23/26 16/12 4/19 3/22 7/25 6/5	U Q I T
11.	13/21 1/16 26/20 8/6 7/22 18/11 17/14 15/9 10/4 12/2	B H V Y
10.	20/15 3/5 14/7 19/12 9/4 25/26 8/2 1/16 24/21 18/23	P Z F A
9.	17/24 19/23 8/25 6/10 18/20 12/7 9/5 13/4 3/1 22/15	J D X W
8.	1/9 5/18 24/22 7/17 21/11 2/16 26/10 20/25 3/14 8/6	E U N K
7.	6/8 17/16 19/10 12/15 4/3 5/20 9/23 2/1 13/26 25/21	G O A U
6.	19/22 20/24 12/16 11/1 21/25 13/18 8/15 3/7 9/14 4/2	V S K G
5.	10/11 2/6 3/18 22/19 9/8 20/12 5/14 17/21 24/16 1/4	K I O N
4.	22/18 23/13 9/4 10/6 21/14 24/15 19/26 8/1 2/3 7/5	Q R G Z
3.	7/10 3/19 16/11 26/4 5/17 6/2 20/9 21/14 15/12 8/24	N V C H
2.	15/20 18/8 7/21 14/25 22/12 23/11 16/10 13/1 9/2 4/6	A P W V
1.	3/12 22/24 18/26 5/20 9/7 4/1 15/13 6/14 16/10 11/8	W K H L

PAGE 40

Figure 15: Example of a German Naval key – Schlüssel M «Triton« («Shark«): a – internal settings; b – external settings (Source: German Naval Ciphers, 1944.

of the message key (»doubly-enciphered« message key) from three randomly chosen letters (trigram), which the Army and Air Force used until 15 September 1938, and was abandoned by the Navy already on 1 May 1937 (Erskine, 1996; Erskine, 2011a; Rijmenants, 2010, 337). This system did not follow the Kenngruppenverfahren; with the rotors in the daily starting position (Grundstellung), which was the same for all Enigmas of code network »Süd«, the operator chose the message key himself. The three randomly chosen letters were typed in twice in a row producing the encrypted trigrams (e.g. SCD PJF), to which two letters of the vertical bigram were added (e.g. DA) as indicators of a specific code. The resulting two groups of four letters (DSCD APJF) were repeated at the start and end of the message (Erskine, 1996, 469). The adoption of the system of double encryption of message key indicators (so-called throw-on or boxing indicators as they were known as in Bletchley Park) in code networks of the Kriegsmarine is described by R. Erskine as a catastrophic, almost unbelievable mistake. Double encryption of the indicator from three identical letters created noticeable patterns (so-called females), which were a goldmine of revelations for the personnel of Hut 8 and OP-20-G, including warfare on land areas of code network »Süd« (all the way to southern Russia). All three valid keys of this network, »Poseidon«, »Uranus« and »Hermes«, were using double encryption of indicators at least until January 1944, while it was in June of the same year at the latest that they started using a 4-letter message key with M4 models (Ulbricht, 2005, 31–32). Code network »Süd« with its subordinate keys produced more than 115,000 deciphered messages in total, which are kept in two series, the second one perhaps also containing messages in other codes of the Enigma (Erskine, 1996, n. 18; Erskine, 2011a).

Apart from the Enigma, vessels were also equipped with RHV – Reservehandverfahren, a backup encryption system where the operator first transferred the text of the message into a frame on a piece of paper and then used coding tables (bigram) to switch the pairs of letters. A radio message coded with RHV looked the same as a message encrypted with the Enigma (Ulbricht, 2005, 46–48; Horenberg, 2012–2021).

From the start of the war, the German Navy used a type of two- and three-letter codes for coastal radio traffic, but most of them were soon abandoned. Among the so-called smaller codes, the spreadsheet from the document kept by NARA also lists coding signals from pairs of letters which the Allies dubbed »LL signals« because of the LL indicator and were used by smaller vessels in the Mediterranean, including the Adriatic, to forward »intelligence data«. These keys consisting of pairs of letters based on the principle of vertical bigrammatic substitution were supposedly of strategic nature and were usually not valid for more than a few weeks. Their encryption did not require an Enigma, but coding tables were used instead. Entries from the accessible journals of MOK Triest (MOK Triest, 1944) only contain the marking FT, i.e. Funktelegraphiemeldung,[17] before messages from individual vessels, but this is not meant to reveal anything about the encryption method (Weierud, 2022). At least part of the answer can be found in the deciphered and translated orders that Marineoberkommando Süd gave for individual missions along the western coast of Istria and are kept on microfilms by The National Archives at Kew, fund DEFE 3. Such an order from 18 April 1945, only a day after the sinking of the R 15, not only designates the formation of the group of vessels, area of operation, navigation speed and commander, but also the type of communication, which, translated by the personnel from Hut 4 in Bletchley Park, reads as: »W/T watch on coastal short wave Adriatic, ((cyphers))«.[18]

CONCLUSION

From 1941 onwards, only the M4 model was still being produced out of all the Naval Enigmas, which is why this machine was distributed to all naval units and coastal positions that used the Enigma. The early models with three rotors – M1, M1a, M2, M2a and M3, which were produced in 1934–1940 in relatively limited numbers (just under a thousand in total), remained in use, but only on smaller and less significant vessels and coastal areas, such as the Baltic. Until the end of the war, a total of more than 11,950 Enigmas of models M1 through M4 were produced, with more than two thirds of them being the M4. Throughout the war, the M4 Enigmas were thus mostly set up in a way that enabled the exchange of messages with the three-rotor models, including the Enigma I (machines of which the serial number starts with the letter 'A') used by the Army (Heer), Air Force (Luftwaffe) and

17 The rulebook for the use of Naval Enigmas for officers and staffs from 1940 which was used for the further wire transfer of the received radio messages of especially classified nature (Ulbricht, 2005, 32), instructs to label them with »*Geheimverschlüsselt FT*« (*Oberkommando der Kriegsmarine*, 1940). It is evident from the initial explanations that the B-issue of the instructions (printed in red, water-soluble ink) was handed out to the personnel of the encryption service of officers or commands of vessels, ranging from warships to supply ships, including minelayers and minesweepers. The rulebook states that the B-issue needs to be kept in a place where it can be easily reached by water in case there is danger of it falling into the hands of the enemy.

18 TNA, DEFE 3/685, p. 351.

the SS, with more than 20,000 made. From February 1942, when the M4 model entered into use, it was equipped in between 700 to 800 submarines, mostly with two Enigmas per submarine (two machines with different settings were needed for the time of the change of the key), while the rest were assigned to other units of the Kriegsmarine. The number of completely preserved M4 machines is extremely low, also owing to the fact that captains of submarines and other vessels were under strict orders to destroy their machines and throw them overboard, or they were destroyed by crews at the end of the war. According to some sources, fewer than 120 complete M4 machines are thought to have survived the war and all of them ended up in the hands of Allied naval units. The completely preserved machines mostly come from command or communication posts on land and are nowadays mostly still kept in intelligence agencies' vaults, with only a small number being kept in museums and private collections. In total, 83 Naval Enigmas with different levels of preservation were recorded in 2017. Two of them are M1 models, three are M2 models, two M3 models and the rest are M4's. Out of the approximately 50 completely preserved Enigmas of all types that are on public display in museums across the world, including the standard model A kept by the Museum of Contemporary History of Slovenia (A 14362/jla/42), 7 are model M4 Enigmas. Not included in the above overview are the Enigma model M2 (M1227) exhibited in the Military Museum in Belgrade, three M4 models (M7976/jla/44, M7968/jla/44, M7969/jla/44), and parts of 7 other Enigmas which are still under the authority of the Ministry of Defence of the Republic of Serbia. All of the abovementioned machines were supposedly seized from the retreating units of German Army Group E, which also included Kriegsmarine units from the Black Sea and bases in Greece (cf. Kovač, 2017, 33–42).

Notable among the finds from archaeological contexts are two Enigma M4 machines recovered from the submarine U-85, sunk in April 1942 by the destroyer USS Jesse Roper near Bodie Island, 15 nautical miles off the east coast of the US. In August 1997 and June 2001, divers salvaged two M4 Enigmas (M2946 and M3131) with their corresponding boxes with the extra rotors from the radio communications room (Funkraum). Additionally, they also managed to salvage fragments of radio message forms and some pages from the book with flag semaphore signals in the adjoining sonar room (Hamer, 2003). The better preserved of the two Enigmas is nowadays kept by the Hatteras Maritime Museum in North Carolina, where it arrived after a successful agreement between the governments of the United States of America and Germany. Since the submarine had not surrendered (after abandoning it, all of the crew members were killed), the U-Boot 85 with all its movable effects is still the property of Germany, which is why salvaging artefacts from the wreck without the express permission from the German government was illegal (Hadley, 2003).[19] Less clear is the background of the sinking of seven Enigma machines off the German Baltic coast, which were recently stumbled upon by divers near Gelting (2020) and in the the port of Kappeln (2021), close to Flensburg, and were handed over to the State Archaeology Department of Schleswig-Holstein (Archäologisches Landesamt Schleswig-Holstein). The M4 model from the bay near Gelting as well as the six Enigmas from Kappeln (three M4's and at least two M3's) are still in the conservation process in the Archaeological Museum Schloss Gottorf (Museum für Archäologie Gottorf). The find from Gelting Bay probably originates from one of the 50 submarines, the commanders of which received a scuttling order on the night of 4–5 May 1945 (codename »Regenbogen«), while the Enigmas from the port of Kappeln were perhaps thrown overboard

19 In legal literature, there are two approaches in the case of loss or transfer of ownership (ownership rights) of sunken military vessels and aircraft. One is the so-called implied abandonment rule and the second is the so-called express abandonment rule. Implied abandonment means that the cessation of ownership rights on a military vessel or aircraft derives from the passing of a certain amount of time. Contrastingly, according to standard international law, a state remains the owner of the sunken vessel or aircraft unless there is a transfer of ownership, the ownership is relinquished on the basis of a disclaimer of ownership, or in the case of capture before sinking or with surrender. The right to an enemy military vessel during the war is transferred to the beneficiary state at the moment when the vessel or aircraft comes into physical possession of that state, if such a transfer is done with intent. A coastal state thus does not obtain any ownership right over the sunken vessel or aircraft simply due to the fact that it is located on land or seabed over which it has sovereignty and jurisdiction. Pursuant to this, a coastal state has the right to possession and executing or allowing legal interventions, e.g. in the realm of removing obstacles for navigation and issuing salvaging permissions, where the UNESCO Convention on the Protection of Underwater Cultural Heritage encourages informing the flag state of the planned interventions and including it in the research. In the case of state immunity of the sunken vessels or aircraft, the prevailing explanation is that with the sinking, the vessel or aircraft loses its legitimacy for state immunity, but it is questionable if this applies to military items on board (e.g. documents, instruments, weapons), which the flag state is interested in keeping secret or protected against other states. In this sense, the sunken military vessel is regarded as a »military security container« of the flag state and, if this argumentation is followed, it falls under a different standard of protection, deriving from state immunity. Taking into account the principle of express abandonment, the Enigma from the R 15 minesweeper is the property of the Federal Republic of Germany as the legal successor of the Third Reich (cf. Daum, 2013; Craig, 2019, 74–119).

from ships heading to the place where they were to surrender to the Allies (Althaus, 2021).

The find from the wreck near Umag is thus completely in line with the belief that the Enigma M4, being the most widespread type of Naval Enigmas in the second half of the war, was a standard piece of equipment of all Kriegsmarine units, including smaller ships. Attesting to the fact that the presence of an Enigma on board the R 15 is not extraordinary, are the production year of the machine (1944) and the nature of the minesweeper's last mission, which does not deviate from the usual missions carried out at that stage of the war.[20]

The final answer to the question of the unit – user of the machine M15648 would have been given by the handwritten information about the the vessel or place of operation in a 6-page accompanying booklet (Begleitbuch für den Schlüssel M), which was issued for each individual machine by a competent authority of MOK. Apart from the machine's serial number, this booklet also contained information about the vessel or place of operation and handover date (Cdvandt, 2022). Begleitbuch or the second handover document (e.g. Merkblatt zum Schlüssel M on the underside of the lid of the wooden box), which probably accompanied the Enigma in question, was not preserved, so the question remains if the machine was kept on board permanently or just occasionally (e.g. during the presence of high command staff in the convoy). Class R 1 minesweepers did not have a designated radio communications room (Funkraum), which is why we presume that the Enigma was kept in the captain's quarters at front of the bow section of the hull. In the case of it being used during navigation, it was probably plugged into the 4V power source there.

The use of reflector type C (UKW-c) and an extra γ (Gamma) rotor (ZW), which were inside the M4 when the minesweeper R 15 sank, does not correspond to the data from the combination tables of reflectors (UKW) and extra rotors (ZW) for individual months in »Shark« traffic (Mahon, 1945, 104; Cryptomuseum, 2022), which proves that the machine from the R 15 used a different key, supposedly from the selection of keys of code group »Süd«. The last setting of the extra rotor (P) did not enable the exchange of messages with a three-rotor machine (M3), corresponding with the keys from the last two months of the war which predicted different settings of the extra rotors and their rings from the previously mandatory A-settings.

The background of the presence of the M4 cipher machine on the minesweeper R 15 definitely requires a more thorough examination and a review of the remaining material from the archives of Marineoberkommando Süd, which was being created between December 1944 and the end of the war. Further examination of the ring settings of the wheels (Ringstellung), i.e. the internal settings of the Enigma, will be especially interesting. If the settings on all 4 rotors could be identified, it would theoretically narrow down the identification of the key of the last use with an accuracy of up to two days. If it were possible to reconstruct at least some of the 10 pairs of plugs on the plugboard and taking into account the unused sockets and known rotor settings (Grundstellung), it would be possible to determine the last use of the Enigma with an accuracy of up to a day. The only way to establish all the settings from the last used coding key would be to compare data from the appropriate codebooks for the last months of the war. Some were captured and are kept in various archives, but it is not clear if they also contain codebooks for the Mediterranean or the Adriatic (Weierud, 2022).

Even though the Enigma could not be brought back to the state it was in upon its discovery, expert conservation efforts made it possible for the Park of Military History to obtain an incredibly interesting and rare exhibit, which has no equal among the documented finds from wrecks of the German Kriegsmarine in the Adriatic. The mystery and complexity of the cipher machine, including the »retro« look from the 1930s and the historical significance of deciphering code keys for the Allies, give the Enigma a special aura, which keeps on growing ever since the project, which became known as »Ultra« (c.f. Lewin, 2001; Horenberg, 2012–2021), was declassified in 1974. Various studies on the development, technical characteristics and the operation of the cipher machine, the exploits of cryptanalysts at Bletchley Park, the memoirs, novels and film adaptations of daring Enigma captures from submarines in the Atlantic and the Mediterranean, the activity in Bletchley Park and the tragic fate of its most famous protagonist Alan Turing (1912–1954), the importance of the Turing-Welchman Bombe for the development of modern computers, the online presentations and software simulations of the machine's operation, the collecting of wartime memorabilia and notable auction sales, and new discoveries from sea and land only stand to increase the interest in this machine.

20 This particular cipher machine is, therefore, most probably not directly linked with the operation of the 29th *U-Flotille*, whose submarines (U-230, U-407, U-565 and U-596) had been using the Pula base until the end of June 1944 (Paterson, 2007, 287), and most certainly not with the specific case of the famous U-81, as that submarine had already been sunk at its mooring in the *Kriegsmarinewerft* during the American bombing on 9 January 1944 (Paterson, 2007, 270–271).

ACKNOWLEDGEMENTS

For their expert help and publishing permission, we would like to thank cryptography and cipher machine specialists Frode Weierud, curator of the web portal Cryptocellar, Paul Reuvers, curator of the web portal Crypto Museum, Dirk Rijmenants, curator of the web portal Cipher Machines and Cryptology, captain Jerry Mason, editor of the web portal U-boat Archive, and dr. Klemen Kocjančič and Marko Ličina. For the photographs of the R 15 and the permission for their publication, we would like to thank Tobias Thelen from the Württembergische Landesbibliothek in Stuttgart. We would like to give special thanks to Peter Kreuzer, Thomas Weis and Reinhard Kramer, members of the web forum Marinearchiv who contributed important commentary and explanations on the history of the R 15 and the use of the Enigma M4 in the Mediterranean theatre. We would also like to thank Janko Boštjančič, director of the Park of Military History, who supported the writing of the study, Paul Reuvers for the expert review, and Tine Verbič for the translation into English.

The study of the first signatory was written as part of the P6-0247 research programme, which is co-financed by the Slovenian Research Agency.

ŠIFRIRNI STROJ ENIGMA M4 IZ RAZBITINE NEMŠKEGA MINOLOVCA R 15 PRI UMAGU

Andrej GASPARI
Univerza v Ljubljani, Filozofska fakulteta, Oddelek za arheologijo, Aškerčeva 2, 1000 Ljubljana, Slovenija
e-mail: andrej.gaspari@ff.uni-lj.si

Danijel GERMEK
Društvo vodnih športov Navtika, Obala 125, Lucija, 6320 Portorož, Slovenija
e-mail: d.vodnihsportov@gmail.com

Aleš JELINČIČ
Muzej novejše zgodovine Slovenije, depo Pivka, Kolodvorska cesta 51, 6257 Pivka, Slovenija
e-mail: ales.jelincic@muzej-nz.si

Miha HREN
Zavod za gradbeništvo Slovenije, Dimičeva ulica 12, 1000 Ljubljana, Slovenija
e-mail: miha.hren@zag.si

Lidija KORAT
Zavod za gradbeništvo Slovenije, Dimičeva ulica 12, 1000 Ljubljana, Slovenija
e-mail: lidija.korat@zag.si

Danijel FRKA
Sušilo 13, 51262 Kraljevica, Hrvaška
e-mail: danijel.frka@gmail.com

POVZETEK

V letih 1984–1986 je Zvonimir Kralj, potapljač in oskrbnik piranskega akvarija, iz razbitine nemškega lahkega minolovca R 15, potopljenega ob zahodni obali Istre med Savudrijo in Umagom, izvlekel šifrirni stroj Enigma in nekaj drugih predmetov. Räumboot iz prve serije teh plovil je plul v sestavi 6. flotilje minolovcev (6. Räumbootsflottille) nemške vojne mornarice, ki je od februarja 1944 iz oporišč v Pulju in Opatiji delovala na srednjem in severnem Jadranu. V zadnjem delu vojne je bila Kriegsmarine zaradi vse pogostejših zračnih napadov prisiljena pluti zlasti ponoči, dodatno nevarnost pa so predstavljale morske mine, ki so jih začeli nastavljali zavezniki. R 15 je v noči iz 16. na 17. april 1945 utrpel zadetek na slepo izstreljenega torpeda z britanskega torpednega čolna MTB 409 in potonil okoli 3 navtične milje severozahodno od Umaga. Od okoli 18 članov posadke R 15 se jih je rešilo samo pet. Minolovec z jeklenim ogrodjem in dvojno leseno oplato, dolg 27,5 m in širok 4,38 m, ki je na morskem dnu ležal z dnom navzgor, se je razmeroma dobro ohranil vse do konca 80-ih let 20. stoletja, nato pa so velik del njegovih ostankov zaradi ovire, ki jo je razbitina predstavljala globinskim ribiškim mrežam, po dnu odvlekli do obale. Kralj je iz razbitine poleg škatle z Enigmo in kodno knjižico dvignil še dve brzostrelki MP 40 in nekaj drugih predmetov ter jih poskušal zaščititi po najboljših močeh. Z razbitine R 15 zelo verjetno izvira tudi protiletalski top (FlaK 38) kalibra 20 mm, ki je danes razstavljen ob vhodu v Akvarij Piran. Leta 2020 je po posredovanju Danijela Germeka brzostrelki in šifrirni stroj, žal v razpadajočem stanju, pridobil Park vojaške zgodovine v Pivki. Pregled ohranjenih delov stroja je razkril, da gre za mornariško Enigmo M4 s štirimi rotorji in povratnim kolutom tipa C. S pomočjo rentgenske računalniške mikrotomografske preiskave so bile ugotovljene serijska številka stroja M 15648 ter zadnja nastavitev rotorjev: C/γ (gamma), III, VI, IV. Zunanji položaj dodatnega, gamma rotorja (P) kaže, da Enigma ni bila nastavljena na način, ki bi omogočal izmenjavo sporočil z modelom M3, kar ustreza kodnim ključem iz zadnjih dveh mesecev vojne. Ozadje prisotnosti Enigme M4, ki naj bi jih po zmotnem prepričanju uporabljali samo na podmornicah in nekaterih bojnih ladjah, na minolovcu R 15 zahteva podrobnejšo preučitev, vendar se zdi, da je povezana s posebej občutljivo nalogo, morda prisotnostjo višjega častnika ali prevozom šifrirne naprave po nalogu Marineoberkommando Süd. Enigma M4 z minolovca R 15 predstavlja eno redkih najdb teh izjemno kompleksih in fascinantnih šifrirnih strojev v arheološkem kontekstu.

Ključne besede: Jadran, Istra, druga svetovna vojna, nemška vojna mornarica, lahki minolovec R 15, 6. Räumbootsflotille, šifirni stroj, Enigma M4, arheološke ostaline

SOURCES AND BIBLIOGRAPHY

Alexander, C. Hugh O'D (1945): Cryptographic History of Work on the German Naval Enigma contents. P.R.O. HW 25/1. http://www.ellsbury.com/gne/gne-000.htm (last access: 2022-05-12).

Alman, Karl (1985): U-Boot Krieg im Mittelmeer – Graue Wölfe in blauer See. Rastatt, Pabel.

Althaus, Johann (2021): Ein kruder Befehl sorgte 1945 für die Versenkung der deutschen U-Boote. https://www.welt.de/geschichte/zweiter-weltkrieg/article232984933/Kriegsende-Die-Enigmas-und-der-raetselhafte-Befehl-Regenbogen.html (last access: 2022-05-08).

Bauer, Arthur O., Erskine, Ralph & Klaus Herold (1997): Funkpeilung als alliierte Waffe gegen deutchen U-Boote: Wie Schwächen und Versäumnisse bei der Funkführung der U-Boote zum Ausgang der Schlacht im Atlantik beigetragen haben. Rheinberg, Liebig Funk.

Birnbaum, Friedrich K. & Carlheinz Vorsteher (1987): Auf verlorenem Posten: Die 9. Torpedoboot-Flottillen. Stuttgart, Motorbuch Verlag.

Breyer, Siegfried (1994): Die deutsche Kriegsmarine 1935–1945: Band 2. Zerstörer, Torpedoboote, Geleitboote, Minensuch- und Räumboote, Minenschiffe, Hilfskreuzer, Vorpostenboote, U-Jäger, Sperrbrecher, Netzleger, Troß- und Sonderschiffe, Küstenartillerie. Friedberg, Podzun-Pallas-Verlag GmbH.

Cdvandt (2022): Begleitbuch für den Schlüssel M Serial number 15835. https://www.cdvandt.org/schluessel_dok.htm (last access: 2022-10-08).

Conyers Nesbit, Roy (2008): Ultra Versus U-Boats: Enigma Decrypts in the National Archives. Barnsley, Pen & Sword.

Craig, Forrest (2019): Maritime Legacies and the Law: Effective Legal Governance of WWI Wrecks. Cheltenham, Edward Elgar Publishing.

Cryptomuseum (2022): Enigma M4. https://www.cryptomuseum.com/crypto/enigma/m4/index.htm (last access: 2022-05-08).

Daum, Oliver (2013): Who Owns Sunken WWII German Military Aircraft? Uncertainties in the Law of Underwater Cultural Heritage. EJIL:Talk! Blog of the European Journal of International Law, July 16, 2013. https://www.ejiltalk.org/who-owns-sunken-wwii-german-military-aircraft-uncertainties-in-the-law-of-underwater-cultural-heritage/ (last access: 2022-06-12).

Dieter, Jung, Maass, Martin & Erich Gröner (1999): Die deutschen Kriegsschiffe 1815–1945, Bd. 2, Torpedoboote, Zerstörer, Schnellboote, Minensuchboote, Minenräumbote. Koblenz, Bernard & Graefe Verlag.

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

Erskine, Ralph (2008): Captured Kriegsmarine Enigma Documents at Bletchley Park. Cryptologia, 32, 3, 199–219.

Erskine, Ralph (2011a): Breaking German Naval Enigma on Both Sides of the Atlantic. In: Erskine, Ralph & Michael Smith (eds.): The Bletchley Park codebreakers: How Ultra Shortened the War and Led to the Birth of the Computer. London, Biteback Publishing Ltd., 159–174.

Erskine, Ralph (2011b): The Naval Enigma Kenngruppenbuch Indicator System – Used with the Main Wartime Ciphers. In: Erskine, Ralph & Michael Smith (eds.): The Bletchley Park codebreakers: How Ultra Shortened the War and Led to the Birth of the Computer. London, Biteback Publishing Ltd., 362–365.

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

Faggioni, Gabriele (2013): La Guerra aeronavale dopo l'8 settembre 1943 tra il Golfo di Venezia e La Costa Dalmata. Bollettino d'Archivio dell'Ufficio Storico della Marina Militare, Dicembre 2013, 71–127.

Freivogel, Zvonimir & Achille Rastelli (2014): Pomorski rat na Jadranu 1940.–1945. Zagreb, Despot infinitus.

Funkaufklärung (2022): Funkschlüssel der deutschen Kriegsmarine. https://www.wlb-stuttgart.de/seekrieg/ultra/ultra-frames.htm (last access: 2022-05-15).

German Naval Ciphers (1944): R.I.P. German Naval Ciphers October 1944. NARA. – Frode Weierud, Crypto Cellar Research. https://cryptocellar.org/enigma/files/nr-4457-rip-401.pdf (last access: 2022-05-08).

Hadley, Miles (2003): Home Found for »Enigmatic« WW II U-boat Relic. https://web.archive.org/web/20120905013432/http://www.navy.mil/submit/display.asp?story_id=6660 (last access: 2022-05-08).

Hamer, David (2014): List of Surviving Enigma Machines. https://enigmamuseum.com/dhlist.htm (last access: 2022-05-08).

Hamer, David H. (2003): The Enigmas – and Other Recovered Artefacts – of U-85. Cryptologia, 27, 2, 97–110.

Hamer, David H. (2022): Dr. David Hamer's List of Surviving Enigma Machines. https://enigmamuseum.com/dhlist.htm (last access: 2022-05-08).

Hammarborg, Astrid (1954): Catalog of Enigma Cipher Machine Wirings. National Security Agency, Technical Information Division, Bibliographic Research Branch. https://cryptocellar.org/Enigma/wiring-catalog/Enigma_rotor_catalog_chap.1.pdf (last access: 2022-05-08).

Historisches Marinearchiv (2022): Deutsche Minenabwehrfahrzeuge: Details R 15. https://www.historisches-marinearchiv.de/projekte/minensucher/ausgabe.php?where_value=1218 (last access: 2022-05-08).

Horenberg, Michael (2012–2021): Breaking German Navy Ciphers. https://Enigma.hoerenberg.com/index.php?cat=Reservehandverfahren (last access: 2022-05-25).

Kovač, Svetko (2017): Enigma i rat u Jugoslaviji. Beograd, Medija centar Odbrana.

Kralj, Zvonimir (2022): Personal communication.

Lewin, Ronald (2001): Ultra Goes to War: the Secret Story. London, Penguin.

Mahon, A. Patrick (1945): The History of Hut Eight, 1939–1945. HW 25/2. http://www.ellsbury.com/hut8/hut8-000.htm (last access: 2022-05-15).

Miller, A. Ray (2019): The Cryptographic Mathematics of Enigma. Center for Cryptologic History. National Security Agency. https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/CryptoMathEnigma_Miller.pdf (last access: 2022-05-08).

MOK Triest (1944): Kriegstagesbuch des komandierender Admiral Adria. Befehlshaber: Vizeadmiral Lietzmann. Befehlsbereich: Istrien, Norddalmatien, Süddalmatien, Albanien. Für die Zeit vom: 1. 9.–15. 9. 1944.

MTB Flotilla (2014): 28th MTB Flottilla. Coastal Forces Veterans Forum. http://cfv.org.uk/forum/viewtopic.php?t=457 (last access: 2022-05-08).

Mulligan, Timothy P. (2005): Records of the German Navy Operational Commands in World War II. Guides to Microfilmed Records of the Geman Navy, 1850–1945, No. 4. Washington, D. C., National Archives and Records Administration.

NARA PG 46525 – National Archive and Records Administration (NARA), KTB Adria/Kommandierender Admiral Adria, 1 Aug–15 Sep 1944, PG 46527, T1022, roll 4289.

NARA PG 46527 – NARA, KTB Adria/Kommandierender Admiral Adria, 1 Aug–15 Sep 1944, PG 46527, T1022, roll 4289.

NARA PG 46531 – NARA, KTB Adria/Kommandierender Admiral Adria, 1–29 Nov 1944, PG 46531, T1022, roll 4289.

NARA PG 73451 – NARA, KTB 7. Räumbootsflotille, 1 Jan 1943–15 Feb 1945, PG 73451, roll 3434.

NARA PG 73452 – NARA, KTB 7. Räumbootsflotille, 1 Jan 1943–15 Feb 1945, PG 73451, roll 3434.

Oberkommando der Kriegsmarine (1940): M.Dv. Nr. 32/1, Der Schlüssel M Verfahren M Allgemein. Berlin. https://www.cryptomuseum.com/crypto/enigma/files/schluessel_m.pdf (last access: 2022-05-08).

PAK PI 19 – Pokrajinski arhiv Koper, Enota Piran (PAK PI), Luška kapitanija Piran, 1910–1973, šk. 55.

Paterson, Lawrence (2007): U-Boat Combat Missions. The Pursuers & the Pursued: First-Hand Accounts of U-Boat Life and Operations. London, Chatham Publishing.

Paterson, Lawrence (2017): Hitler's Forgotten Flotillas: Kriegsmarine Security Forces. Barnsley, Seaforth Publishing.

Paterson, Lawrence (2019): U-boats in the Mediterranean 1941–1944. New York, Skyhorse Publishing.

Pope, Dudley (2014): Flag 4. The Battle of Coastal Forces in the Mediterranean 1939–45. Looe, House of Stratus.

Porzellanfabrik (2022): Porzellanfabrik Wilhelm Jäger in Eisenberg/Thüringen. Produktion zwischen 1933 ... 1945. https://www.porzellanfieber.de/Porzellanfabrik-Jaeger_im-Nationalsozialismus_Erzeugnisse.html (last access: 2022-05-08).

Pröse, Michael (2004): Chiffriermaschinen und Entzifferungsgeräte im Zweiten Weltkrieg: Technikgeschichte und informatikhistorische Aspekte. Dissertation, Technischen Universität Chemnitz. https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/ (last access: 2022-05-08).

Rahn, Werner (2002): Warnsignale und Selbstgewißheit. Der deutsche Marine-Nachrichtendienst und die vermeintliche Sicherheit des Schlüssels M (»Enigma«) 1943/44. Militärgeschichtliche Zeitschrift, 61, 141–154.

Räumbootsflottille (2022): 6. Räumbootsflottille. https://de.wikipedia.org/wiki/6._R%C3%A4umbootsflottille?veaction=edit (last access: 2022-05-08).

Räumboots-Flottillen (2022): Räumboots-Flottillen. https://www.lexikon-der-wehrmacht.de/Gliederungen/Sicherungsflott/RFlot.htm (last access: 2022-05-08).

Reynolds, Leonard C. & H. F. Cooper (1999): Mediterranean MTB´s at War – Short MTB Flotilla Operations 1939–1945. Stroud, Sutton Publishing Imperial War Museum.

Rijmenants, Dirk (2004): Technical Details of the Enigma Machine. https://www.ciphermachinesandcryptology.com/en/Enigmatech.htm (last access: 2022-05-08).

Rijmenants, Dirk (2010): Enigma Message Procedures Used by the Heer, Luftwaffe and Kriegsmarine. Cryptologia, 34, 4, 329–339.

Rohwer, Jürgen (2018): Chronik des Seekrieges 1939–1945. Februar 1945. https://www.wlb-stuttgart.de/seekrieg/45-02.htm (last access: 2022-05-08).

Rössler, Eberhard (1999): Uboottyp II – Die »Einbäume«. Vom Original zum Modell. Bonn, Bernard & Graefe.

Sebag-Montefiore, Hugh (2004): Enigma: The Battle for the Code. New York, Wiley.

Stehr, Werner F. G. & Siegfried Breyer (1999): Leichte und mittlere Artillerie auf deutschen Kriegsschiffen. Marine-Arsenal, Sonderband S-18, 1999. Wölfersheim-Berstadt, Podzun-Pallas Verlag.

TNA DEFE 3/685 – The National Archives (TNA), Records of the Ministry of Defence (DEFE), Admiralty: Operational Intelligence Centre: Intelligence from Intercepted German, Italian and Japanese Radio Communications, WWII, 1945 Apr 13-May 6 (DEFE 3/685).

Ulbricht, Heinz (2005): Die Chiffriermaschine Enigma – Trügerische Sicherheit: Ein Beitrag zur Geschichte der Nachrichtendienste. Dissertation. Braunschwig, Technische Universität Carolo Wilhelmina. https://publikationsserver.tu-braunschweig.de/receive/dbbs_mods_00001705 (last access: 2022-05-08).

Weierud, Frode (2022): Personal communication.

Williamson, Gordon (2009): Kriegsmarine Coastal Forces. Oxford, Osprey.