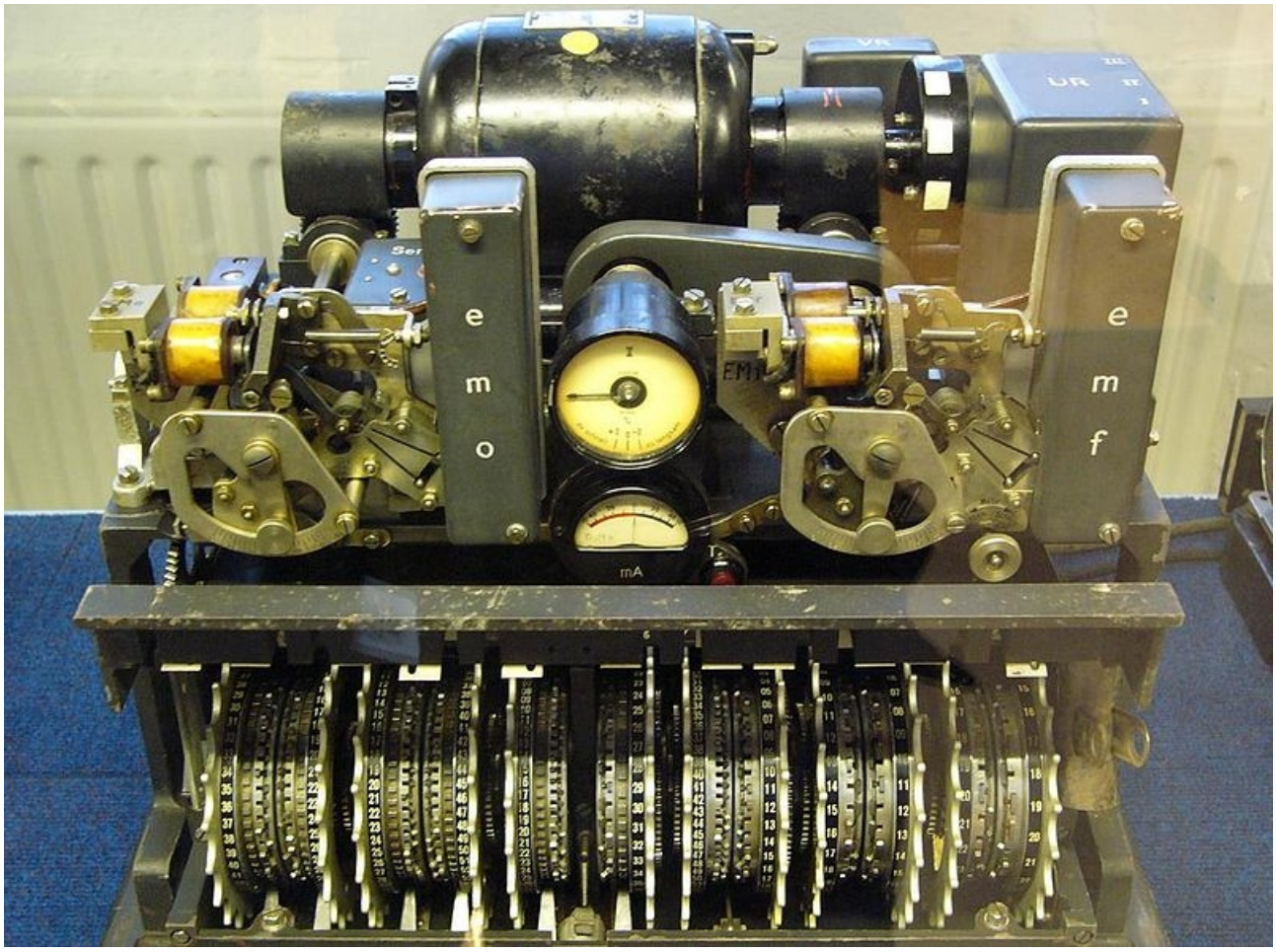
Lorenzova šifra

Rozlúštenie správ Adolfa Hitlera



V tejto práci sa budem snažiť popísať fungovanie šifrovacích strojov Lorenz, ktoré počas 2. svetovej vojny používalo Oberkommando der Wehrmacht, teda Vrchné velenie ozbrojených síl a aj samotný Adolf Hitler. Zameriam sa na princípy použité pri šifrovaní a spôsob, akým bola šifra prelomená bez toho, aby britský kryptoanalytici vlastnili alebo vôbec videli šifrovací prístroj.

Stroj Lorenz SZ

Lorenz SZ40, SZ42A, SZ42B (SZ znamená Schlüsselzusatzgerät – šifrovacie prídavné zariadenie) boli šifrovacie zariadenia, ktoré si pre komunikáciu štábu a hlavného velenia objednala na začiatku 2. svetovej vojny nemecká armáda. Vyrobila ich spoločnosť C. Lorenz A.G. v Berlíne. V súčasnosti sú ďaleko menej známe ako stroje Enigma, ktoré boli častejšie používané, keďže sa jednalo o komerčný stroj.

Lorenz SZ boli klasické ďalekopisné stroje – zariadenia, ktoré sa do 90. rokov 20. storočia používali na prenos textu bežnými telekomunikačnými vedeniami. Ďalekopis je vlastne elektrický písací stroj – má bežnú klávesnicu, na ktorej sa písal odosielaný text. Lorenz SZ boli doplnené o šifrovací systém, ktorý

pozostával z 12 rotorov a používal prúdovú šifru používajúcu logickú operáciu exkluzívnej disjunkcie – XOR (v ďalšom texte ⊕). Pri kódovaní znakov sa používalo 26 znakov bežnej abecedy spolu so znakmi, ktoré zodpovedali 3, 4, 8, 9, + a /. Celkovo bolo teda 32 znakov, každý sa šifroval pomocou 5 impulzov (bitov).

12 rotorov malo generovalo pseudonáhodnú postunosť impulzov „**x**" a „**.**" ako kľúč (key stream), ktorý bol skombinovaný (pomocou operácie ⊕) s nezašifrovaným textom a vytvoril text, ktorý rovnako nastavený stroj skombinoval s tým istým kľúčom a tým dešifroval správu.

5 rotorov sprava, **chí**, menilo 5 impulzov každého znaku, otáčajúc sa o jednu pozíciu pri každom. 5 rotorov zľava, **psí**, menili výsledok **chí** transformácie, ale neotáčali sa s každým znakom. 2 centrálne rotory, **mý**, určovali, či sa **psí** rotory otočia s novým znakom.

Každý rotor mal niekoľko zarážok, ktorých bolo dohromady v stroji 501. Každá mohla byť v dvoch polohách – zatlačená, čo malo za následok „**.**" alebo zdvihnutá, čo malo za následok „**x**". Počty zarážok na jednotlivých rotoroch boli navzájom nesúdeliteľne. V každom šifrovacom kroku je jedna zo zarážok na každom rotore aktívna - ovplyvňuje kľúč. Po otočení rotora je aktívna nasledujúca. Celkový počet možných kombinácií bol teda 2^{501}. V praxi ale bola približne polovica zarážok na každom rotore v zdvihnutej polohe, čo bola jedna zo slabostí, ktorá viedla k prelomeniu šifry.

V každom kroku šifrovania prístroj vygeneroval jeden znak kľúča, ktorý vznikol operáciou XOR použitou na aktuálne nastavenia **psí** a **chí** rotorov. Každý z piatich rotorov pritom odpovedal jednému z piatich impulzov (bitov) znaku kľúča.

Na konci šifrovacieho kroku sa otáčanie rotorov riadilo nasledujúcimi pravidlami:

- **chí** rotory sa otáčajú v každom kroku
- prvý **mý** rotor sa otáča v každom kroku
- druhý **mý** rotor sa otáča iba vtedy, keď je prvý **mý** rotor (pred otočením) nastavený tak, že aktívna zarážka je zdvihnutá
- **psí** rotory sa otáčajú iba vtedy, keď je druhý **mý** rotor (pred otočením) nastavený tak, že aktívna zarážka je zdvihnutá

Poradie zdvihnutých a zatlačených zarážok sa menilo denne na **mý** rotoroch, **psí** rotory sa menili každé 3 mesiace do októbra 1942, odkedy sa menili mesačne. Od 1.8.1044 sa nastavenia **psí** aj **chí** rotorov menili denne.

Počet začiatočných pozícií rotorov bol 43×47×51×53×59×37×61×41×31×29×26×23 (počet zarážok na každom z rotorov) čo je približne $1{,}6\times10^{19}$. Spôsob nastavenia rotorov rotorov pred vysielaním správy sa nazýva indikátor. Počas skúšok prenosov pozostávali indikátory z 12 nemeckých krstných mien, ktorých prvé písmená značili nastavenia rotorov. Od októbra 1942 sa zmenil systém indikátorov. Všetky začínali písmenami QEP a pokračovali dvojmiestnym číslom, ktoré odkazovalo na nastavenie rotorov, ktoré bolo zapísané v knihách, ktoré mali operátori.

Tunny – Tuniak

Briti označovali všetku šifrovanú ďalekopisnú komunikáciu Nemcov ako Ryby, čo vysvetľuje, prečo správy šifrované Lorenzovým strojom získali označenie Tuniak - Tunny

Šifra

Použitú šifru vyvinul v roku 1917 Gilbert Vernam. Jedná sa o symetrickú šifru, teda k šifrovaniu aj dešifrovaniu používa rovnaký kľúč. V prípade Vernamovej šifry je kľúč rovnako dlhý ako otvorený text a naviac je náhodne generovaný.

Ak je $p_1p_2.....p_n$ je otvorený text a $k_1k_2.....k_n$ je náhodne generovaný kľúč, tak šifrovaný text $c_1c_2.....c_n$ je definovaný ako $c_i=p_i+k_i$ mod 32 (v prípade stroja Lorenz)

Claude Shannon dokázal, že Vernamova šifra je absolútne bezpečná.

Každý znak šifrovanej správy bol vysielaný ako 5 impulzov, ktoré boli buď „**x**" alebo „**.**". Z ich kombinácie boli vytvorené všetky použité znaky, ako napríklad **.x.x.** - R. Pri používaní operácie XOR sa „**x**" chápalo ako pravda a „**.**" ako nepravda.

VSTUP		VÝSTUP
A	B	A⊕B
.	**.**	**.**
.	**x**	**x**
x	**.**	**x**
x	**x**	**.**

Pri šifrovaní sa na každý znak správy použila operácia ⊕, kde A je znak správy a B je znak kľúča. Následne sa poslal takto zašifrovaný text.

Platí, že: Otvorený text⊕Kľúč=Šifrovaný text

Šifrovaný text⊕Kľúč=Otvorený text

Šifrovanie každej správy preto záviselo od kľúča, ktorý bol vytvorený nastavením a otáčaním rotorov stroja.

M⊕N=T **..xxx⊕..xx.=....x**

T⊕N=M **....x⊕..xx.=..xxx**

Lúštenie šifry

Prvým krokom k prelomeniu novej šifry je diagnóza logiky procesu šifrovania a dešifrovania. V tomto prípade šlo o pochopenie štruktúry a fungovania prístroja. Bolo to dosiahnuté bez toho, aby mali prístroj k dispozícii, čo sa stalo až v roku 1945, krátko pred víťazstvom spojencov.

John Tiltman, skúsený a nadaný kryptoanalytik z Bletchley Park študoval šifrované texty Tuniaka a identifikoval, že používajú Vernamovu šifru.

Zlomom v britskom snažení o prelomenie šifry bol dátum 30.8.1941, kedy bola vysielaná správa o dĺžke približne 4000 znakov z Atén do Viedne s indikátorom HQIBPEXEZMUG. Avšak, správa nebola prijatá a preto (po tom čo príjemca zaslal nezašifrovanú žiadosť o znovuzaslanie) bola správa poslaná znovu s rovnakým nastavením stroja, čo nebolo dovolené. Správa mala rovnaký indikátor HQIBPEXEZMUG, čo zaujalo britských kryptoanalytikov. Naviac, druhý krát urobil operátor veľa malých zmien – skratok, čo

spravilo druhú správu kratšou. Ak sa pri prenose použije dva krát ten istý kľúč tak pri kombinácií dvoch šifrovaných textov sa kľúč vzájomne „vyruší“. Ak O_a a O_b sú dva otvorené texty, K je kľúč a Z_a a Z_b sú šifrované texty, tak potom platí:

$O_a \oplus K = Z_a$ $O_b \oplus K = Z_b$

z toho plynie, že $Z_a \oplus Z_b = O_a \oplus O_b$

Ak sa príde na obsah otvoreného textu, tak sa dá získať kľúč z hociktorého páru O a Z

$Z_a \oplus O_a = K$ alebo $Z_b \oplus O_b = K$

Pri použití tejto techniky na správu z augusta 1941 :

Z_a JSH5N ZYZY5 GLFRG

Z_b JSH5N ZYMFS /885I

$Z_a \oplus Z_b$ ///// //FOU GFL4M

John Tiltman skúšal rôzne pravdepodobné slová na kombináciu otvorených textov, ktorú získal a zistil, že prvá správa začínala slovom SPRUCHNUMMER – číslo správy, zatiaľčo v druhej už operátor skrátil slovo na SPRUCHENR. To umožnilo Tiltmanovi v priebehu 10 dní správu rozlúštiť a bol schopný získať aj kľúč, ktorý bol použitý pri šifrovaní.

Členovia Výskumnej Sekcie pracovali na matematickom popise procesu generujúceho kľúč, ale neúspešne. V októbri 1941 sa k sekcii pripojil aj mladý matematik William (Bill) Tutt, ktorému zverili túto úlohu. Použil techniku Kasiskiho testu, ktorá spočívala v písaní kľúča na papier s novým riadkom po stanovenom počte znakov, ktoré boli predpokladanou periódou opakovania kľúča. Ak bolo číslo správne, matica znakov by ukazovala viacero opakovaní sekvencií znakov. Tutte vedel, že Tuniakové indikátory používali 25 písmen (bez J) pre 11 rotorov, ale iba 23 pre posledný. Preto vyskúšal Kasiskiho metódu s opakovaním 575. Nepozoroval veľké množstvo opakovaní v stĺpcoch, ale pozoroval opakovanie na diagonálach. Preto opakoval postup aj s 574, čo ukazovalo opakovania v stĺpcoch. Prvočíselné delitele 574 sú 2, 7 a 41, takže skúsil znova s periódou 41 a „dostal obdĺžnik bodiek a krížikov, ktoré boli preplnené opakovaniami“.

Avšak bolo zjavné, že prvý impulz kľúča bol viac komplikovaný ako keby bol vytvorený len jedným rotorom so 41 pozíciami. Tutte nazval tento komponent kľúča **chí**. Zistil, že musí byť aj iný komponent, ktorý bol aplikovaný operáciou ⊕ na **chí** komponent. Ten nemenil každý znak a Tutte ho nazval **psí**. Po Tuttovom prelome sa zbytok výskumnej sekcie pridal k analýze a ustálilo sa, že existuje 5 **psí** rotorov, ktoré sú pod kontrolou dvoch **mý** rotorov.

Diagnostika fungovania Tuniaka týmto spôsobom bol skutočne pozoruhodný kryptoanalytický úspech.

Bill Tutte naviac navrhol techniku hľadania úvodného nastavenia **chí** rotorov, zvanú 1+2 technika. Jej cieľom bolo nájsť pôvodné nastavenie **chí** komponentu kľúča skúšaním všetkých možných kombinácií so šifrovaným textom a hľadaním neuniformného rozdelenia znakov (ako je tomu v otvorenom texte). Podmienkou bolo, aby boli nájdené správne nastavenia zarážok, aby bolo možné skúmať relevantné sekvencie, ktoré mohli byť generované **chí** rotormi. V praxi bolo nemožné generovať 22 miliónov znakov zo všetkých piatich rotorov, takže skúmali iba 41×31=1271 z prvých dvoch. Na urýchlenie tohto procesu boli navrhnuté dešifrovacie stroje.

Dešifrovacie stroje

Heath Robinson

Heat Robinson bol prvý elektrický stroj, ktorý bol použitý pri lámaní šifry stroja Lorentz. Bol navrhnutý Tommym Flowersom a Frankom Morellom v General Post Office research station v Dillis Hill (severozápadný Londýn). Tommy Flowers bol predstavený kryptoanalitikovi Maxovi Newmanovi Alanom Turingom, ktorý obdivoval Flowersove znalosti elektroniky. Max Newman vytvoril funkčné špecifikácie požadovaného stroja, ktorý neskôr úspešne postavili.

Heath Robinson mal dve čítacie vstupy na papierové pásky – jeden na šifrovaný text a druhý na testované nastavenie **chí** rotora. Stroj dosahoval rýchlosť čítania až 1000 znakov za sekundu, avšak napínanie pásky pri takej vysokej rýchlosti spôsobovalo problémy pri zladení dvoch pások. Navyše mal prístroj iba niekoľko desiatok elektónok, čo neposkytovalo dostatočný výkon.

Colossus

Keď boli postavené a funkčné prvé stroje Heath Robinson, Tommy Flowers začal pracovať na plánoch na nový a ďaleko pokročilejší stroj, ktorý by nebol iba rýchlejší, ale aj flexibilnejší. Preto bol Colossus prvý programovateľný počítač, ktorý vznikol ešte pred americkým počítačom ENIAC, ktorý sa považoval za prvý. To bolo z dôvodu, že existencia Colosssusu bola utajená až do roku 1974.

Prototyp bol prvý krát predvedený v decembri 1943 a v Bletchy Park pracoval od 5.2.1944. Kedže obsahoval viac ako 1700 elektónok a ledva sa zmestil do miestnosti, Tommy Flowers ho nazval Colossus – Kolos. Vylepšený Colossus Mark 2, ktorý používal posuvné registre, čím sa rýchlosť čítania zvýšila päťnásobne, začal pracovať od 1.6.1944, iba 5 dní pred Dňom D, vylodením v Normandii. Ku koncu vojny ich pracovalo celkovo 10.

Colossus Mark 1 bol schopný čítať až 5000 znakov za sekundu, čo značne urýchlilo hľadanie nastavenia **chí** rotorov, ale bol k tomu potrebný komplikovaný systém podporných kolies, ktoré regulovali napätie čítacej pásky, aby nedošlo k jej roztrhnutiu. Vylepšený Colossus Mark 2 zvládal 25000 znakov za sekundu.

Colossus bol prvý programovateľný počítač, avšak podľa moderných štandardov bol dosť limitovaný, kedže nemal vnútornú pamäť s programom. Na nastavenie novej úlohy musel operátor zmeniť zapojenie.

Po vojne boli Colossusy na príkaz Winstona Churchilla rozobraté.

Záver

Táto práca má za úlohu informovať o existencii šifrovacích strojov Lorenz, ale hlavne o prelomení šifry, čo bolo označené ako „...jeden z najväčších intelektuálnych počinov 2. svetovej vojny.“, ako to pomenoval Tony Sale, a o pohnútkach, ktoré viedli k vývinu prvého programovateľného počítača vôbec.

Viliam Valent

Zdroje

The Lorenz Cipher and how Bletchley Park broke it by Tony Sale - http://www.codesandciphers.org.uk/lorenz/fish.htm

General report on Tunny by Good, J., Michie, D., Timms, G. A. - http://www.alanturing.net/turing_archive/archive/index/tunnyreportindex.html

Luštění německého šifrovacího stroje Lorenz by Petr Veselý

Cryptomuseum - http://www.cryptomuseum.com/crypto/lorenz/sz40/

The Rutherford Journal - http://www.rutherfordjournal.org/article030109.html

Root.cz - http://www.root.cz/clanky/usvit-hackeru-lorenzova-sifra-tunak-a-kolos/

Ukázky aplikací matematiky NMAG166 – prezentace 1 - http://www.karlin.mff.cuni.cz/~tuma/aplikace14.htm

Wikipedia - http://en.wikipedia.org/wiki/Lorenz_cipher

http://en.wikipedia.org/wiki/Cryptanalysis_of_the_Lorenz_cipher

http://en.wikipedia.org/wiki/Colossus_computer

http://en.wikipedia.org/wiki/Heath_Robinson_(codebreaking_machine)

http://en.wikipedia.org/wiki/Kasiski_examination

http://en.wikipedia.org/wiki/Tony_Sale

http://sk.wikipedia.org/wiki/%C4%8Ealekopisn%C3%BD_stroj