ZÁPADOČESKÁ UNIVERZITA

Fakulta aplikovaných věd

Katedra kybernetiky
SEMESTRÁLNÍ PRÁCE Z PŘEDMĚTU

HKUI

Téma: Referát na téma Enigma

Datum: 4. 02. 2018 Po / 11:10 / přednáška
Vypracovala: **Markéta Rajnyšová** Osobní číslo: **A17B0570P**

Enigma

Co je Enigma

Enigma je přenosný šifrovací mechanismus, používaný k šifrování a dešifrování tajných informací, který byl vyráběn od začátku dvacátých let 20. století, konkrétně byla Enigma vynalezena v roce 1918 Albertem Schreibusem, který návrh přinesl do německé armády, ta však o Enigmu nejevila zájem, takže patent byl prodán firmě Gewershaft.

Enigma byla založená na kombinaci elektrického a mechanického systému. Skládala se z rotujících disků (3 – 4) a klávesnice, která každým stisknutím uzavřela elektrický obvod, proud pak prošel různými komponenty a došel až k jedné z mnoha žárovek, které signalizovaly jednotlivé zašifrované písmeno. Enigma v sobě měla také zabudovaný reflektor, který zajistil to, aby se zpráva dala i stejně dešifrovat.

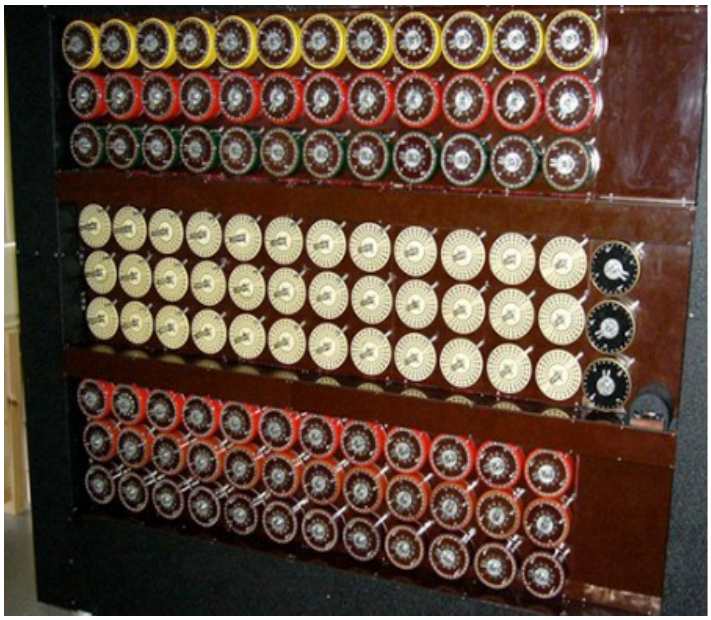
Civilní Enigma

Enigma byla vyráběna nejdříve jako civilní. Jelikož o ni neměly armády zájem, začala se vyrábět Enigmy typu A, který byl vystaven na kongresu Světově poštovní unie. Stroj byl velký (65cm x45cm x35cm) a vážil něco málo přes 50kg. Při výrobě modelu B se snažili tuto nevýhodu odstranit, avšak skutečně se jim to povedlo až u modelu C, který v sobě neměl zabudovaný psací stroj ale již zmíněné žárovky. I tento model byla ale později nahrazen modelem D, který se ve velkém množství vyvážel do celého světa.

Armádní Enigma

Poté byla Enigma vyráběna jako armádní. První verzi měla Německá armáda, konkrétně model Funkschlüssel C, který se do výroby dostal v roce 1925. Obsahoval klávesnici s 29 znaky, včetně přehláskovaného A, O a U. Více známa verze Enigmy, Wehrmacht, byla představena roku 1928, v 1930 přejmenována na Enigma I. Pro komunikaci na vyšší úrovni byla později používána Enigma II s osmi rotory, ale ta nebyla tolik spolehlivá, takže se z ní upustilo. Počet vyrobených strojů se pohybuje kolem 100 000, a díky tomu, že se Britům podařilo utajit schopnost prolomení šifry, využívala se Enigma i v 50. letech v SSSR i v rozvojových zemích, což pro spojence znamenalo velké výhody ve špionáži.

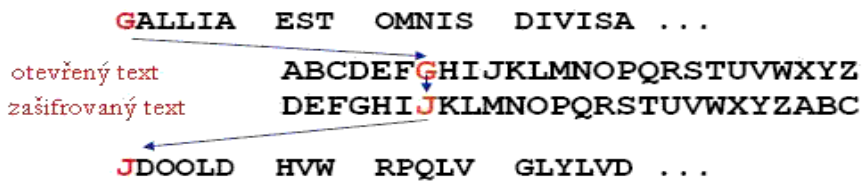
Enigma a její význam v druhé světové válce i po ní



Německá armáda o Enigmu začala jevit zájem až po usednutí Adolfa Hitlera k moci, viděli v ní možnost zadávání šifrovaných rozkazů, určování poloh jednotek a lodí, aniž by spojenci měli jakékoliv informace o pohybu jednotek německé armády, proto se Enigma stala největší Německou zbraní druhé světové války a zároveň armáda odkoupila patent na Enigmu a stáhla ji z obchodů. Enigma byla nejvíce využívána v ponorkách, které měly tím pádem vysokou výhodu oproti spojeneckým konvojům. Když se spojenci dostali k ponorce U-110, Enigmu vzali a poslali do Blatchey Parku, kde se snažili nejlepší šachisté, matematici a kryptoanalitici z celé Anglie (přibližně 5000 zaměstnanců), kteří se pod vedením Alana Turinga prolomit kód.
Tato Enigma však nebyla prvním šifrovacím zařízením ukradeným Německé armádě. První stroj sestrojený na princip Enigmy byla Bomba, která Polským vojskům umožňovala sledovat pohyb Němců. I díky tomu se Britům následně podařilo rozluštit kódy jako třeba Vážka (luftwaffe). Narazili i na kód jménem Žralok, který nebyli schopni rozluštit, protože měl čtvrtý přídavný disk který nabízel až 150 triliónů kombinací, až do té doby, kdy Blatchey Park pronikl do Žraloka díky meteorologickým hlášením, které se vysílaly pomocí tří disků, a rozluštění těchto šifer bylo již snadné. Když Německá armáda měla několik neúspěšných akcí v Pacifiku, začali tušit, že jsou spojenci schopni rozluštit kód z třídiskových strojů, začali proto využívat pouze stroje se čtyřmi disky. Tyto šifry Bletchey Park prolomil až po 10 měsících, kdy v Egyptě chytli ponorku U-559 s čtyřdiskovou Enigmou na palubě. Díky té mohli pak Britské armády spolu se Spojenci znát předem taktiku Němců a vyhrát válku.

Kryptografie

Kryptografie je nauka o tom, jakými způsoby se dají zprávy šifrovat. Tato věda velmi ovlivnila průběh a vývoj dějin. Období kryptografie se dělí na dvě období. Prvním obdobím je klasická kryprografie, trvající do poloviny 20. století. K šifrování se používal psaný text na papíře. Vynalezením Enigmy ale začalo druhé období, kde se začaly používat sofistikované přístroje, v současnosti používáme počítače. Dobře známé metody jsou například steganografie (neviditelné inkousty), Caesarova šifra (posouvání písmen v abecedě), tabulka záměn nebo již zmíněná Enigma. V současnosti používáme například AES nebo HASH.



Použité zdroje:

Enigma machine online - https://en.wikipedia.org/wiki/Enigma_machine

BBC History – Enigma online - http://www.bbc.co.uk/history/topics/enigma

History of War – The Enigma machine online - https://www.historyanswers.co.uk/history-of-war/the-enigma-machine/

Alan Turing: The Enigma - paperback