

Enigma!

Giocarci per capire come funziona

Storia dell'Informatica
a.a. 2020/21

- Le procedure d'uso originali
 - Personale, circuiti, chiavi giornaliere...
 - Nel caso di una Enigma I con riflettore B, il modello “base” usato dalla Wehrmacht

- Il simulatore, grazie a Dirk Rijmenants

- Un paio di esempi, codifica e decodifica

una macchina, tre operatori



Geheime Kommandosache
Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28
für Oktober 1944

Nr. 00008

| | Datum | Wahzenlage | Ringstellung | Steckerverbindungen | Kennguppen |
|----|-------|------------|--------------|-------------------------------|-----------------|
| St | 31. | IV V I | 21 15 16 | KL IT FQ HY XC NP VZ JB SE OG | jkm ogi ncj glp |
| St | 30. | IV II III | 26 14 11 | ZN YO QB ER DK XU GP TV SJ LM | ino udl nam lax |
| St | 29. | II V IV | 19 09 24 | ZU HL CQ WM OA PY EB TR DN YI | nci oid yhp nip |
| St | 28. | IV III I | 03 04 22 | YT BX CV ZN UD IR SJ HW GA KQ | zqj hlg xky ebt |
| St | 27. | V I IV | 20 06 18 | KX GJ EP AC TB HL MW QS DV OZ | bvo sur ccc lqe |
| St | 26. | IV I V | 10 17 01 | YV GT OQ WN FI SK LD RP MZ BU | jhx uuh giw ugw |
| St | 25. | V IV III | 13 04 17 | QR GB HA NM VS WD YZ OF XK PE | tba pnc ukd nld |
| St | 24. | III II IV | 09 20 18 | RS NC WK GO YQ AX EH VJ ZL PF | nfi mew xbk yes |
| St | 23. | V II III | 11 21 08 | EY DT KF MO XP HN WQ ZL IV JA | lsd nuo vcr vex |
| St | 22. | I II IV | 01 25 02 | PZ SE OJ XF HA GB VQ UY KW LR | yji rwy rdk nso |
| St | 21. | IV I III | 06 22 03 | GH JR TQ KF NZ IL WM BD UQ EC | ema mlv jji iqh |
| St | 20. | V I II | 12 25 08 | TF RQ XV DZ PY NL WI SJ ME GB | xjl pgs ggh znd |
| St | 19. | IV III II | 07 05 23 | ZX EU AC GD KP VO QS NW HL RM | vpj zqe jrs cgm |
| St | 18. | II III V | 19 14 22 | WG OM RL DB ST AQ PZ XH YN IJ | oxd lmb iou ytt |
| St | 17. | IV I II | 12 08 21 | ME HX BF WY ZD TR FJ AG IL KQ | tak pjs kdh jvh |
| St | 16. | I II III | 07 11 15 | WZ AB MO TF RX SG QU VY YN EL | pzg evw wyt iye |
| St | 15. | III II V | 06 16 02 | GT YC EJ UA RX PN IS WB MH ZV | bhe xzm yzk evp |
| St | 14. | II I V | 23 05 24 | AZ CJ WF UY SO QV MI NH DP GX | fdx tyj bmq typ |
| St | 13. | IV II V | 03 25 10 | CX KN JR DQ IU TL HZ MF EP WB | zfo bjr zwx gvn |
| St | 12. | I III II | 26 01 18 | QB YE WN AI GJ TO HR FK PS CM | upc anf tkr pwz |
| St | 11. | V I III | 17 13 04 | SV GO PA ZR FN HI YM WT DE BJ | vdh ego wmy uti |
| St | 10. | I V IV | 26 07 16 | SW AQ NF FO VY UX MK CL HT ZJ | rpl anw vpr mhn |
| St | 9. | I III IV | 17 10 18 | EH IR GK NZ SP UA LD CQ JM YV | knq ysq rhj tlj |
| St | 8. | V II I | 23 11 25 | QY OG ST HA CB WD KL JN VX IU | lro avw axh gws |
| St | 7. | II III I | 06 12 03 | BG FS TH JE VK PI CU QA OD NM | aty mbb mvo jnz |
| St | 6. | I IV V | 24 19 01 | IR HQ NT WZ VC OY GF LF BX AK | bhc iwo zgz rnr |
| St | 5. | II IV III | 05 22 14 | MK GO RQ XT DW IA ZL SY PJ EN | bok rzw kzo ryl |
| St | 4. | IV II I | 15 02 21 | KD PG CO FW HJ RY MT QL VB UZ | kpk php xmo pfw |
| St | 3. | III V IV | 03 23 04 | DY CP WN OV QH UZ RA TI GL SM | hjj nkt ytn pvo |
| St | 2. | I III V | 13 18 01 | DR VJ FS KJ IU HX AQ GT YO FC | ppq fqw oiy ruj |
| St | 1. | II IV I | 06 17 26 | AC LS BQ WN MY UV FJ PZ TR OK | bol ooi ywv sfb |

- Per il proprio circuito, una volta al dì
- Walzenlage und Ringstellung
 - La scelta e il posizionamento dei rotori
 - La traslazione del disco cifrante di ogni rotore
- Steckerverbindungen
 - I cavetti sul frontale della macchina
 - Complicata... ma alla fine aggiunge solo una monoalfabetica in più (parziale anche)

- Identificare il circuito (Buchstabenkennggruppe)
 - Scegliere, a caso, uno dei gruppi del Kennggruppen
 - Completare il campo con 2 lettere scelte a caso messe prima o dopo, a caso

- Stabilire il Grundstellung
 - È la chiave del messaggio, diversa per ogni messaggio
 - Scegliere 3 lettere, a caso!

- La raccomandata casualità fu spesso disattesa

- Crittare la chiave del messaggio
 - Impostare i rotori alle prime 3 lettere del messaggio, cioè del Buchstabenkenngruppe
 - Crittare le 3 lettere della chiave

- Crittare il testo del messaggio
 - Impostare i rotori alla chiave del messaggio
 - Crittare il resto del messaggio

- Appuntarsi lettera per lettera e trasmettere

- La striscia del giorno del circuito destinatario
 - | III II V | 06 16 02 |
 - | GT YC EJ UA RX PN IS WB MH ZV |
 - | bhe xzm yzk evp |

- Il testo del messaggio e la chiave del messaggio
 - DIE RATIONEN SAUGTEN
 - HMR

- In pratica
 - YZKAB HMRDI ERATI ONENS AUGTE N
 - YZKAB WYMEU LVJKT IEQCA RCSRL G

- In genere si ascoltano più circuiti
 - La prima cosa da fare è identificare il circuito
 - Dal Buchstabenkennggruppe, i primi 5 caratteri
 - Apposta in chiaro, anche se apparentemente no

- Il resto è facile: in pratica il processo è lo stesso
 - Identificato il circuito si imposta la macchina
 - Si decodifica la chiave (con le prime tre lettere)
 - Si decodifica il testo del messaggio (con la chiave)

□ Supponiamo di ascoltare tre circuiti

- | V IV III | 13 04 17 | QR GB HA NM VS WD YZ OF YK PE | tba pnc ukd nld |
- | III II V | 06 16 02 | GT YC EJ UA RX PN IS WB MH ZV | bhe xzm yzk evp |
- | I III II | 26 01 18 | QB YE WN AI GJ TO HR FK PS CM | upo anf tkr pwz |

□ E che il marconista ci abbia portato

- YZEVV GJMAM RAPGF JQIHT MEYHC CDZMM BUDGI HPQAX EBTPR

□ Buon lavoro :)