Portál pre odborné publikovanie ISSN 1338-0087

História kryptografie

Brezovský Michal · Elektrotechnika, Študentské práce

25.01.2010

Kryptológia a jej história tvoria významnú oblasť ľudského poznávania v súvislosti s bezpečnosťou, dôvernosťou a utajením. Jej cieľom od počiatku je chrániť utajované dáta pred nepovolanými osobami. Dnes je kryptológia súčasťou každodenného života.

1. Úvod

V mojej práci sa budem zaoberať históriou kryptológie, od rannej éry kryptografie (Egypt, Mezopotámia), cez staroveké Grécko. V prvej časti vymedzím základné pojmy, potom priblížim významné metódy v histórii kryptografie, ktoré boli historickým prelomom v kryptológií, vysvetlím počiatky princípu substitúcie, transpozície, polyalfabetických šifier, prvých mechanických a elektronických šifrovacích strojov, až po začiatky éry počítačov.

1.1. Kryptológia

Slovo kryptológia pochádza z Gréčtiny zo slov $\kappa\rho\upsilon\pi\tau o\varsigma$ [kryptós], čo znamená ukryť a $\gamma\rho\alpha\varphi\omega$ [grafó], čo znamená písať. V dnešnej dobe je kryptológia považovaná za časť matematiky a počítačových vied a je veľmi pridružená k informatike, počítačovej bezpečnosti a počítačovému inžinierstvu.

Je nenahraditeľná v oblastiach živote, kde je nevyhnutné nejakým spôsobom utajiť komunikáciu pred treťou stranou. V minulosti bola kryptológia spojená najmä s vojnovým obdobím, no v súčasnosti je spojená s každodenným životom (zabezpečenie bankomatov, počítačov heslom, komunikácia na internete, atď.). Kryptológia sa rozdeľuje na kryptografiu, kryptoanalýzu a steganografiu [6].

1.2. Kryptografia

Je oblasť kryptológie, kde sa snažíme navrhnúť šifrovací systém, ktorý bude spĺňať autenticitu, dôvernosť, dostupnosť, integritu.

1.3. Kryptoanalýza

Je oblasť kryptografie, ktorá skúma metódy lúštenia šifrovacích systémov, čiže rozoberá správy a snaží sa rozšifrovať správu a preniknúť do systému.

1.4. Steganografia

Je oblasť kryptológie, ktorej cieľom je zatajiť existenciu danej správy. Steganografia v preklade znamená ukryté pred zrakom.

1.5. Substitučné šifry

Podstata substitučných šifier je v tom, že každý znak pôvodnej nezašifrovanej správy sa nahradí nejakým iným znakom. V tomto článku bude uvedených niekoľko významných predstaviteľov substitučných šifier z hľadiska histórie.

1.6. Transpozičné šifry

Zatiaľ čo substitučné šifrovacie metódy sú založené na nahradzovaní znakov inými znakmi, transpozícia je poprehadzovanie znakov textu. Každý znak si zachováva svoju podobu, ale mení svoju pozíciu. Ako daná transpozícia prebieha závisí od šifrovacieho algoritmu. Existuje veľké množstvo jednoduchých transpozičných šifier, ale existujú aj odolné šifry bežne používané aj dnes. V tomto článku bude uvedených niekoľko významných predstaviteľov transpozičných šifier z hľadiska histórie.

1.7. Polyalfabetické šifry

Je zloženie niekoľkých, zvyčajne jednoduchých šifier, ktoré vytvoria „silnú“ polyalfabetickú šifru.

1.8. Hybridné šifry

Existujú mnohé šifry, ktoré v sebe zahŕňajú znaky substitúcie aj transpozície. Takéto hybridné šifry majú za úlohu spojiť výhody oboch metód a zvýšiť tak bezpečnosť algoritmu. Príkladmi takýchto šifier sú napr. šifra ADFGVX, DES a AES [4].

2. Ranná éra kryptografie

Egyptskí pisári okolo r. 1900 p. n. l. používali neštandardné hieroglyfické symboly namiesto obvyklých hieroglyfov, čím sa text pre bežného čitateľa stal zašifrovaným.

Tabuľka z Mezopotámie okolo r. 1500 p. n. l. obsahovala zašifrovanú formulu na výrobu glazúrovej keramiky. Použitá šifra využívala substitúciu písmen za písmená, ktoré majú rovnakú zvukovú hodnotu v rôznych slovách.

Hebrejci okolo roku 600-500 p. n. l. používali jednoduchú reverznú substitučnú šifru atbaš. V tejto šifrovacej metóde je prvé písmeno abecedy nahradené posledným, druhé predposledným atď. a naopak. Názov atbaš je odvodený od toho, že prvé písmeno hebrejskej abecedy „alef“ je nahradené posledným písmenom „tav“, druhé „bet“ je nahradené predposledným „sin“. Prejavy tohto šifrovania nájdeme aj v Starom zákone. V hebrejskej literatúre sú známe podobné ďalšie dve substitúcie: albam a atbah.

V starom Grécku v Sparte okolo r. 500 p.n.l. používali prvú známu mechanickú

pomôcku na šifrovanie – skytalé. Tento šifrátor mal tvar dreveného valca, na ktorý sa prúžok za prúžkom tesne vedľa seba namotal pruh papyrusu, kože alebo pergamenu. Správa sa vypisovala smerom od jedného konca valca k druhému, až sa zaplnil celý papyrus. Potom sa pruh odmotal. Správa na ňom nedávala zmysel, pokiaľ sa u príjemcu nenamotala na rovnako hrubý valec, pretože písmena boli poprehadzované (transponované) [7].

Obr. 1. Skytalé

3. Významné metódy v histórií

Nasledujúce šifrovacie metódy a postupy sa zapísali významným spôsobom v histórií kryptografie a výrazne ovplyvnili nasledujúce obdobie vývoja šifrovacích systémov.

3.1. Cézarova šifra

Julius Caesar (100-44 p. n. l.) používal jednoduchú substitučnú šifru, ktorá nesie po ňom aj pomenovanie. Caesar používal niekoľko šifier, ale kniha, kde sa popisovali, sa nezachovala.

V Caesarovej šifre sa každé písmeno nahradí písmenom, ktoré v abecednom poradí leží tri písmena za ním. Na tú dobu to bola prakticky nerozlúštiteľná šifra, jednoduchá a účinná, až kým ju neprezradil Cicero, ktorý prešiel do tábora Caesarových protivníkov.

Napr. výrok LIST ZNICIT by v Caesarovom liste nadobudol tvar OLVW CQLFLW. Napriek tomu, že Cézarova šifra nebola bezpečná, stala sa základom pre neskoršie šifrovacie metódy [5].

3.2. Albertiho disk

Leon Battista Alberti – nazývaný aj otcom západnej kryptológie. Bol všestranne vzdelaný človek, je známy ako autor prvej učebnice kryptoanalýzy. Albertiho 25 stranová práca je prvá práca napísaná v západnej Európe venovaná kryptoanalýze. Dielo obsahuje výklad lúštiteľských postupov na základe jazykových znalostí, roztriedenie systémov šifrovania na substitúciu a transpozíciu, objav *polyalfabetickej* substitúcie a šifrovanie kódov.

Albertiho disk bola pôvodne mechanická pomôcka na realizovanie Cézarovej šifry. Pozostával z dvoch otáčavých kotúčov reprezentujúcich otvorené a zašifrované znaky, pričom ich otáčanie simulovalo polyalfabetickú substitúciu [1, 109].

Neskôr tento systém vylepšil tak, že na zašifrovanie správy používal viacero takýchto

posunov. Každú zmenu vylepšil úvodným veľkým písmenom. A ešte silnejšia verzia mala vnútorný disk vymeniteľný, a na ňom bola abeceda daná ľubovoľnou permutáciou.

3.3. Trithemiusova tabuľka

Prvá tlačená kniha s kryptologickou náplňou bola kniha od známeho benediktínskeho mnícha Johannesa Trithemiusa. V piatej knihe jeho súboru šiestich kníh "Polygraphiace libri sex" je zavedená tzv. "tabula recta", ktorá je základom pre polyalfabetické šifry. Tabula recta bola štvorcová tabuľka, v ktorej každý riadok tabuľky je posunutý o jedno písmeno do ľava [2].

Tabula recta, bola označovaná ako predpočítačová šifra, ktorá bola ekvivalentom Albertiho disku, a ktorú využívala aj Vigénerova šifra.

Všetky polyalfabetické šifry sú založené na Cézarovej šifre.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Obr. 2. Tabula recta

3.4. Tajný kľúč

V r. 1553 Vyšla brožúra "La cifra" nenápadného talianskeho šľachtica Giovana Batistu Belasa popisujúca kryptosystém, ktorého základom je tajný kľúč. Tajným kľúčom je tu slovo, príp. veta, ktorá sa opakovane píše nad otvorený text. Každé písmeno otvoreného textu je potom šifrované abecedou, ktorá je určená písmenom nad ním. Pri šifrovaní sa používala Trithemiusovu tabuľku. V tomto systéme už význam a úloha *kľúča* vystupujú do popredia. Jeho výhoda je zrejmá. Jeden a ten istý systém je možné podľa potreby variabilne meniť. To už nie je ďaleko od myšlienky, vytvoriť taký systém, v ktorom by bola kľúčom samotná správa. Takýto autokľúč navrhol v roku 1586 Vigenére [5].

3.5. Portov disk

Talian Giovanni Battista Porta napísal niekoľko kníh. Jeho najslávnejšia kniha z oblasti kryptológie sa nazývala "De Furtivis Literarum Notis" vyšla v roku 1563 a "vládla" v kryptografií 300 rokov. Porta v knihe jasne a výstižne sústredil kryptologické poznatky

vtedajšej doby, rozdelil šifry na substitučné a transpozičné, uviedol prvú digrafickú šifru.

Ďalej zverejnil návod na lúštenie monoalfabetickej substitúcie a vypracoval aj niekoľko metód lúštenia polyalfabetických šifier.

Portova digrafická šifra bola tvorená tabuľkou, kde riadky a stĺpce boli označené písmenami abecedy. Vo vnútri tabuľky boli symboly (značky), ktoré reprezentovali šifrové výrazy vždy namiesto dvojice písmen otvoreného textu, určených riadkom a stĺpcom tabuľky. Jeho najväčším prínosom bola malá poznámka, ktorá definovala *všeobecnú polyalfabetickú šifru*.

Doporučil čo najdlhší kľúč v Belasovom systéme a potom poznamenal, že Trithemiusovu tabuľka nemusí obsahovať len vzájomne posunuté abecedy, ale abecedy úplne poprehadzované, nesúvisiace. Tým vznikla všeobecná polyalfabetická substitúcia, pretože jednotlivé písmená otvoreného textu sú šifrované rôznymi substitúciami, ktoré určuje kľúč.

Portov disk zdokonaľoval Albertiho, Belasovu a Trithemiovu metódu [1, 111].

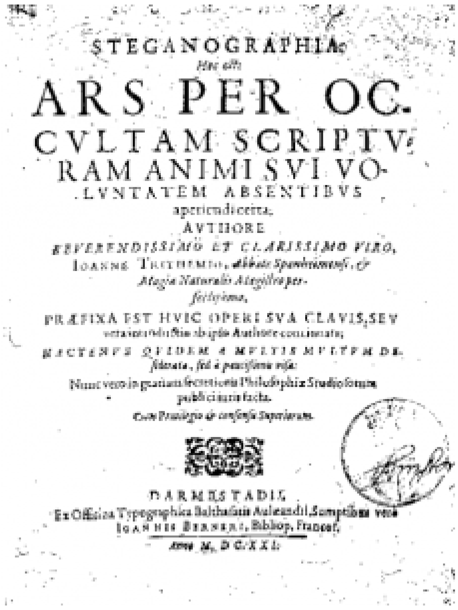
4. Steganografia

Počiatky steganografie siahajú až ku koreňom našej civilizácie. Počas jej vývoja sa používali rôzne metódy ukrývania správ v závislosti od stupňa vývoja civilizácie a jej záznamových techník.

Používali ju už v starovekom Grécku a prvú písomnú zmienku o nej prináša Herodotos. Bežný bol v tom období spôsob písania na drevené platne, ktoré boli pokryté voskom. Doň bola správa vyrytá. Ak však chceli správu ukryť, zotreli z platne vosk a text napísali na drevenú platňu. Potom ju znova prekryli voskom, a tak sa zdalo, že ešte nebola použitá. Podľa Herodota použil tento spôsob Demeratus, keď chcel varovať Sparťanov pred Xerxesovým plánom zničiť Grécko lebo neplatilo dane.

Inou metódou bolo vytetovanie správy na temeno hlavy, z ktorej oholili vlasy. Keď potom vlasy vyrástli, správa bola ukrytá. Príjemca správy posla oholil, a tak si mohol posolstvo prečítať.

Písomnosti o steganografii sa zachovali už zo stredoveku. Na obr. 2 si možno pozrieť titulnú stranu diela Steganografia, ktoré napísal Johannes Trithemius v roku 1500.


STEGANOGRAPHIA: Hoc est:
ARS PER OC-
CVLTAM SCRIPTV-
RAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
IOANNE TRITHEMIO, Abbate Spanheimensi, &
Magiae Naturalis Magistro perfectissimo,
PRAEFIXA EST HVIC OPERI SVA CLAVIS, SEV
vera introductio ab ipso Authore concinnata;
HACTENVS QVIDEM A MVLTIS MVLTVM DE-
siderata, sed à paucissimis visa:
Nunc vero in gratiam secretioris Philosophiae Studiosorum
publici iuris facta.
Cum Privilegio & consensu Superiorum.
DARMSTADII,
Ex Officina Typographica Balthasaris Aulaeandri, Sumptibus vero
IOANNIS BERNERI, Bibliop. Francof.
Anno M. DC. XXI.

Obr. 3. Johannes Trithemius: Steganografia

Neviditeľný atrament je známy už zo staroveku. Využíval sa však dokonca ešte v druhej svetovej vojne. Jeho použitie si môžete bez problémov vyskúšať aj doma. Stačí na to obyčajné mlieko, ktorým napíšete text na biely papier. Text by mal byť napísaný medzi riadkami normálneho textu, aby bol nenápadnejší. Nahriatím papiera nad plameňom mlieko zhnedne a objaví sa stegospráva.

Okrem tohto jednoduchého neviditeľného atramentu existujú ešte mnohé reagujú iba na veľmi špecifické typy chemikálií, čo zabraňuje ich náhodnému zviditeľneniu.

Veľmi významná v oblasti steganografie je tzv. mikrobodka. Vyvinuli ju Nemci počas druhej svetovej vojny. Je to mikrofotografia, ktorá sa podobá svojou veľkosťou štandardnej bodke za vetou, napísanej písacím strojom. Do tejto mikrofotografie však možno uložiť celú stránku textu, napísanú písacím strojom, alebo aj fotografiu.

Mikrobodka bola uložená do štandardnej korešpondencie, ktorá bola úplne nevinná a nahradila v nej jednu z bodiek za vetou. Nie je v ľudských silách skontrolovať každú bodku pod mikroskopom, či neobsahuje mikrofotografiu, a tak tieto stegosprávy unikali pozornosti cenzorov a prechádzali cez hranice k nepriateľským špionážnym službám.

Medzi ďalšie techniky patrí ukrývanie textu pod známku na liste. Správy sa kódovali aj do kreslených obrázkov, kde význam mali typy čiar, ich hrúbka, použitá farba, rôzne prvky obrázka atď. Keďže táto metóda bola všeobecne známa, počas prvej a druhej svetovej vojny existoval zákaz posielania detských kresieb v listoch.

Zaujímavou metódou, ktorá už súvisí s počítačmi, je použitie neproporčného písma. Tu je každé písmeno rovnako široké, a teda sú v správe úhľadne podpísané pod sebou. Ak však chceme umiestniť do takéhoto textu stegosprávu, stačí správne slovíčka v nič nehovoriacom texte posunúť o jediný pixel doprava. Ľudský zrak nie je schopný tento posun zaregistrovať, ale počítač to zistí a vyextrahovaním takto posunutých slovíčok poskladá stegosprávu [8].

5. Mechanické a elektronické šifrovacie stroje

5.1. Jeffersonov valec

Americký minister zahraničných vecí (neskôr prezident) Thomas Jefferson v r. 1790 vynašiel mechanický šifrátor, ktorému sa hovorí Jeffersenov valec.

Pozostáva z 36 rovnakých koliesok, ktoré sú nasunuté na spoločnú os a tak vytvárajú valec. Na obvode jednotlivých koliesok sú napísané všetky písmená abecedy v rozhádzanom poradí. Pri šifrovaní sa jednotlivé kolieska proti sebe otáčajú tak, že nakoniec dávajú vo zvolenom riadku na obvode valca požadovanú správu. Šifrovaný text sa prečíta z riadku nasledujúceho, alebo z iného vybraného z 26 možných. Kolieska boli číslované a mohli byť menené alebo poprehadzované.

V 20. storočí bol intenzívne analyzovaný a bola uznaná vysoká miera bezpečnosti. Ak by sme chceli rozšifrovať text, museli by sme vyskúšať 36! x 26! = 10^{60} možností. Autor bol nazvaný otcom americkej kryptografie [1, 112].

Obr. 4. Jeffersonov valec

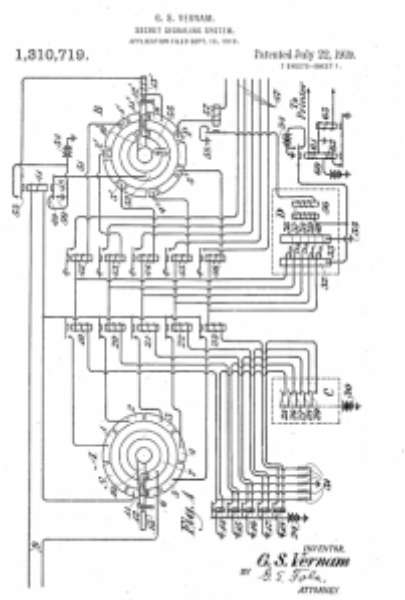
5.2. Playfair

Anglický fyzik Charles Wheatstone v r. 1854 vynašiel tzv. Playfairovú šifru (publikoval ju jeho priateľ Lyon Playfair), ktorou sa šifrovali vždy dve písmená otvoreného textu na dve písmená šifrovaného textu. Bola to vôbec prvá písmenková digrafická šifra (znakovú vynašiel Porta) [5].

5.3. Vernamova šifra

Gilbert S. Vernam, zamestnanec americkej AT&T, vymyslel polyalfabetický šifrovací stroj schopný používať náhodný neopakujúci sa kód. Tento systém je dodnes známy ako jediný teoreticky *bezpečný kryptosystém* [3, 109].

Do stroja sa vkladala dierna páska s otvoreným textom spolu s diernou páskou, na ktorej bol náhodne vydierkovaný kľúč. Šifrogram vznikol sčítaním príslušných bitov obidvoch pások modulo 2. Veľkou výhodou stroja bolo, že proces šifrovania aj dešifrovania prebiehal úplne rovnako. Tento systém ostáva bezpečným, ak náhodný kľúč je rovnako dlhý ako šifrovaná správa a používa sa iba raz (One Time Pad) [1, 188] [8].



Obr. 5. Schéma Vernamovho šifrovacieho stroja

5.4. Nemecká šifra ADFGVX

Pred koncom prvej svetovej vojny začali Nemci používať poľnú šifru ADFGX a jej zosilnenú verziu, systém ADFGVX. Obidva systémy navrhol v roku 1918 nemecký dôstojník Fritz Nebel (1891-1967).

Boli to kombinované šifry, ktoré využívali substitúciu aj transpozíciu. Spojencom sa spočiatku nedarilo do nich preniknúť. Riešenie komplikovala aj denná výmena kľúčov a ich dĺžka (pre obidva kľúče bolo predpísaných aspoň dvadsať znakov).

Rozlúštil ju tesne pred koncom vojny francúzsky kryptoanalytik poručík Georges-Jean Painvin (1886 – 1980). K rozlúšteniu využil znalosť predpokladaného slova v otvorenom texte. Šifra a jej lúštenie sú však výrazne zložitejšie ako u systému ÜBCHI. Prelomenie šifry (3. 6. 1918) významne ovplyvnilo prípravu na nemeckú jún ovú ofenzívu, ktorá smerovala na Paríž. [9]

5.5. Enigma

Američan Edward Hugh Hebern sa zaoberal otázkou, bezpečnosti šifry s malou periódou. Jeho idea inšpirovala konštruktérov v mnohých krajinách. V r. 1923 odkúpil jeho patenty Scherbius a v r. 1924 predstavil na svetovom poštovom kongrese v Štokholme svoj vlastný stroj – Enigma. [9]

Obr. 6. Logo ENIGMA

Nemec Arthur Schrebius získal patent 23.2.1918 v r. 1927 odkúpil patent od Kocha, aby tak poistil svoju exkluzivitu na trhu.

Holanďan Hugo Alexander Koch získal patent 7.10.1919.

Švéd Arvid Gerhard Damn získal patent 10.10.1919. V .r. 1927 jeho firmu odkúpil iný Švéd, Boris Hagelin a vytvoril vo Švajčiarsku vlastný rotorový šifrátor.

Prvá ENIGMA A sa objavila na trhu v r. 1923 a jej hmotnosť bola 50 kg, spolu s integrovaným písacím strojom. Vynález reflexného rotora (pridanie involutórnej permutácie) patrí Willimu Kornovi pracujúcemu pre Scherbiusa. Prvý raz sa objavil v ENIGME C. V tejto verzii sa tiež objavili svietiace lampy namiesto písmen. Potom, v r. 1927 nasledovala ENIGMA D, ktorá sa predávala v rôznych verziách po celej Európe. Napríklad, švajčiarska armáda používala ENIGMU K, talianske námorníctvo ENIGMU D...

Niektoré verzie boli úspešne dešifrované šifrovými službami iných štátov. V r. 1934 nemecké námorníctvo upravilo armádnu ENIGMU pod názvom Funkschlussel M, resp. M3. Zo sady 8 rotorov sa volili 3. Od r. 1942 sa už používal model M4 so štyrmi rotormi. Tá zostala neporaziteľná až do konca 2. svetovej vojny [1, 191].

Obr. 7. Prístroj ENIGMA

6. Éra počítačov

Éra počítačov v kryptológií začína v roku 1970 a trvá dodnes. Éra počítačov je postavená na nových poznatkoch a na historických vynálezoch, ktoré boli vylepšené.

6.1. Lucifer

Horst Feistel v r. 1970 viedol výskumný projekt v IBM Watson Research Lab, ktorý počas šesťdesiatych rokov vyvíjal šifru LUCIFER. Táto šifra neskôr inšpirovala americký štandard DES a ďalšie šifry označované ako šifry *Feistelovského typu*.

6.2. DES

Návrh firmy IBM, založený na šifre Lucifer a upravený (zmenené S-boxy a zredukovaná dĺžka kľúča) americkou bezpečnostnou agentúrou NSA, bol prijatý ako

americký národný štandard U.S. Data Encryption Standard, skrátene DES. Algoritmus si získal celosvetové uplatnenie až do konca 90. rokov.

7. Záver

V práci som sa zaoberal históriou kryptológie od najprimitívnejších „šifier“ (boli to skôr rôzne utajovacie metódy), cez metódy, ktoré boli prelomom v kryptológií až po sofistikované metódy používané počas II. svetovej vojny. Niektoré z nich boli tak silné, že bolo nutné získať samotné šifrovacie zariadenie, aby došlo ich rozlúšteniu.

Dnes je téma kryptológie oveľa aktuálnejšia ako v minulosti, nakoľko rozšírenie počítačov rapídne stúplo, a s ním aj potreba utajovania informácií, či už ide o štátne záležitosti, utajovanie firemných dát, alebo obyčajná komunikácia na internete. Vo všetkých prípadoch je jednoznačne požadovaná bezpečnosť, dôvernosť a utajenie pred treťou stranou.

V súčasnosti je kryptografia a kryptológia úzko spätá s matematikou a nie je možné tieto dva vedné odbory oddeliť.

Som študentom na Katedre aplikovanej informatiky a výpočtovej techniky, kde téma kryptografie má svoje miesto. Konkrétne môžem spomenúť niekoľko mien ľudí z Fakulty elektrotechniky a informatiky, ktorý sa témou kryptografie zaoberajú intenzívne zaoberajú. V prvom rade je to prof. RNDr. Otokar Grošek, PhD. z Katedry aplikovanej informatiky a výpočtovej techniky a taktiež Doc. RNDr. Satko Ladislav CSc. z Katedry matematiky, ktorý sa zaoberá skúmaním moderných metód v tejto oblasti.

8. Odkazy na literatúru

1. O. Grošek, M. Vojvoda, P. Zajac: Klasické šifry. Vydavateľstvo STU Bratislava: STU Bratislava 2007, ISBN 978-80-227-2653-5
2. O. Grošek, M. Vojvoda, M. Zanechal, P. Zajac: Základy kryptografie. Vydavateľstvo STU Bratislava: STU Bratislava, 2006
3. G. S. Vernam: Cipher printing telegraph systems for secrets wire and radio telegraphic communications. Journal of the Americans Institute for Electrical Enginnerings 55, 1926.
4. Kryptografia – http://server.gphmi.sk/pages/sifry/
5. Dôležité medzníky v histórii kryptografie - http://www.fpv.umb.sk/~huraj/historia/historia.html
6. Kryptológia – http://sk.wikipedia.org/wiki/Kryptológia
7. Skytalé – http://en.wikipedia.org/wiki/Scytale
8. Branislav Madoš: Tajomstvá Steganografie - http://www.gljs.sk/~sjiricek/inf/pcrevue/steganografia.pdf
9. Enigma (šifrovací stroj) – http://sk.wikipedia.org/wiki/Enigma_(šifrovací_stroj)
10. Kvantová kryptografia I: Úvod do šifier - http://blackhole.sk/topickvantova-kryptografia-i-uvod-do-sifier
11. Historický vývoj kryptológie – http://friedo.szm.sk/hist1.html

---

Spoluautorkou tohto článku je Tatjana Šimanovská, Oddelenie ekonómie a manažmentu

podnikania ÚM STU, Fakulta elektrotechniky a informatiky v Bratislave