



ENIGMA

Teknologien – Menneskene – Historien

Leif Nilsen

Thales Norway AS



19 May, 2009

Thales Norway AS

ULTRA was the greatest secret of World War II after the atom bomb. With the exception of knowledge about that weapon and the probable exception of the time and place of major operations, such as the Normandy invasion, no information was held more tightly The security implies ULTRA's significance. ULTRA furnished intelligence better than any in the whole long history of humankind. It was more precise, more trustworthy, more voluminous, more continuous, longer lasting, and available faster, at a higher level, and from more commands than any other form of intelligence - spies or scouts or aerial reconnaissance or prisoner interrogations It may be concluded that ULTRA saved the world two years of war, billions of dollars, and millions of lives. David Kahn," Seizing the Enigma"

2009.05.19

1 Thales Norway AS

THALES

- Krypto etter 1. verdenskrig
- De første rotormaskiner
- Enigma – teknologi
- Enigma – operasjon
- Forsering av Enigma
- Andre rotormaskiner
- Konklusjon

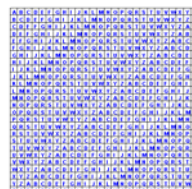


2009.05.19



- Manuelle chiffer
 - Polyalfabetisk substitusjon
 - Dobbelt transposisjon
 - ADFGVX
- Tungvindt og usikkert
- Framveksten av radiokommunikasjon øker behovet for sikker og effektiv kryptering

	A	D	F	G	V	X
A	S	U	B	J	E	C
D	T	A	D	F	G	H
F	I	K	L	M	N	O
G	P	Q	R	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

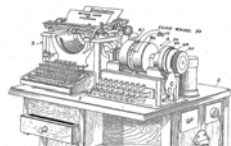


2009.05.19

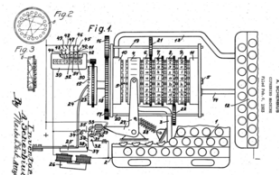


De første rotormaskiner

- Arthur Scherbius (1878-1926)
 - Tysk patentsøknad 23. februar 1918
- Hugo Koch
 - Nederlandsk patentsøknad 7. oktober 1919
 - T. A. van Hengel & R. P. C. Spengler 1915?
- Arvid Gerhard Damm
 - Svensk patentsøknad 11. oktober 1919
- Edward Hugh Hebern (1869-1952)
 - Initielle konstruksjoner 1917
 - US patentsøknad 1921



SH 9 HEBERNS „Elektr. Coding Maschine“ (1921)™



2009.05.19

 Thales Norway AS



THALES

Fra patent til Enigma

- Scherbius grunnlegger Scherbius & Ritter i 1918 → Gewerkschaft Securitas → Chiffriermaschinen – AG i 1923 → Heimsoeth & Rinke 1934
- Viser fram Enigma A i 1923, Enigma B i 1924
 - Integret skrivemaskin og veier 50 kg
- Willi Korn finner opp reflektoren (Umkehrwalze)
 - Mer kompakt og lettere Enigma C → “Funkschlüssel C”, tysk marine til 1934
 - Enigma D lanseres i 1927 som en kommersiell maskin
 - Solgt til flere europeiske land for militær og diplomatisk bruk
- Wehrmacht modifierer Enigma D og tar i bruk Enigma G 1928 → Enigma I 1930 (Steckerbrett) Klassiske Wehrmacht/Services Enigma



CHIFFRIERMASCHINEN
FABRIKATIONSGESAMTSCHAFT
BERLIN W 35
KREUZBERG 2
FERNAB- UND LANGABHÖR- UND
TELEFON-CHIFFRIER-BERLIN



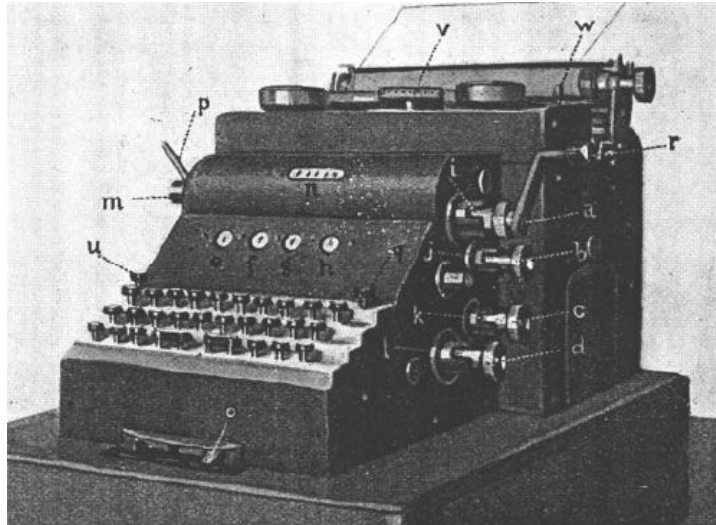
2009.05.19

 Thales Norway AS



THALES

Enigma A 



2009.05.19

 Thales Norway AS



THALES

Enigma A 

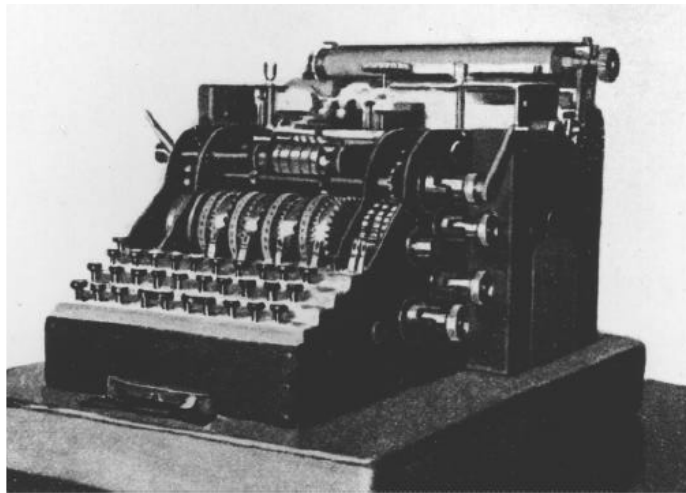


Figure 4. Model A with face plate removed.

2009.05.19

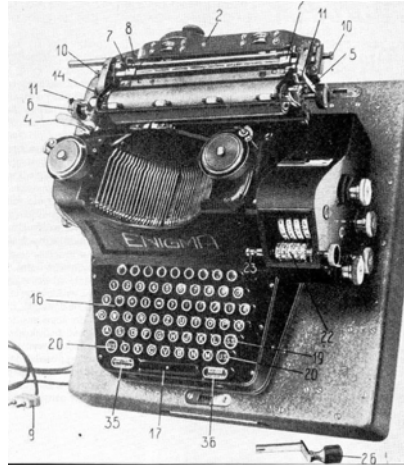
 Thales Norway AS



THALES

Enigma B

- Produksjonsår 1924
- 57 taster
- Små og store bokstaver, tall og tegn ble kryptert til små bokstaver i et 26 tegns alfabet
- 2 x 4 innstillbare rotorer
- Nøkkel ble valgt som 8 bokstaver



2009.05.19

 Thales Norway AS



THALES

Enigma C

- Produksjonsår 1924(1925)
- Chiffertegn angis ved hjelp av glødelampe
- Benytter reflektor (Umkehrwalze)
- Justerbar ring på hver rotor
- Grunnlag for senere varianter
- Militær versjon C* (Funkschlüssel C) tas i bruk av Reichsmarine fra februar 1926



2009.05.19

 Thales Norway AS



THALES

- Produktionsår 1927
- Grunnlag for kommersielle varianter
- Reflektoren kan settes i 26 ulike posisjoner
- Reflektoren var i tillegg roterbar basert på "Influenz-buchstabe"
- Sveitsisk utgave ofte omtalt som Enigma K



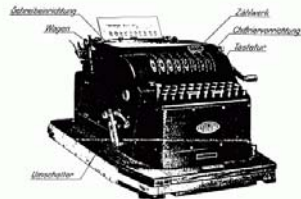
2009.05.19



Die schreibende

Enigma - Chiffriermaschine

Typenhebel – Elektrischer Antrieb



Unangreifbar in ihrer Chiffriersicherheit

Jeder Entzifferungsversuch Zeitverschwendung

Volle Geheimhaltung auch bei Uebermittlung von Schlüsselwechslern in Klarschrift

17 576 Perioden / Jede Periode 15 777 450 Zeichen

In einer halben Minute
ist jeder der 277 504 461 200 Schlüssel eingestellt

Kein Teil wird zur Schlüsseländerung ausgetauscht

Die schreibende Enigma

chiffriert

300 Zeichen in der Minute.

dechiffriert

auch Klarschrift.

schreibt

das Chiffriert in Reihen von 50 und in Gruppen von 5 Buchstaben ein.

teilt

liefert

das Dechiffriert in **Ursprungsform** mit Buchstaben, Ziffern, Interpunktionszeichen, Wortabständen.

zählt

die Zeichen.

dechiffriert

alles richtig übermittelt, auch bei Lücken im Chiffriert.

verweigert

ihren Dienst, solange falsche Bedienung.

bedient man

nach einer Leertaste von 30 Minuten.

Abmessungen: Länge etwa 65 cm
Breite etwa 45 cm
Höhe etwa 35 cm
Gewicht etwa 50 kg

Chiffriermaschinen Aktiengesellschaft

Berlin W 25, Steglitzer Straße 2
Fernsprecher: D 3, Nollendorf 2599

2009.05.19



Abwehr Enigma

- Enigma brukt av den militære etterretningstjenesten Abwehr fra 1939
- Tre rotorer pluss bevegelig reflektor
- Ingen "Stecker"
- Rotorene hadde 11, 15 og 17 steppesposisjoner
- Rekonstruert i BP av D. Knox basert på dobbelkrypterte meldingsindikatorer



2009.05.19

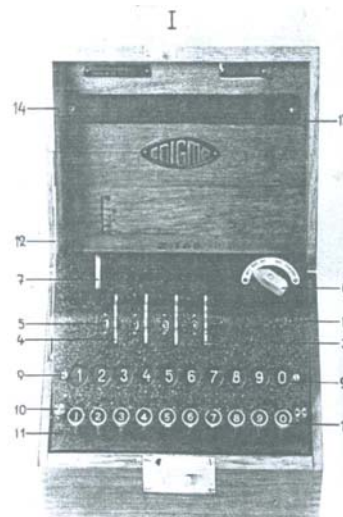
 Thales Norway AS



THALES

Enigma Z

- Enigma variant som kun krypterte desimale siffer
- Tilbudt til spansk UD 1931
- Tre bevegelige rotorer pluss roterbar reflektor
- Periode $10^4 = 10\ 000$
- Kan ha blitt brukt til å kryptere desimale kodeord
- Ble ikke kjøpt av Spania
- Bruk og utbredelse ukjent



2009.05.19

 Thales Norway AS



THALES

Enigma I (Klassisk militær Enigma)



2009.05.19

14 Thales Norway AS



THALES

Naval Enigma



2009.05.19

15 Thales Norway AS



THALES

Enigmaproduksjon

Type	Antall
Wehrmacht Enigma	20.306
Naval Enigma	17.900
Wehrmacht spesial Enigma (B – machine)	24
Enigma K	1.000
Enigma G	400
Enigma T	500
Totalt	40.130

Kilde: Frode Weierud

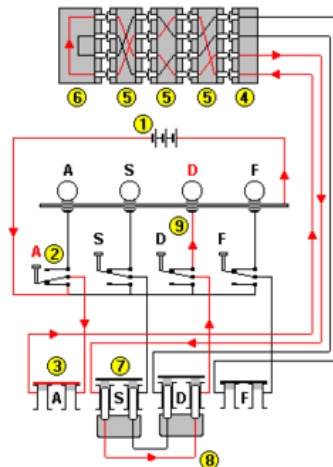
2009.05.19

16 Thales Norway AS



THALES

Koplingskjema



- ① - Batteri
- ② - Tastatur
- ③ - Koplingsbrett
- ④ - Inngangsvalse
- ⑤ - Rotorer (L M R)
- ⑥ - Reflektor
- ⑦ - Kortslutningsplate
- ⑧ - Støpselforbindelse
- ⑨ - Lampe

2009.05.19

17 Thales Norway AS



THALES

Enigma rotor



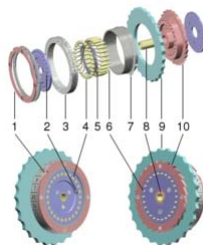
2009.05.19

18 Thales Norway AS



THALES

Enigma rotor



- 1 - Ring med "hakk"
- 2 - Markering for nøytralstilling
- 3 - Alfabetring
- 4 - Flate kontakter
- 5 - Internkoplinger
- 6 - Fjærbelastede kontakter
- 7 - Fjærbelastet låsering
- 8 - Aksling
- 9 - Innstillingshjul
- 10 - Drivhjul

2009.05.19

19 Thales Norway AS



THALES

Abwehr Enigma Rotors



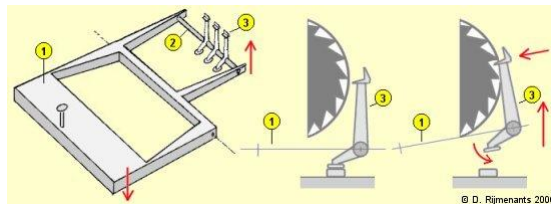
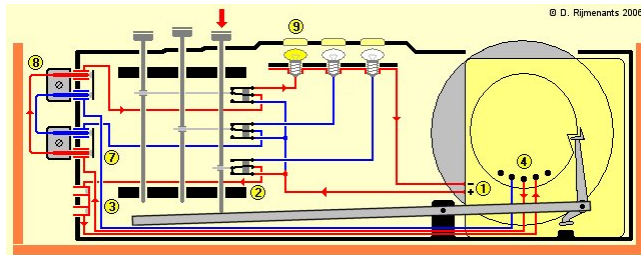
2009.05.19

20 Thales Norway AS



THALES

Drivverk



2009.05.19

21 Thales Norway AS



THALES

- Rotorene ble steppet ved at hvert tastetrykk beveget 3 hendler (paler)
- Høyre pal roterte drivverket på høyre rotor (fast)
- Midterste og venstre pal "red" på rotorringen til sin høyre naborotor
- Dersom pal traff hakket ("notch") i rotorringen vil den også bevege rotoren til venstre som dermed steppet
- Midterste rotor ble også steppet av venstre pal når denne falt ned i hakket (til forskjell fra vanlig odometrisk stepping)
- Perioden ble derfor $26 \times 25 \times 26 = 16.900 \neq 17.576 = 26^3$
- Senere rotorer kunne ha flere hakk på ringen og dermed gi oftere stepping av naborotor (Naval VI, VII, VIII & Enigma-T)



2009.05.19

 Thales Norway AS

THALES

- Opprinnelig Service-Enigma hadde 3 rotorer (I, II og III)
- 6 bokstaver ble sammenkoblet via pluggbrettet
- Reflektor B ble innført i 1/11-1937
- Rotor IV og V innført 15/12-1938
- Rotor VI, VII og VIII innført i M3/1939
- Prosedyrer for sending av meldingsindikator endres 15/9-1938
- Antall koblinger i pluggbrettet ble endret fra 1/1-1939

2009.05.19

 Thales Norway AS

THALES

Melding: "Ich bin sicher, daß unser Führer eine lose Schraube hat"

Enigma Simulator For Windows. ©1995-1999 Geoff Sullivan. Norway build 002

Thu Mar 06 15:46:40 2008

Rotor Order: B V I III Ringstellung: T E K [20 05 11]

Steckers:

Message Key: A A A [01 01 01]

Klartekst: ICHBI NSICH ERDAS SUNSE RFUHR EREIN ELOSE SCHRA
UBEHA T

Chiffertekst: OVKWR IZXJE OXFNR YPBZJ DBVCG SWLFR TGHPF
KEOQL KKRLQ I

2009.05.19



1. Pluggbrett med 0 til 13 doble forbindelser
2. 3 ulike rotorer i rekkefølge med 26 innkontakter forbundet med 26 utkontakter: $26! \times (26! - 1) \times (26! - 2)$ muligheter
3. 26 mulige posisjoner for hver rotor: $26^3 = 17\,576$ muligheter
4. Bevegelig ring på hver rotor som styrte stepping for neste rotor: $26^2 = 676$ muligheter
5. Reflektor som koplet innganger og utganger til samme ring av 26 kontaktpunkter: $7\,905\,853\,580\,625$ muligheter

2009.05.19



p	Kombinasjoner	p	Kombinasjoner
0	1	7	1 305 093 289 500
1	325	8	10 767 019 638 375
2	44 850	9	53 835 098 191 875
3	3 453 450	10	150 738 274 937 250
4	164 038 875	11	205 552 193 096 250
5	5 019 589 575	12	102 776 096 548 125
6	100 391 791 500	13	7 905 853 580 625

Totalt : 532 985 208 200 576 $\approx 5 \cdot 10^{14}$

2009.05.19



Teoretisk antall mulige konfigurasjoner blir nå:
 $N = 532985208200576 \cdot$
 $55929374591444682974054734803717536158968412$
 $98988710328553805190043271168000000 \cdot 17576 \cdot 676$
 $\cdot 7\ 905\ 853\ 580\ 625$
 $=$
 $32838835137969741987008820698827528783799552$
 $61095623685444055315226006433615627409666933$
 $182371154802769920000000000 \approx 3 \cdot 10^{114}$

2009.05.19



- Typiske forutsetninger ved kryptoanalyse under krigen:
 - 3 av 5 rotorer med kjente koblinger
 - 10 steckerforbindelser
 - Kjent reflektor

$$N = 150\,738\,274\,937\,250 \cdot 60 \cdot 17\,576 \cdot 676 = 107458687327250619360000 \text{ (77 bits)}$$



2009.05.19



- Grunnet reflektorkonstruksjonen kan vi se:
- I enhver posisjon er en Enigma-permutasjon karakterisert med følgende egenskaper:
 - En bokstav kan aldri krypteres til seg selv
 - Dersom "T" i en gitt posisjon krypteres til "F", vil "F" i den samme posisjonen krypteres til "T"
 - Enhver permutasjon er derfor et produkt av 13 disjunkte transposisjoner
- For konfigurasjonen $\{ \{ I, II, III \}, \{ A - A - A \}, \{ A - A - A \} \}$ vil $P = (BA)(QC)(MD)(FE)(XG)(IH)(SJ)(WK)(PL)(YN)(TO)(VR)(ZU)$

2009.05.19



Opprinnelig oppsett av Enigma

- Kodebøker inneholdt:
 - Rotorposisjon : III – I – II
 - Ringinnstilling: T – M – R
 - Pluggbrettkoplinger: AD – UN – PL – QX – MC – KS
 - Grunninnstilling: F – W – O
- Operatør velger meldingsindikator: T – C – I
 - Still Enigma i henhold til kodebok
 - Krypter: TCI-TCI ⇒ NBR-LTD
 - Sett rotorstilling til: T – C – I
 - Krypter klartekst:
 - FESTU NGXNO RWEGE N ⇒ ZDXKM OMNDV MISUL M
 - Send melding: NBRLT DZDXK MOMND VMISU LM
- Mottager
 - Still Enigma i henhold til kodebok
 - Tast inn NBR LTD ⇒ TCI TCI
 - Sett rotorinnstilling til T – C – I
 - Dekrypter ved å taste inn mottatt melding

2009.05.19

 Thales Norway AS



THALES

Utdrag fra tysk kodeliste

Geheim!

Sonder - Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Grundstellung
31.	IV II I	F T R	HR AT IW SK UY DF OV LJ BG KX	vyj
30.	III V II	Y V P	OR KI JV OE ZN KU DP YC DS GP	oqr
29.	V IV I	O H R	UX JC FB BH TA ED ST DS LU FI	vnf

2009.05.19

 Thales Norway AS



THALES

VIII. Beispiel.

17. Öblicher Tagesschlüssel:
(Kaufkraft von der für die Verschlüsselung der Klartexte in Deutsch zusammenen Schlüssel, z. B. r.....
Schlüssel für Spezial (Wort))

Datum	Einzeltag	Ringstellung	Stromführung
4.	I III II	16 11 13	04-10-10

Stromführung	Stromgruppen- Einzeltag	Stromgruppen
OO 14 PR HU JW L3 TX	2	ndj von ope van

Nach diesem Tagesschlüssel ist die Schlüsselmaschine einzustellen (vgl. S. 4 und 5).
Der im nachfolgenden Beispiel eingetragte Schlüssel ist aus dem Klartext durch den Schlüssel nicht mit der Schlüsselmaschine zu entschlüsseln, sondern mittels des Schlüssel zu lesen.

A. Schlüssel:

18. Der Schlüssel ist durch:
Tag 4 5
Schlüssel 17, 10 11
Kaufkraft VI
eingestellt. Die Schlüsselmaschine ist mit 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 100. 101. 102. 103. 104. 105. 106. 107. 108. 109. 110. 111. 112. 113. 114. 115. 116. 117. 118. 119. 120. 121. 122. 123. 124. 125. 126. 127. 128. 129. 130. 131. 132. 133. 134. 135. 136. 137. 138. 139. 140. 141. 142. 143. 144. 145. 146. 147. 148. 149. 150. 151. 152. 153. 154. 155. 156. 157. 158. 159. 160. 161. 162. 163. 164. 165. 166. 167. 168. 169. 170. 171. 172. 173. 174. 175. 176. 177. 178. 179. 180. 181. 182. 183. 184. 185. 186. 187. 188. 189. 190. 191. 192. 193. 194. 195. 196. 197. 198. 199. 200. 201. 202. 203. 204. 205. 206. 207. 208. 209. 210. 211. 212. 213. 214. 215. 216. 217. 218. 219. 220. 221. 222. 223. 224. 225. 226. 227. 228. 229. 230. 231. 232. 233. 234. 235. 236. 237. 238. 239. 240. 241. 242. 243. 244. 245. 246. 247. 248. 249. 250. 251. 252. 253. 254. 255. 256. 257. 258. 259. 260. 261. 262. 263. 264. 265. 266. 267. 268. 269. 270. 271. 272. 273. 274. 275. 276. 277. 278. 279. 280. 281. 282. 283. 284. 285. 286. 287. 288. 289. 290. 291. 292. 293. 294. 295. 296. 297. 298. 299. 300. 301. 302. 303. 304. 305. 306. 307. 308. 309. 310. 311. 312. 313. 314. 315. 316. 317. 318. 319. 320. 321. 322. 323. 324. 325. 326. 327. 328. 329. 330. 331. 332. 333. 334. 335. 336. 337. 338. 339. 340. 341. 342. 343. 344. 345. 346. 347. 348. 349. 350. 351. 352. 353. 354. 355. 356. 357. 358. 359. 360. 361. 362. 363. 364. 365. 366. 367. 368. 369. 370. 371. 372. 373. 374. 375. 376. 377. 378. 379. 380. 381. 382. 383. 384. 385. 386. 387. 388. 389. 390. 391. 392. 393. 394. 395. 396. 397. 398. 399. 400. 401. 402. 403. 404. 405. 406. 407. 408. 409. 410. 411. 412. 413. 414. 415. 416. 417. 418. 419. 420. 421. 422. 423. 424. 425. 426. 427. 428. 429. 430. 431. 432. 433. 434. 435. 436. 437. 438. 439. 440. 441. 442. 443. 444. 445. 446. 447. 448. 449. 450. 451. 452. 453. 454. 455. 456. 457. 458. 459. 460. 461. 462. 463. 464. 465. 466. 467. 468. 469. 470. 471. 472. 473. 474. 475. 476. 477. 478. 479. 480. 481. 482. 483. 484. 485. 486. 487. 488. 489. 490. 491. 492. 493. 494. 495. 496. 497. 498. 499. 500. 501. 502. 503. 504. 505. 506. 507. 508. 509. 510. 511. 512. 513. 514. 515. 516. 517. 518. 519. 520. 521. 522. 523. 524. 525. 526. 527. 528. 529. 530. 531. 532. 533. 534. 535. 536. 537. 538. 539. 540. 541. 542. 543. 544. 545. 546. 547. 548. 549. 550. 551. 552. 553. 554. 555. 556. 557. 558. 559. 560. 561. 562. 563. 564. 565. 566. 567. 568. 569. 570. 571. 572. 573. 574. 575. 576. 577. 578. 579. 580. 581. 582. 583. 584. 585. 586. 587. 588. 589. 590. 591. 592. 593. 594. 595. 596. 597. 598. 599. 600. 601. 602. 603. 604. 605. 606. 607. 608. 609. 610. 611. 612. 613. 614. 615. 616. 617. 618. 619. 620. 621. 622. 623. 624. 625. 626. 627. 628. 629. 630. 631. 632. 633. 634. 635. 636. 637. 638. 639. 640. 641. 642. 643. 644. 645. 646. 647. 648. 649. 650. 651. 652. 653. 654. 655. 656. 657. 658. 659. 660. 661. 662. 663. 664. 665. 666. 667. 668. 669. 670. 671. 672. 673. 674. 675. 676. 677. 678. 679. 680. 681. 682. 683. 684. 685. 686. 687. 688. 689. 690. 691. 692. 693. 694. 695. 696. 697. 698. 699. 700. 701. 702. 703. 704. 705. 706. 707. 708. 709. 710. 711. 712. 713. 714. 715. 716. 717. 718. 719. 720. 721. 722. 723. 724. 725. 726. 727. 728. 729. 730. 731. 732. 733. 734. 735. 736. 737. 738. 739. 740. 741. 742. 743. 744. 745. 746. 747. 748. 749. 750. 751. 752. 753. 754. 755. 756. 757. 758. 759. 760. 761. 762. 763. 764. 765. 766. 767. 768. 769. 770. 771. 772. 773. 774. 775. 776. 777. 778. 779. 780. 781. 782. 783. 784. 785. 786. 787. 788. 789. 790. 791. 792. 793. 794. 795. 796. 797. 798. 799. 800. 801. 802. 803. 804. 805. 806. 807. 808. 809. 810. 811. 812. 813. 814. 815. 816. 817. 818. 819. 820. 821. 822. 823. 824. 825. 826. 827. 828. 829. 830. 831. 832. 833. 834. 835. 836. 837. 838. 839. 840. 841. 842. 843. 844. 845. 846. 847. 848. 849. 850. 851. 852. 853. 854. 855. 856. 857. 858. 859. 860. 861. 862. 863. 864. 865. 866. 867. 868. 869. 870. 871. 872. 873. 874. 875. 876. 877. 878. 879. 880. 881. 882. 883. 884. 885. 886. 887. 888. 889. 890. 891. 892. 893. 894. 895. 896. 897. 898. 899. 900. 901. 902. 903. 904. 905. 906. 907. 908. 909. 910. 911. 912. 913. 914. 915. 916. 917. 918. 919. 920. 921. 922. 923. 924. 925. 926. 927. 928. 929. 930. 931. 932. 933. 934. 935. 936. 937. 938. 939. 940. 941. 942. 943. 944. 945. 946. 947. 948. 949. 950. 951. 952. 953. 954. 955. 956. 957. 958. 959. 960. 961. 962. 963. 964. 965. 966. 967. 968. 969. 970. 971. 972. 973. 974. 975. 976. 977. 978. 979. 980. 981. 982. 983. 984. 985. 986. 987. 988. 989. 990. 991. 992. 993. 994. 995. 996. 997. 998. 999. 1000.

Abbildung 1.5: Tagesschlüssel

- Dobbelkrypterte Mler i grunnstilling var en fundamentalt uheldig måte å benytte Enigma på!
- 15/9-38 ble denne prosedyren endret:
 - Tilfeldig startposisjon : LEC
 - Velg meldingsnøkkel: OSW
 - Krypter meldingsnøkkel : YDE (GHU)
 - Sett meldingsposisjon og krypter melding
 - LEC YDE (GHU) sendes som preamble
- Marinen benyttet seg av mer komplekse prosedyrer

2009.05.19



- Kompliserende faktorer
 - Indikatorsystem
 - Kodebøker
 - Offizier

2009.05.19



1. Avsender velger 2 "trigram" fra "Kenngruppenbuch", f.eks. BFA og LXZ
2. Adder tilfeldig bokstav C i starten på første trigram og en ekstra bokstav B til slutt i andre trigram og dann to rader:

C B F A	→	Bigram- tabell	→	R V M K
L X Z B				E Y P W

3. Sett Enigma til dagens grunnstilling, f. eks. ABC
Krypter andre trigram LXZ → RGL
Meldingsindikator blir da RGL
4. Sett Enigma til RGL og krypter meldingen
5. Send indikator R E V Y M P K W foran chiffterkst

2009.05.19



W/T RED FORM.

Date: 26.12.43
 Time: 12.00
 Location: ...
 ...

UTRE	0000	0000	0000
UTRE	0000	0000	0000
UTRE	0000	0000	0000
UTRE	0000	0000	0000
UTRE	0000	0000	0000
UTRE	0000	0000	0000
UTRE	0000	0000	0000
UTRE	0000	0000	0000
UTRE	0000	0000	0000
UTRE	0000	0000	0000

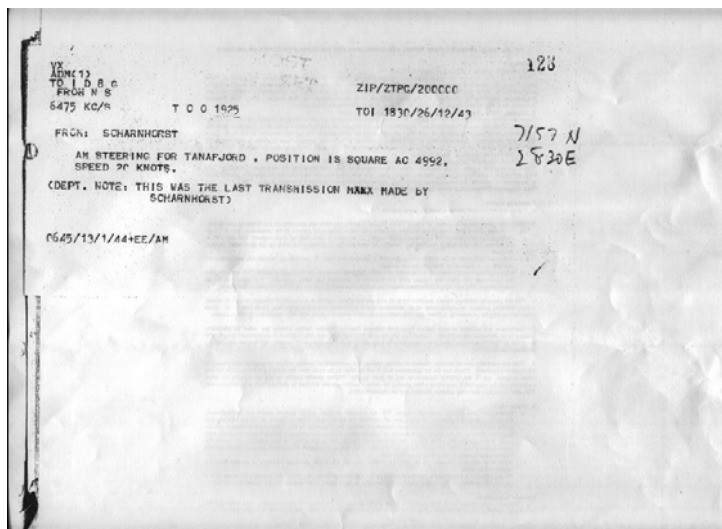


HMS Duke of York

2009.05.19



Er dette samme melding? ←



2009.05.19

36 Thales Norway AS



THALES

Dekryptering med M3 mai 2008 ←

The Enigma key for Scharnhorst's Last Message:

UKW: B

Wheel Order : 368

Stecker: AN, EZ, HK, IJ, LR, MQ, OT, PV, SW, UX

Rings : AHM

Message key : UZV

The raw German plaintext is:

**steuere j tanafjord j an standort qu aaa ccc vier neun neun zwo fahrt zwo nul
sm xx scharnhorst hco**

Written out in full it becomes:

**Steuere Tanafjord an. Standort Qu. AC 4992, Fahrt 20 sm [Seemeilen].
Scharnhorst**

2009.05.19

37 Thales Norway AS



THALES