První rotorové šifrovací stroje …

Crypto-World 3/2005
Pavel Vondruška, ČESKÝ TELECOM, a.s
(pavel.vondruska@crypto-world.info **)**

Těsně po skončení první světové války – hned ve čtyřech různých zemích a to zcela nezávisle na sobě – zažádali různí vynálezci o patent na šifrovací stroj, jehož základem byly otočné rotory. Mezi nimi byl také přístroj, který se po několika vylepšeních stal jednoznačně nejznámější šifrovacím strojem na světě – **Enigma** německého vynálezce Arthura Scherbia. Zájem o vzestup a pád tohoto přístroje, který tak významně ovlivnil průběh druhé světové války, dodnes do řad kryptologů přivádí další mladé adepty o tuto překrásnou vědu.

Seznamme se v této krátké glose se jmény a osudy dalších vynálezců a řekněme si něco o obchodním úspěchu (či spíše neúspěchu) jejich přístrojů.

Mimo již zmíněného německého vynálezce **Arthura Scherbia (1878 -1929),** který svůj patent nahlásil 23. 2. 1918, se zabývali šifrátory na obdobném rotorovém principu jako Enigma další vynálezci a to Americe, Holandsku a Švédsku.

- **Edward Hebern (USA, 1869-1952), patent 1917, 21.3.1921**

Jeden z prvních vynálezců, který se myšlenku rotorových šifrovacích strojů pokusil uplatnit a který ve svůj vynález (ostatně jako všichni zde jmenovaní) hluboce věřil, byl americký vynálezce Edward Hebern (1869 –1952). Během svého života podal více patnetů na stroje založené na uvedeném principu.

Na doprovodném obrázku je jeden ze starších typů jím vyráběných šifrátorů. Přesné datum podání patentu k tomuto zařízení se mi nepodařilo zjistit, v jednom ze zdrojů je uváděn rok 1917. Pozdější patent, na již dokonalejší zařízení, pochází z března roku 1921 a má číslo # 1,510,441.

V polovině 20. let 20. století začal Hebern stavět továrnu nákladem 380 000 dolarů. Prodal však jen dvanáct přístrojů, celkem asi za 1 200 dolarů, a roku 1926 byl nespokojenými akcionáři pohnán k soudu a podle kalifornského obchodního práva shledán vinným.

Singh ve své knize Kniha kódů a šifer uvádí, že příčinou jeho obchodního neúspěchu bylo to, že právě v tomto období se začala nálada americké společnosti měnit. Prezidentem se stal Herbert Hoover, který se pokusil zahájit novou éru mezinárodních vztahů. Jeho ministr zahraničí Henry Stimson vyslovuje svůj proslulý výrok, že „gentleman nečte cizí dopisy“. Stát, který věří, že není správné číst cizí dopisy, časem začne věřit i tomu, že jeho korespondenci také nikdo nečte, takže nevidí důvod pro pořízení kvalitních šifrovacích strojů.

Osobně se však domnívám, že rozhodujícím faktorem, proč zařízení Edwarda Heberna neuspělo při prodeji armádě nebo obecněji „státu“ (diplomatické služby, policie atd.), bylo to, že zařízení nemělo pro svůj jednoduchý design z hlediska bezpečnosti velkou odolnost. Hebern totiž nevěděl, že jeden z velikánů kryptoanalýzy William F. Friedman (24.9, 1891 – 12.11, 1969) podrobil jeho zařízení analýze a ve své práci demonstroval, že zařízení je luštitelné.

- **Hugo Alexander Koch (Holandsko, 1870-1928), patent 7. 10. 1919**

Přístroj na podobném principu (pohyblivé rotory) si v roce 1919 nechal patentovat Hugo Alexander Koch (patent č. 10 700). Ani jemu se však nepodařilo svůj nápad na vývoj a prodej šifrovacích strojů proměnit v obchodní úspěch a roku 1927 (podle jiných zdrojů 1928) svá patentová práva prodává a přebírá je firma Arthura Schrebia. Díky tomu se v návrhu Enigmy objevuje další vylepšení, tzv. Kochův reflektor.

Nebyl však první, kdo se v Holandsku zabýval rotorovými šifrátory. Prvními, kdo je vyvinul a postavil pro využití v holandském námořnictvu, byli dva důstojníci **Theo A. van Hengel (1875 – 1939)** a **R. P. C Spengler (1875 – 1955)** a to již během první světové války – přesněji v roce 1915. Jejich práce však byla utajena a nezachovalo se žádné z jimi navržených zařízení. Jejich jména a práce tak upadla v zapomnění, a proto lze předpokládat, že o těchto šifrátorech H. A. Koch nevěděl a pracoval zcela samostatně. Právem mu tedy patří označení vynálezce.

- **Arvid Damm (Švédsko, ?-1927), patent 10. 10. 1919**

Ve Švédsku získal patent na rotorový šifrátor zakladatel firmy AB Cryptograpf Arvid Damm. Byl však obchodně neúspěšný a v roce 1921 firmu společně s patentem kupují Karl Hagelin a Emanuel Nobel. Syn Karla Hagelina **Boris Hagelin (1892-1983)** se rozvojem původní myšlenky rotorového šifrátoru dále zabýval a neustále jej zdokonaloval. V roce 1948 se stěhuje ze Švédska do Švýcarska. Zde zakládá firmu Crypto AG. Firma v následujících letech získala světovou proslulost prodejem šifrátorů, které koncepčně navázaly na původní modely (jeden z pozdějších modelů je na doprovodném obrázku). Dodnes Crypto AG úspěšně působí na trhu s kryptologií.

Použité zdroje :

[1] Karl de Leeuw: The dutch invention of the rotor machine, 1915 - 1923. Cryptologia 27 (2003), 73 - 94
[2] Simon Singh : Kniha kódů a šifer, DoKořán, Praha 2003, str.137-138
[3] Bengt Beckman: ”Svenska kryptobedrifter”, 1996
[4] http://www.staff.uni-mainz.de/pommeren/Kryptologie/Klassisch/4a_ZylRot/HistRot.html
[5] http://www.meydaonline.com/crypto/history/hebern.htm
[6] http://www.jproc.ca/crypto/hebern_1.html
[7] http://www.geocities.com/ResearchTriangle/Node/3751/cypher.html