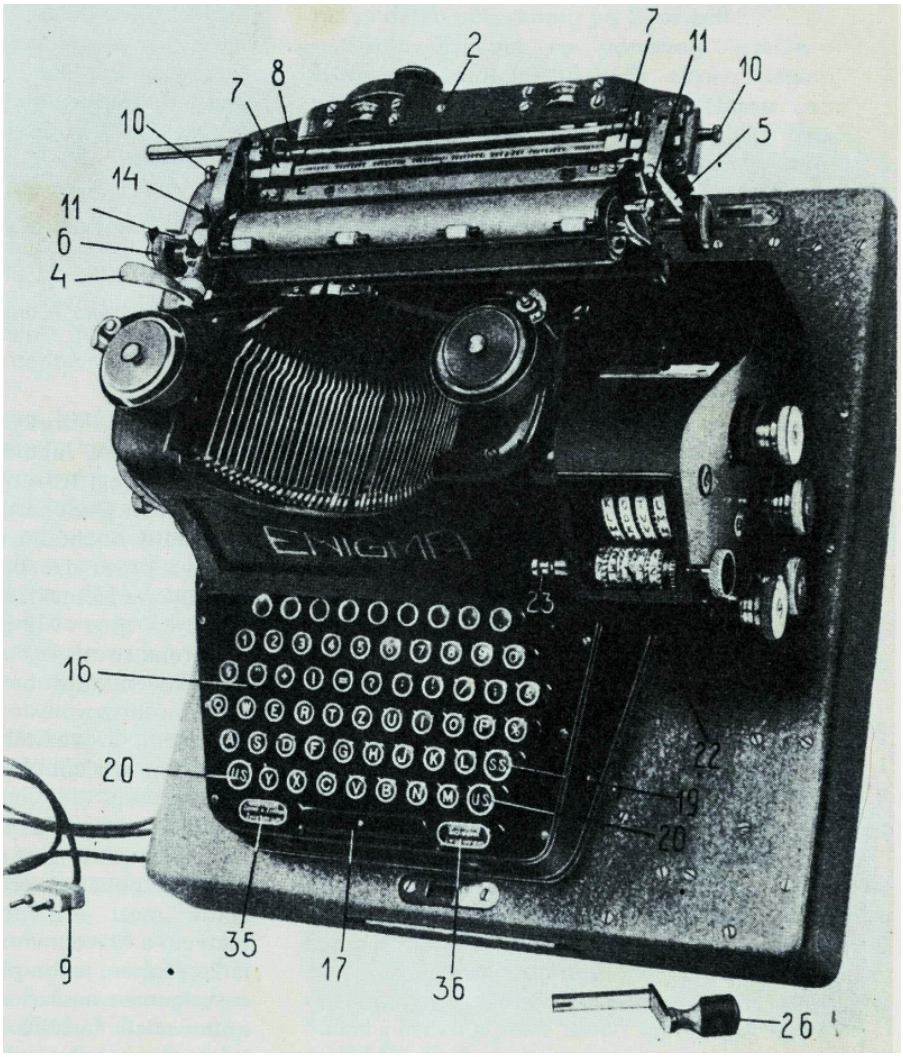
Enigma :)

Šifrovací stroj používaný počas Druhej svetovej vojny hlavne v nemeckej (nacistickej) armáde a armádach ich spojencov.

Vynašiel ho roku 1919 Holanďan Hugo Koch, ktorý si ho dal v Den Haagu patentovať[1]. Chcel ho začať vyrábať vo veľkom ako pomôcku pre banky, obchodníkov a podobne. Mal však problémy technického rázu a tak predal patenty strojnému inžinierovi Arthurovi Scherbinsovi z Nemecka. Tomu sa podarilo v roku 1923 vyrobiť a zdokonaliť prvý fungujúci prototyp, ktorému dal meno Enigma[2]. Predaj však bol minimálny. Chytila sa ho až nemecká armáda v roku 1924, kedy na Svetovom poštovom kongrese v Stockholme niekoľko prístrojov zakúpila. Po otestovaní a zdokonalení ho v roku 1926 zaradila do svojho výstroja. Od roku 1935 bola Enigma zavedená ako hlavný kódovací prístroj pre spojenie medzi armádou, letectvom, námorníctvom a výzvednými službami.

Zloženie prístroja Enigma

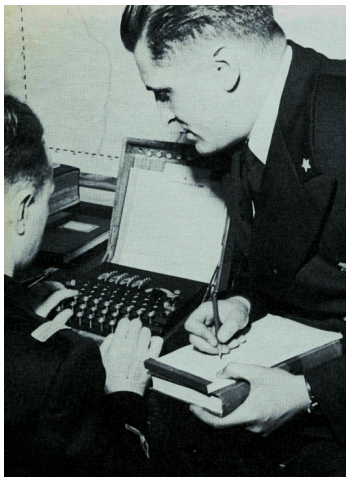


2. skrutka pre upevnenie vozíka; 4. posun riadka; 5. uvoľnenie papiera; 6. uvoľnenie valca; 7. nastavenie okraja; 8. kontrolky prevádzky: kódovanie, dekódovanie, čistý text; 9. zástrčka elektrického kabelu; 10. skrutka uvoľnenia vozíka ; 11. rukoväť pre vybratie vozíka; 14. páka pre vybratie valca; 16. klávesnica; 17. medzerník; 19. zmena na veľké písmená; 20. zmena na malé písmená; 22. počítadlo; 23. nulovací gombík počítadla; 26. kľučka; 35. číselná zmena; 36. písmenová zmena

Už v roku 1929 začali na rozlúštení kódov Enigmy pracovať poľskí odborníci. Vojenským kryptológom v spolupráci s mladými matematikmi Marianom Rejewským, Jerzym Róyyckým a Henrykom Zygalským sa do v decembri 1932 podarilo. V nasledujúcich rokoch vyrobili 15 kópií stroja a pokračovali v štúdiu jeho možností. Roku 1939 odovzdali po jednom prístroji francúzskej a britskej výzvednej službe. Poľské dešifrovacie stredisko bolo evakuované pred Nemcami cez Rumunsko do Francúzska, roku 1940 do Alžírska a odtiaľ späť do okupovaného Francúzska. Roku 1942 konečne skupinu prepašovali do Anglicka. Od tej doby spolupracovali pri lúštení s anglickými odborníkmi na šifry a kódy v britskom Bletchley Parku, kde sa podarilo nielen prelomiť

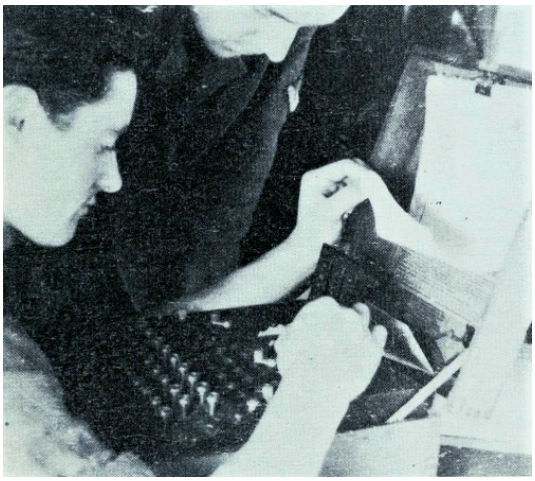
ďalšie, zložitejšie kódy, ale ich prelomenie na viac ako 30 rokov dokonale utajiť. Podľa odborníkov sa vďaka prelomeniu nemeckých šifier podarilo skrátiť Druhú svetovú vojnu o dva roky.

Enigma zohrala veľkú úlohu počas Druhej svetovej vojny. Nemci sa totiž domnievali, že k ich šifrovaným správam nemá prístup nikto nepovolaný. Ich kódovací prístroj Enigma však nebol neporaziteľný.



Šifrovanie depeše pre Enigmu v talianskom námoníctve

Kópia Enigmy postavená podľa poľských plánov v rokoch 1939-1940 vo Francúzsku



Nastavovanie Enigmy

[1] Číslo patentu bol 10700.

[2] Zariadenie na prvý pohľad pripomína robustný písací stroj, pre laika však bolo dosť zložité. Klávesnica prenášala elektrické signály vyrobené kontaktom cez elektricky prepojené valčeky. Dvadsaťšesť kontaktov na vonkajšom povrchu valčeka predstavovalo dvadsaťšesť písmen latinskej abecedy. Za klávesnicou bol každý z kontaktov jedného valčeku prepojený s nejakým kontaktom iného valčeku a spojovací káblik bol pripojený ku kontrolke, ktorá signalizovala, aké písmeno elektrický systém vytvoril z písmena pôvodného, napísaného na klávesnici. Prvý model Enigma bol vybavený troma kódovými valčekmi a napájaný bol z batérií. Mohol vytvoriť okolo 22 miliónov kombinácií (možnosti kódovaní).