Petr Vokáč

PÍSMENA, KTERÁ MĚNILA SVĚT

Slovo Enigma pochází z řečtiny a znamená záhadu. Z toho, co produkovala, nebyl skutečně nikdo moudrý. Enigma je název nejslavnějšího šifrovacího stroje z II. světové války. Bestseller spisovatele Roberta Harisse o tajemném přístroj „Enigma" přišel do kin a zavedl nás do světa války, špionáže, matematiky a milostných citů.

Dva lidé jsou k sobě připoutáni válkou. Tom Jericho, geniální matematik z Cambridge, který se nevyznačuje právě nervovou stabilitou, a Hesper, trošku kulatější slečna s tlustými skly v brýlích, ale s pevným rozhodnutím něco ze sebe udělat. A to za nejtajnějšími zdmi v Anglii v Bletchley Parku, ve „Station X", kde se tisíce mozků snažily dešifrovat radiodepeše německého wehrmachtu, kde se vedla válka na intelektuální úrovni.

TRILIONY KOMBINACÍ

Ve Station X bojuje Jericho se šifrovacím strojem, který produkuje 150 trilionů, tedy 150 milionů milionů milionů kombinací. Správné seřazení písmen z radiogramů odvysílaných německými ponorkami znamenalo v Atlantiku záchranu tisíců životů, tisíců zachráněných vojáků, zdravotních sester a dětí, kteří se v konvojích plavili mezi Anglií a Amerikou. Znamenalo to záchranu vojenského materiálu, od tisíců tun pohonných hmot, tisíců tanků a tisíců tun potravin, na které čekali obyvatelé Anglie, od Londýna po Glasgow.

„Zlámání" kódu Enigmy znamenalo najít místo v Atlantiku, kde na spojenecké konvoje čekaly německé ponorky. Film ukazuje boj s časem, kde každá vteřina znamenala záchranu tisíce lidských životů. Boj geniálního matematika s mocí šifrovacího stroje, o kterém se Němci domnívají, že jeho kód je nerozluštitelný.

Jericho nebojuje jen s triliony kombinací. Jericho bojuje s milostnými city, protože jej opustila Claire. Film, to je válečná story a detektivka zároveň, je to politicko – milostný thriller. Je to pohled na válku přes písmena a matematické kombinace. Bez dvou minut, dvě hodiny hrůzy zabalené do hledání kódů a štěstí. Jsou to dvě hodiny boje lidského ducha s ocelí.

Dost fantazie, vstupme do reálného světa, ve kterém kralovala Enigma.

Historie kódování

Enigma je vynálezem 20. století. Avšak idea kódovat zprávy je daleko starší, o celé 4 tisíciletí. Alespoň některé kódovací pokusy od starého Egypta až do II. světové války.

Rok 1900 př. n. l. je s největší pravděpodobností rokem prvního zakódování textu. Text byl egyptské provenience, byly to hieroglyfy. Zakódované se od standardních lišily pozměněním obrázku.

Rok 487 př. n. l. – Řekové aplikovali jako kódovací instrument „Skytalu", v podstatě hůlku s pevným poloměrem. V případě, že na ni byl navinut pásek z kůže, na kterém byl napsán zakódovaný text, „poskládala" se jednotlivá písmena tak, že vznikl souvisle čitelný text. Důležité bylo, aby odesilatel i příjemce měli hůlky o stejném poloměru, aby se písmena „správně" poskládala.

Asi kolem roku 60. př. n. l.– César zvolil jednoduchý, ale na tehdejší dobu úspěšný kódovací postup. Jednoduše posunul jednotlivá písmena o několik míst a ž A bylo D, z D bylo G a potom se Julius César, aplikováno na německou abecedu psal MXOLXV FHVDU.

V letech 500 – 1400 n. l. – To je čas kryptogramů v Evropě. Mnoho kryptografických vědomostí se ztratilo, na mnoho se zapomnělo. Byla to doba, kdy kryptografie byla postavena na roveň černé magie a přirovnávala se k učení pekla. Jinak tomu bylo v Persii. Tam přicházeli oblíbenosti kódování na chuť. První kniha o kryptogramech vyšla v arabském prostoru v roce 1375.

Rok 1379 – Antipapež Klement VII. pověřil Gabriela di Lovinde vymyslet kódovací systém. Systém, i když poměrně jednoduchý, vydržel celých 450 let. Vatikán měl údajně už v 16. století oddělení lamačů kódů.

Rok 518 – V německy mluvícím prostoru se objevuje první tištěna kniha o kryptologii. Autor Johannes Trithemius.

Rok 1790 – Thomas Jefferson vyvinul první šifrovací válec. Tak vznikl první šifrovací stroj. Upadl v zapomenutí a byl později mnohokráte znovu vynalezen. Jedním z vynálezců byl Angličan Charles Babbaget nebo roku 1891 Francouz Etienne Bezeries.

Rok 1918 – Inženýr Artur Scherbius nabízí německé „marině" ké koupi Enigmu. Je odmítnut.

Šifra, otázka života a smrti

Tajné zprávy a dekódování, to je historie mnohdy života a smrti. Skotská královna Marie Stuartovna byla popravena po tom, co se prokázalo, že se zúčastnila na spřádání příprav vraždy Alžběty I. Důkazy byly nalezeny v dekódování jejích dopisů.

Kódování souviselo obvykle s válkou nebo přípravou na válku. Odhalený kód byl například zodpovědný za to, že Amerika vstoupila do I. světové války. Jak se to stalo? Vedoucí na německém ministerstvu zahraničních věcí Arthur Zimmermann poslal v lednu 1917 telegram na německé velvyslanectví do USA, ve kterém sděloval, že by bylo, v případě že USA nezůstanou neutrální, potřebné dostat Mexiko a Japonsko na německou stranu. A netrvalo dlouho a USA vyhlásily Německu válku.

Max Klausen byl radiotelegrafista špiona Sorgeho v Japonsku a poslal Stalinovi dekódovanou zprávu, že Japonsko nenapadne Sovětský svaz. Stalin tak mohl s klidem nasadit celou sovětskou armádu proti Německu. Klausen byl v Japonsku zatčen, ale ani po třech letech, tedy do konce II. světové války nebyl kód rozluštěn. Klausen zemřel jako hrdina v NDR v roce 1979.

Druhá světová válka, to byla válka kódování, šifer a lamačů kódů.

Jak pracovala Enigma?

Bylo to v podstatě velice jednoduché šifrování. Základem byla abeceda, německá abeceda, skládající se z 26 písmen:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

A princip? Místo A se psalo B a podobně jako to dělal César. Pak zašifrované slovo Enigma se napsalo FOJHNB. Žádný problém k rozluštění. A navíc to mělo jednu nevýhodu. Příkladně slovo Anna by pak bylo zakódováno jak BOOB. Němci jsou důslední. Pro šifrování bylo nutno celý postup trošku zkomplikovat. Vymyslel se klíč – bloky pro jednotlivá písmena.

Klíč pro :

První písmeno: BCDEFGHIJKLMNOPQRSTUVWXYZA
Druhé písmeno: CDEFGHIJKLMNOPQRSTUVWXYZAB
Třetí písmeno: DEFGHIJKLMNOPQRSTUVWXYZ ABC
Čtvrté písmeno: EFGHIJKLMNOPQRSTUVWXYZABCD
Páté písmeno: FGHIJKLMNOPQRSTUVWXYZABCDE
Šesté písmeno: GHIJKLMNOPQRSTUVWXYZ ABCDEF

a tak se postupovalo pro 26 písmen, pro takový počet, jaký má německá abeceda. Pak se celý postup opakoval.

A podle výše uvedeného bylo slovo Enigma zašifrováno písmeny FPLKRG. Jak toho bylo dosaženo? Prvním písmen následujícím v bloku pro první písmeno, které se má zašifrovat, je písmeno F. Druhým písmenem v bloku pro druhé písmeno je P. Druhým písmenem po N je písmeno P. Třetím písmenem v třetím bloku po I, je L. A tak se pokračuje pro další písmena slova. A když napíšeme znovu slovo Anna, tak zašifrováním vznikne BPQE.

To byla „práce" jen pro jeden válec Enigmy, a i ta nejjednodušší měla 3 válce.

A ještě navíc se po 26 otáčkách prvního válce druhý válec posunul o jedno písmeno a po dalších 26 otáčkách druhého válce se o jedno písmeno posunul třetí válec.

Mimo to bylo na konci u Enigmy používané v námořnictvu odrážecí zrcadlo, které provedlo další sérii šifrování a zašifrované písmeno prošlo předchozími 3 válci, a bylo opět zašifrováno jako v předchozích případech.

K dalším komplikacím vedlo to, že písmena na válcích byla sice napsána v abecedním pořádku, ale jejich elektrické propojení mohlo být příkladně blok pro první písmeno:

MNUXASTDEVWFHYZIJKGLOPBCQR

a pak by prvním zakódovaným písmenem našeho slova Enigma bylo písmeno V.

Řeknete si, dokonalost sama. Nikoliv.

Školácká chyba

Dešifrování stejné jako u Rubikovy kostky. Stačilo znát, které „úrovně" byly nastaveny, a dostat se do výchozí stavu. A to bylo právě 150 trilionů kombinací.

Enigma měla písmena na jednotlivých válcích seřazena podle abecedy a písmeno, které se mělo zašifrovat se nikdy neobjevilo jako zašifrované. Čili po stisknutí A na klávesnici Enigmy nemohlo být zašifrovaným písmenem A. A tak to bylo se všemi písmeny. B se nikdy nemohlo zašifrovat jako B.

Resumé lamačů kódů. Byly to školácké chyby. Nebo naopak. Nebyla to přílišná důvěra v německý vynález? V případě, že by na válci byla písmena psána mimo abecední pořádek, měli by dešifrátoři mnohem více práce.

Pro ovládání Enigmy nebylo třeba žádného dlouhého zaučování. Bylo to v podstatě psaní na psacím stroji a nastavení válců.

Dekódovat Enigmu pomohly dvě skutečnosti.

Hlášení o počasí se mezi ponorkami v Atlantiku a německým velením předávaly rádiem. Stávalo se, že totéž hlášení bylo jednou v otevřeném, a jednou v šifrovaném textu. To byla velká pomoc pro dešifrátory. Měli vlastně text šifrovaný i otevřený. Důvěra v Enigmu musila být velká, když si to mohli dovolit.

Tím se zjišťoval klíč šifrování. Byla to však jen malá pomoc, protože nastavení válců se měnilo velmi často.

Jako u hieroglyfů

Lamačům kódu nechtěně pomohli sami němečtí vojáci, kteří obsluhovali Enigmu. Jak k tomu došlo? Jeden německý radiotelegrafista, byla mu zřejmě dlouhá chvíle, stále ťukal na jedno písmeno Enigmy. Enigma stále šifrovala jedno písmeno a postupně se měnily válce. Když někdo vyťukával stále stejné písmeno, vznikne řetězec různých písmen, a to všech kromě toho, které se vyťukává. Nic nového. To byl přece princip Enigmy.

Nezapomeňme, že předtím, než byla Enigma použita u wehrmachtu, byl její princip znám a nabízela se jako každý jiný obchodní artikl. Tento detail, že ve vysílání chybí kompletně jedno písmeno, objevila pracovnice z Bletchley Parku. A to expertům pomohlo poznat nastavení válců na jeden den. Každý krůček je dobrý.

Místo Německa Hirošima

Nemůže být pravdou, že údajně měli dekódování napomoci radiotelegrafisté sami, tím, že neměnili nastavení válců po několik dní. Na kódování byly knihy a kódování bylo nutno termínově dodržovat. Pravděpodobnější je následující story, podobná jako při rozluštění hieroglyfů.

V Bletchley Parku pracovali kryptologové, jejichž mateřštinou byla němčina. A ti přišli s nápadem, že se musí v zašifrovaném textu objevit slovo „Vaterland – vlast." Začali po něm pátrat, a podle něho hledali nastavení rotorů a nacházeli řešení.

Zdá se vám, že je to nesmysl? Začalo se stavět na velice vratké hypotéze? Zdaleka ne.

V Bletchley Parku nebyli tímto nápadem ani originální. Už 120 let před nimi stejným způsobem začal luštit hieroglyfy jistý Champollion. Také si řekl, že jeden z těch hieroglyfů musí znamenat královna, a vyluštil hieroglyfy. Rozdíl tady byl. V Bletchley Parku začali luštit kódy, to bylo mnohem horší než luštit hieroglyfy.

Jak velkou roli v historii lidstva hrála šifra, šifrované zprávy a lamači kódů, a důsledky jejich vyluštění nám nejlépe přibližuje historie Enigmy. Je to jen historie části psacího stroje a systematické záměny 26 písmen, napsaných na třech nebo čtyřech vál-

cích. Historie změti drátů a uspořádaných elektrických obvodů a důmyslu lidského ducha.

Enigma měnila chod dějin na planetě Země. Domysleme story Enigmy v historických souvislostech II. světové války. Vztáhněme historie Enigmy na použití atomové bomby. Její shození nebylo původně plánováno na Hirošimu a Nagasaki, ale na Německo. V důsledku „dřívějšího" konce druhé světové války v Evropě, a to i díky lidem z Bletchley Parku bylo shození atomové bomby předisponováno na Japonsko.

I přes všechny rafinovanosti, které Němci pro nerozluštitelnost Enigmy vymysleli, drželi s nimi v Bletchley Parku krok, a byli schopni číst radiodepeše jako ti, kterým byly určeny. A domysleme to do konce. Kdo zabránil tomu, že nad Německem neexplodovala atomová bomba? Nedokonalost Enigmy nebo dešifrovací schopnosti personálu v Bletchley Parku?

První kroky Enigmy

Vynález a použití šifrovacího stroje Enigmy sahá do let I. světové války, kdy americký stavební podnikatel Edward Hugh Hebern vynalezl zařízení zaměňující písmena prostřednictvím válců. Nabízel svůj vynález – ovšem marně – armádě, a to už v roce 1918.

V témže roce oznámil německý inženýr Arthur Scherbius „rotující princip" záměny písmen a předvedl v Berlíně šifrovací stroj, který nazval Enigma. Předváděl jej také v roce 1923 v Bernu a o rok později na světovém poštovním kongresu ve Stockholmu.

V roce 1919 patentoval Holanďan Hugo Alexander Koch vynález, který nazval „Tajný psací stroj." Koch jej chtěl komerčně zpeněžit. V dalších letech dokonce budoucí Enigmu vylepšil.

I přes intenzivně vedenou reklamu a podporu vídeňského institutu pro kriminologii a jeho doporučení se obchodní úspěch nedostavil.

V roce 1923 Artur Scherbius zakládá firmu „Šifrovací stroje A. G." Pokouší se dostat stroj do světa. Marně. Úspěch se nekonal. K obratu dochází teprve za 3 roky.

V roce 1926 projevilo zájem německé námořnictvo. Předtím si však stroj dokonale vyzkoušelo a hned nato koupilo větší počet strojů. Pak se připojila Říšská bezpečnostní služba, Abwehr, Říšské dráhy a vlivné úřady. Z toho vyplynulo, že každý „úřad" vydal vlastní pokyny pro užívání Enigmy. Nabízela vysokou spolehlivost a vylučovala možnost „zlámání kódu." To Enigmu předurčilo pro použití u všech druhů vojsk. Nákupy šifrovacích strojů se staly přímo masovými. Odhaduje se, že jich bylo vyrobeno téměř 200 tisíc kusů.

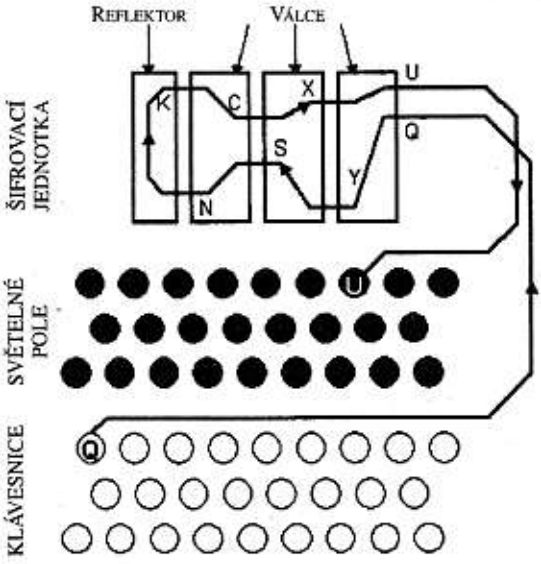


SCHÉMA ENIGMY

Repro: arnut

VÝVOJ

Enigma prošla několika vývojovými stadii, ale základ zůstával stejný. Vážila o něco více než běžný psací stroj, asi kolem 20 kilogramů. Měla okna pro nastavení válců, a klapky s jednotlivými písmeny byly nastaveny jako na psacím stroji. Nad nimi bylo pole žárovek. Na něm bylo možno kontrolovat zakódovaná písmena. Kontrolovat, zda napsané písmeno a rozsvícené písmeno se shodují. Enigma byl stroj, který kódoval elektro – mechanicky.

Na počátku své éry Enigma nebyla tajná.

V roce 1927 Scherbius koupil patent od Holanďana Hugo Alexandra Kocha, který měl od roku 1919 patentován rotační princip

záměny písmen. Po smrti Scherbiuse v roce 1929 se o uvedení Enigmy do života se střídavými obchodními úspěchy staral Willy Korn.

První pokusy v Polsku

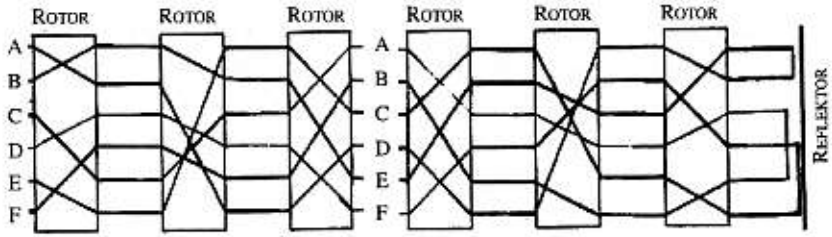
V Anglii sice fungovala instituce, která se zajímala o šifrovací zprávy, ale z pohledu kódovacích předloh, tedy tabulek a písemného materiálu, nikoliv strojů. A již tehdy bylo sídlo organizace v Bletchley Parku. Nedocilovalo žádných velkých úspěchů, a snad to ani nebylo možné. Permanentně se potýkala s nedostatkem peněz. A ještě navíc tato organizace patřila námořnictvu, které nechtělo zaměstnávat civilisty, a u námořníků nebylo dost specialistů.

Na šifrování se zde sešli experti, kteří se rekrutovali z matematiků, filozofů, luštitelů křížovek, ale i herců Někteří z nich pracovali už v „Room 40", to byl krycí název kryptografického oddělení za I. světové války v Anglii.

Když v Anglii byla doceněna role Enigmy, bylo skoro pozdě. Jednoduše řečeno v Anglii byli schopni odposlouchávat zašifrované zprávy, ale nebyli schopni je dekódovat.

Mnohem dál byli Poláci. Už v roce 1938 se šéf Bletchley Parku Dillwyn Knox zúčastnil konference o šifrách v Polsku. Mnoho se toho nedozvěděl, a z toho usoudil, že Poláci jsou také na začátku. V červnu 1939, prakticky před vypuknutím II. světové války, dostali Angličané polskou dokumentaci a zkušenosti a vzali Enigmu útokem.

Už mezi dvěma světovými válkami byla polskými matematiky v čele s Marianem Rejewskim dekódována tříválcová Enigma. Bylo to umožněno několika okolnostmi. Konkrétně špionáží a nepořádkem. Z Německa se podařilo „získat" několik válců , které byly určeny ke zničení. Na druhé straně to byla „lenost" Němců, kteří pro různé zprávy používali stejné kódy. Němci měnili nastavení válců jen jednou denně, někdy dokonce za více dní a to umožnilo shromáždit obrovské množství podkladů pro jedno nastavení válců. Polákům se podařili text zašifrovaný Enigmou dešifrovat.



PŘÍKLAD PROPOJENÍ VÁLCŮ ENIGMY, VPRAVO PŘÍSTROJ S REFLEKTOREM Repro: araut

Zanedlouho se konstrukce Enigmy znovu změnila. Bylo to v době, kdy už bylo jasné, že Polsko bude v příští válce prvním napadeným. Rejewski a jeho spolupracovníci, vlastně polská vláda se rozhodli předat veškeré zkušenosti a podklady britské vládě. To se stalo 25. července 1939.

ALAN TURING

Neutěšená situace se s nástupem války v Anglii změnila. Anglická vláda vybudovala pár desítek kilometrů od Londýna v Bletchley Parku centrum pro kryptologii. Pracovali zde nadaní matematikové, lingvisté, lidé s kombinačními schopnostmi, včetně šachistů. Jeden z matematiků byl i Alan Turing, který pokračoval v práci svých polských předchůdců.

Turing přišel do anglického týmu v Bletchley Parku podle některých pramenů v roce 1935, podle jiných v roce 1940, to mu bylo necelých 30 let. Měl za sebou skončené studium Kings College, zakončenou ve 23 letech a titul doktora přírodních věd.

Intenzivně se věnoval matematické logice a elektrickým počítačům. Byl to on, kdo začal uplatňovat teoretickou matematiku při dekódování. Spolu s Gordonem Welchmanem zkonstruoval „bombu". To nebyla bomba ve vlastním slova smyslu, ale pojmenování počítacího stroje na dekódování zpráv zašifrovaných Enigmou. Byl to primitivní computer.

Vlastně od tohoto času by se měl datovat vynález computeru. Škoda jen, že Turing nedostával od začátku všechno, co pro stavbu bomby potřeboval. Nebyly to jen technické díly, ale i třeba papír.

Poukazovalo se totiž na to, že materiál je třeba pro válku a ne na hraní pro pár extravagantních matematiků, kteří chodí v ošuntělých šatech a mají nepochopitelné chování. Pak se Turing rozhodl a napsal dopis ministerskému předsedovi Churchillovi. I při velké shovívavosti nelze dopis zařadit do kategorie slušných, natož pak zdvořilých. Účinek byl okamžitý. Materiální zabezpečení, na které dohlédl sám ministerský předseda pro Bletchley Park, fungovalo do konce války bez jediného problému.

Netrvalo dlouho a fungoval první prototyp bomby. Za pár měsíců už jich v Bletchley Parku stálo několik. Všechno se dělo tajně, a proto o stavbě bomby jsou jen sporadické podklady, a sem tam se objeví nějaký účet. Bomby byly prakticky velké skříně, dlouhé 5 a vysoké 2 metry a umísťovaly se do velkých hal. Dohled nad bombami měly ženy, které neměly ani tušení, nač stroje jsou a měnily jen v bombách podle pokynů kryptologů válce.

Alan Turing byl, jak někteří říkali, zvláštní člověk. Jezdil do Bletschley Parku na kole a s plynovou maskou na obličeji, která ho chránila proti senné rýmě. Je překvapivé, že ve filmu zmíněném v úvodu článku o něm není ani zmínka, stejně jako o práci, kterou vykonali Poláci a přenechali Britům.

Skutečnost, že Turing se ve filmu neobjevuje, může být spojena s jiným důvodem. Po válce byl stíhán pro homosexualitu a v roce 1954 spáchal sebevraždu otráveným jablkem.

Velmi brzy po válce napsal o dekódování Enigmy knihu. Její rukopis byl do roku 1996! považován za tajný a byl vydán anglickou vládou až po tomto roce.

Nelogické? Naopak. Jak pochopíme později, bylo to velmi logické a dokonce nutné.

U 110

Co se dělo v Atlantiku na počátku II. světové války, se v Německu dozvěděli teprve dlouho po válce. I Britové nechtěli, ani neoficiálně, přiznat, že byl zastřelen velitel ponorky, kterou posádka opustila v domnění, že se potápí. Ponorka se nepotápěla, a kapitán ji chtěl donutit k potopení. Nechtěl potopit ponorku,

chtěl jen zabránit tomu, aby se Angličané nedostali k Enigmě. První zásadou radiotelegrafisty po napadení bylo ponořit veškeré instrukce a šifry do vody a zajistit, aby se ponorka potopila současně s Enigmou a se nedostala se do rukou nepřítele.

„Inkoust", kterým byly instrukce psány, byl ve vodě rozpustitelný. U ponorky U110, kterou poslal ke dnu britský křižník Bulldog, to vypadalo z počátku tak, že ponorka se potopí, a kapitán dal posádce rozkaz vyjít na anglickou loď, tedy do zajetí. Ponorka se neponořovala. Kapitán jí chtěl „pomoci".

Bylo už pozdě. V ponorce už „úřadovala" britská Secret Service. Díky tomu se Britové dostali k fungující Enigmě a dokonce na další dva měsíce k platným šifrovacím knihám. A to umožnilo Britům číst rozkazy německé mariny a potopit šest z osmi zásobovacích lodí bitevní lodě Bismark. O tom nemělo německé velení ani ponětí.

Kdo zavedl ponorkovou válku?

Velkoadmirál Dönitz byl po sebevraždě Hitlera 30. dubna 1945 krátce říšským prezidentem. Narodil se v roce 1891 nedaleko Berlína. V I. světové válce byl námořním důstojníkem a později velitelem ponorky. Není proto divu, že podporoval nasazení ponorek proti spojeneckým konvojům. Pomocí Enigmy byly akce ponorek koordinovány a rozpracována taktika napadání ve skupinách. První dva roky II. světové války slavily ponorky wehrmachtu v Atlantiku velké úspěchy.

Sám Hitler jmenoval Dönitze svým nástupcem. Dne 1. května 1945 sestavil Dönitz úřednickou vládu, se sídlem na severu Německa, ve Flensburgu. Aby se co nejvíce vojáků a utečenců z východní oblasti dostalo na západ, do zóny vlivu Američanů, oddaloval kapitulaci. Dne 7. května podepsalo velení wehrmachtu na Dönitzův rozkaz kapitulaci ve francouzském městě Remeši a 8. května v Berlíně v Karlshorstu.

Za 14 dní poté byl Dönitz spojenci zatčen a postaven před norimberský tribunál. Byl odsouzen k 10 letům, které strávil v berlínské věznici Spandau. Po svém propuštění v roce 1956 žil v ústraní

v Hamburku. Zemřel 24. prosince, na Ježíška, v Aumühle, nedaleko Hamburku.

Enigma vydává tajemství

Na začátku února 1942 už kódovací tabulky z ponorky U 110 neplatily. A navíc Enigma dostala ke svým třem základním kotoučům další, čtvrtý kotouč. V dekódovací řeči to znamenalo 26násobné zvětšení původních kombinačních možností.

To se okamžitě projevilo v počtu potopených lodí. Jestliže před zavedením kódu potápěli Němci 48 plavidel, pak v únoru 1942 to bylo už 73 lodí, v březnu 95 a v květnu téměř 130 spojeneckých plavidel.

Tunigův tým pracoval na plné obrátky. Do zlámání kódu byly nasazeny další bomby. Výsledek. Enigma vydala za pár měsíců Britům svoje tajemství. V Bletchley Parku se začaly číst tajné německé depeše. Britové a Američané věděli o každé v Atlantiku číhající ponorce a konvoje nechali doprovázet bojovými loděmi, vybavenými vrhači podmořských pum. Nad Atlantikem se objevila letadla s radary, které upřesňovaly polohu ponorek. Z hledajících se stali hledaní, lépe snad honění po celém Atlantiku. Německé vedení si bylo jisto, že příčinu neúspěchu ponorek nemá na svědomí Enigma, ale špion, který se vloudil do vedení wehrmachtu. Tak mnoho věřili geniálnímu systému šifrovací Enigmy. Hledali do konce války špiona ve vlastních řadách. Ponorková válka, válka „šedých vlků," jak Němci říkali ponorkám v Atlantiku, skončila.

Trochu nostalgie

Málo se ví, že Enigma byla v provozu také ve Švýcarsku. Švýcaři dokonce vyvinuli vlastní šifrovací stroj, který však měl za základ Enigmu.

Začátkem května 1994 se na celé okolí hlavního města Bernu snesl déšť. Češi by řekli, že to bylo počasí, do kterého by ani psa nevyhnal. V bernských Alpách byli však lidé, kterým déšť nevadil a spěchali do švýcarského výletního města Meiringen. Nepřišli tam jen ti z okolí, ale přijížděli i z Německa. Ne, žádná turistika to nebyla. Před třemi týdny uveřejnil vojenský departement

anonci s velkým nadpisem „Výprodej vojenského materiálu". Takových výprodejů bylo už ve Švýcarsku mnoho. Prodej nebyl nijak slavný, mnoho se toho neprodalo. Buď sběratelé už všechno měli, anebo o nabízené neměli zájem.

Překvapení přišlo na konci

V inzerátu stálo černé na bílém, že se nabízí k prodeji šifrovací stroj Enigma anebo šifrovací stroj s názvem Nema, to byl obchodní název švýcarského provedení Enigmy. Absolutně neuvěřitelné. Akce, která nemá obdoby. Tak se vyjadřovali i otrlí sběratelé, specialisté. Nikde na světě se dosud něco podobného neuskutečnilo. Kdo o prodeji věděl, koupil Enigmu za 150 švýcarských franků. Porovnáme-li to se skutečnými cenami Enigmy, pak to bylo doslova za spropitné.

Koupit Enigmu znamenalo přivézt si domů kus historie. Jednomu zájemci se prodávala jedna Enigma. Do bernských Alp přijížděli proto sběratelé s plným autem přátel.

V čem je fascinace ne právě levného hobby? Fascinující už je to tajemné, že člověk něco napíše, co mohou přečíst jen ti, kterým je to určeno. A navíc napíšete písmeno a vidíte, jak se písmeno začíná měnit, co se s ním děje. Stroje se můžete dotknout. Pozdější elektronické stroje všechno ztratily. U nich se už nic nevidí, na nic si nesáhnete, jen na vás mrkají barevná světla. Dnes se šifrování omezilo na software, a to tajemné dráždění je zcela pryč.

Kdo jsou sběratelé?

Průměrný sběratel v německy mluvících zemích je v penzi a měl něco společného s šifrováním ve vojsku, tajných službách nebo v diplomatické službě. Standardní německá Enigma se třemi rotory se cení asi na 40 tisíc dolarů, čtyřválcová námořní, která se ke koupi objevuje jenom zřídka na více než 50 tisíc dolarů. Švýcarskou Nemu lze koupit za 3 tisíce dolarů. Pak není divu, že ve švýcarském Meinigen bylo tolik zájemců.

Co s Enigmou sběratelé dělají? Odpověď je přímo překvapující. Píší si dopisy. Ovšem takový dopis není vůbec levný. Ty stroje

mají za sebou více než 50 let a začínají se u nich projevovat nemoci. Jedno takové léčení, třeba jenom malé žárovky stojí 20 švýcarských franků. O větších opravách ani nemluvě. Přesto mezi zájemci jsou skalní, kteří mají doma jednu švýcarskou Enigmu, jednu německou Enigmu a ve sbírce nesmí chybět jeden stroj švédsko-švýcarské firmy Haglin. To byla vedoucí firma na poli krypto grafických strojů.

Tito sběratelé mají k šifrovacím strojům zvláštní vztah. Někdy je koupě Enigmy i nad jejich možnosti. Když ji sám nemůže koupit, tak se postará alespoň o to , aby se Enigma „neztratila". Jeden sběratel, který nechtěl prozradit svoje jméno zprostředkoval koupi ručního šifrovacího stroje pro německé muzeum, a budete se divit od koho, od Vatikánu.

A jak takový zašifrovaný dopis vypadá? To si zkusit sami. Stačí když si na Internetu najdete http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/

Už jsem pro vás zašifrovaný text připravil.

Co potřebuje vědět, je nastavení reflektoru a válců. Jinak by to pro vás představovalo těch 150 miliard kombinací. Popis je anglický, a proto se budu držet originálního popisu.

Rotor/Reflektor:	3,	7,	6
	Rotor I:	Rotor II:	Rotor III:
Rotor Type:	3	4	5
Initial Position:	3	8	9

A ted'text: JHRYX NCNKR NVGAJ LPGFE YNZEY ARNGG SOVXA VREQL LMJNS KXRPA JJO

Text napište myší „Displey" jako na psacím stroji. Jen jedna poznámka. Šifruje se jen 20 písmen a pak se Enigma „resetuje" a začíná opět od začátku.

U-571

Záhady kolem Enigmy lákaly filmaře už dříve. Americký superakční film „Ponorka U-571" líčí přepadení německé ponorky americkou ponorkou, která se vydává za německou záso-

bovací ponorku. Američanům ve filmu jde především o získání šifrovacího stroje Enigma a šifrovacích tabulek. Filmově to Američané přehnali. Smůla byla v tom, že německé ponorky byly číslovány průběžně a nikdy se u nich neobjevovalo stejné číslo. Inkriminovaná ponorka byla skutečně spuštěna na vodu v roce 1941 a pod vedením poručíka Lüssova potopila 7 spojeneckých lodí.

Sama byla potopena dne 28. ledna 1944 západně od Irska hlídkovým bombardérem. Záměna je vyloučena. To už v Bletchley Parku dekódovali německé radiogramy jako na běžícím pásu.

Ukradli Enigmu

Bletchley Park byl v době II. světové války tajnou „Station X", kde na dešifrování německých zpráv pracovalo asi 10 tisíc zaměstnanců a před pár roky byla změněna v muzeum. A právě z tohoto muzea byla ukradena Enigma, a to dokonce během normální otevírací doby. Vynalézaví zloději pracovali v týmu a „zaměstnali" dozorce. Dohady v různých novinách mluví o tom, že se jednalo o krádež na zakázku. Cena přístroje se oceňuje asi na 150 tisíc eur. Byl to prakticky neprodejný přístroj. Jednalo se totiž o parádní kousek přímo z doby, kdy tam pracoval Alan Turing.

Paní Christine Large označila krádež za egoistické jednání, které návštěvníkům vzalo možnost obdivovat jedinečný kus dějin. Celá krádež Enigmy byla dána do souvislosti se sérií spektakulárních krádeží uměleckých předmětů v nedávné době z muzea v Oxfordu.

Přílišná důvěra

Podle Němců byla Enigma absolutně bezpečná a bylo vyloučeno aby člověk rozluštil její kód. Zapomněli jen na jednu maličkost. Zapomněli na sílu lidského ducha, co nedokáže člověk, mohl by dokázat člověkem sestavený computer, který by nedělal jako člověk jednu operaci za druhou, ale tisíce za vteřinu. Rozlousknutí Enigmy se jeví jako zázrak.

Zázrak, kterého bylo dosaženo díky vysoké skříni, vyplněné dráty, kolečky a páchnoucím olejem. Skříní, která byla schopna simulovat deset Enigmen.

Kódování a čísla ovlivnily chod dějin světa. Mnohdy nezáleželo na tom, zda kódována byla čísla nebo písmena, a velmi často je kódovali excentričtí a špatně oblečení muži, jako ve smyšlených postavách filmu Enigma. Jedni to dělali z výzkumné zvědavosti, druzí z patriotismu, dobrodružství, nebo v záhadách odhalovali jejich krásu, nebo je prostě jen mystifikovala čísla, a čísla posunují člověka k lákavému tajemství. Byli tací, kteří dokonce obdivovali kódování, dokonce na svých nepřátelích.

Dešifrování láká

Vypadá to, že shluky čísel a písmen určují chod světa. Proč se tak mnoho lidí zajímá o dějiny šifrování? Na to nám odpoví událost spojená s 11. zářím roku 2001. Od té doby se do popředí dostalo slovo válka. A mnoho lidí se začalo ptát, jak to tehdy bylo. Jak by mohla válka vypadat dnes.

A navíc kódování, to se neděje na frontě, ale v domě za stolem, a to zaměstnává mnohé. Lze se poučit z minulosti? Tehdy se postavilo mnoho inteligentních lidí proti násilí a oceli a zkrátilo válku. Bletschley Park se stal továrnou na budoucnost. Alan Turing dal základ prvnímu programovanému computeru. Vědění o computrech umožnilo, že se člověk dostal na Měsíc a třeba „vynalezl" Internet. Co se tehdy používalo v top secret Station X je dnes součástí našeho všedního života.

Na co si vzpomněla historie?

My, lidé 21. století jsme přešli od písmen k bitům. Písmena jsme rozložili na 0 a 1, ale stále čteme v písmenech. Zakódované zprávy dnes už nejsou jen textové, ale zakodováváme i mluvené slovo a dokonce i obrázky.

Enigma a Praha

A odkud měli spojenci vůbec první zprávy o Enigmě? S pravděpodobností, hraničící s jistotou z pražské Malé Strany. Tam Mr. Harald Lehrs Gibson, rezident britské tajné služby, chytil „vítr", že na dešifrování Enigmy pracují Poláci,

A druhá stopa, že Enigma pracuje ve vojenských službách? Zásluha patří francouzské zpravodajské službě. No, zásluha, jen v tom případě, že na zpravodajské frontě je všechno možné, i to, že 2 roky před II. světovou válkou přijde na francouzské velvyslanectví v Bernu člověk a nabídne tajné dokumenty wehrmachtu. Němec dostal jméno „Popel", pardon, jsme na francouzském velvyslanectví, tedy „Cender", ale tak se říká popelu ve francouzsky mluvících zemích.

A když jsme u zavádění Enigmy do wehrmachtu, pak si historie musí vzpomenout, kdo zaváděl šifrovací stroje Enigma do wehrmachtu. Jistý pan plukovník Erich Fellgiebel. Jméno si zapamatovala historie, zapamatujte si je i vy!

Vraťme se k tajemnému muži, který dostal přezdívku „Popel". Objevil se i u nás. Monsieur Gustav Bertrand – jinak důstojník francouzské tajné služby, byl jeden z prvních, kdo se o bernské story dověděl. Za nedlouho si přijel prohlédnout Prahu. Líbilo se mu Václavské náměstí a také Krkonoše, a úplně nejvíce okolí Davidovy boudy. A stejnou zálibu v české horské krajině má i „Popel".

Při tom obdivování přírody předá Bertrandovi organizační schémata německé zpravodajské služby, návod na použití šifrovacího stroje Enigma. A „Popel" dostane dobře zaplaceno. Spokojenost na obou stranách.

A Mr. Gibson zapracoval ještě jednou. Zajel do Varšavy a setkal se s inženýrem – vynikajícím matematikem, jehož jméno, jak už to u zpravodajských služeb bývá, na veřejnost neprosáklo. Pan inženýr byl žid, pracoval v Berlíně v továrně, kde se vyráběly Enigmy. Za obstarání vystěhovaleckého pasu do Francie pro sebe a svou ženu si vzpomněl, jak byla Enigma konstruovaná. Mr. Gibson pochopil co znamenají informace o Enigmě.

Marian Rejewski

V polovině roku 1939 doslova pár dní před přepadením Polska se Marianu Rejewskému a dalším jeho dvěma spolupracovníkům podařilo dostat na jih Francie. Ani ve Francii není bezpečno.

Jeden ze dvou spolupracovníků, jeden z tria, který byl přitom, když rozlouskli před II. světovou válkou kód Enigmy, zahynul v roce 1942 za nevyjasněných okolností.

Jak k tomu došlo? Bylo rozhodnuto, že bude v Alžíru zřízeno dešifrovací stanoviště a Rejewského přítel Rózycki tam odplouval na lodi, která za nevyjasněných okolností u Baleár ztroskotala, a nikdo se nezachránil. Náhoda? Smůla?

Rejewski se dostal až do Gibraltaru a přeplul do Anglie. Do dění s Enigmou už ale nezasáhl. To už byla výlučně britská záležitost. Je vůbec otázka, zda ti, kteří kolem Alana Turinga na dešifrování Enigmy pracovali, věděli o pionýrských pracích Rejewského.

Africký El Alamejn

„Působení" Enigmy nebylo omezeno jen na oblast Atlantiku. Dešifrování Enigmy umožnilo údajně zachránit RAF, anglické královské letectvo před Geringovou Luftwaffe.

Informace, které Enigma dodávala, měly mnohem širší působení. V Africe operoval generál Erwin Rommel – liška pouště. I jeho spojaři používali Enigmu. V Bletchley Parku zachytili Rommelovu zprávu, ve které se stanovoval den útoku a jeho směr. Dne 31. srpna 1942 byli Angličané připraveni v dostatečné síle. Dne 4. září bylo po bojích. Rommel odtáhl od Alam Halfy a později porážka u El Alamejnu jeho debakl zpečetila. Nikdy se nedověděl, že o výsledku bitvy u El Alamejnu se rozhodovalo tisíce kilometrů od vlastního bojiště, v Bletchley Parku v Anglii.

Bylo to také dílo Enigmy?

Za II. světové války ve Švýcarsku fungovala vysílačka, která dodávala zprávy Moskvě. Jejím šéfem byl Sándor Radó. Ty nejbrilantnější zprávy dodával Rudolf Rössler, který před fašisty utekl z německého města Kaufbeuren. To byly naprosto přesné a nejtajnější zprávy, které musely pocházet z okolí samotného Hitlera. Jak se k němu zprávy dostávaly? Bylo podezření, že mezi Německem a Švýcarskem existoval „čilý pohraniční styk".

Podezření bylo později vyvráceno. Zprávy se nemohly dostávat do Švýcarska „pěšky", vlakem nebo automobilem. Dostávaly se do Švýcarska velmi rychle. Radó dal Rösslerovi určité otázky a odpověď byla velmi rychlá. Klasickými dopravními prostředky to nebylo možno stihnout. Z toho vyplývalo, že Rössler – jinak záhadný Lucy – musel vlastnit vysílačku.

A je otázka, kdo byl na druhém konci rádiového spojení, kdo byl dodavatelem zpráv.

Je podezření, že zprávy pocházely zprostředkovaně od teď už generála Ericha Fellgiebela. Ano toho Fellgiebela, který ještě jako plukovník zaváděl Enigmu do německého wehrmachtu.

Patřil do okruhu spiklenců, kteří připravovali atentát na Hitlera. Byl šéfem zpravodajské služby, tedy šéfem bezdrátového spojení a znal se s plukovníkem Stauffenbergem, který položil bombu ve Vlčím doupěti. Generál Fellgiebel byl v září 1944 popraven. Proč takové podezření?

Jedna věc je dosud nevysvětlena. Vysílačka nebyla nikdy Němci zaměřena. Přitom Němci už díky zaměřovacím přístrojům věděli o všech vysílačkách, pracujících na jimi okupovaném teritoriu. V poměrně krátkém čase byli schopni místo vysílačky lokalizovat. Tato, která dodávala zprávy Rösslerovi, nebyla nikdy odhalena. Byla to „legální" německá vysílačka?

Je ještě jedna spekulace. Nemohly zprávy chodit z Bletchley Parku? Podezření by mohlo existovat. Důkazy jako obvykle chybí.

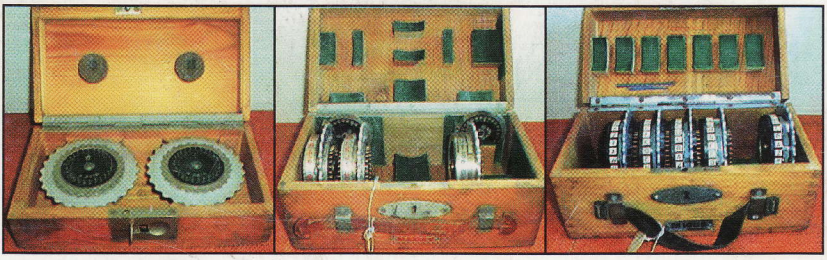
A PERLIČKU NAKONEC

Až do 70. let minulého století zamlčovali Angličané vše, co bylo spojeno se „Station X". Všechna svědectví byla zničena. Bylo to proto, že bylo odhaleno příliš mnoho?

Nemůže být vysvětlení v tom, že přístroje typu Enigma se prodávaly i po II. světové válce jiným státům, aniž ty měly tušení, že kód Enigmy lze zlomit?

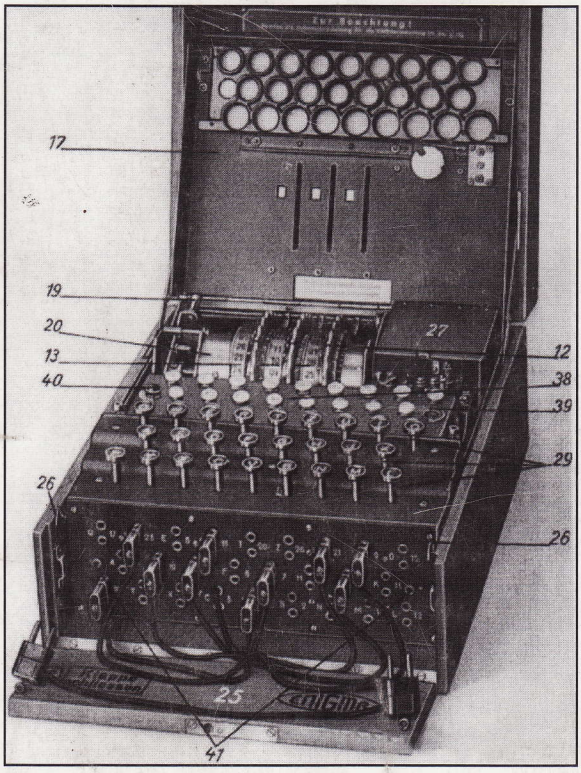
Zašifrované:

USPEC HJEDE VADES ATDEV ETPRO CENTD RINYJ EDNOP ROCEN TOSTE STI



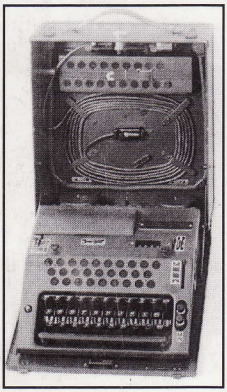
Repro: arred

KRABICE S ROTORY ENIGMY

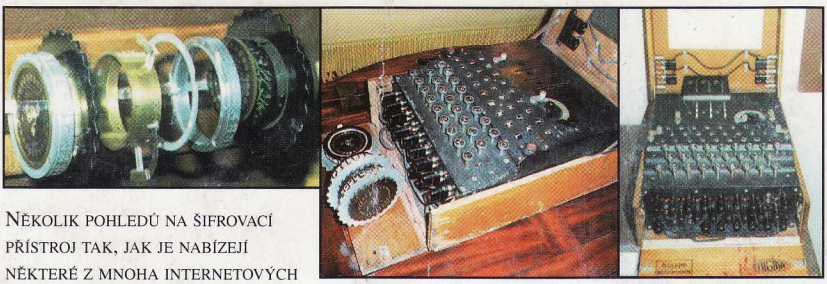


Repro: araut

ENIGMA V NĚMECKÉM MUZEU V MNICHOVĚ A JEJÍ NEJDŮLEŽITĚJŠÍ ČÁSTI:
12 – ŠIFROVACÍ VÁLCE,
27 – BATERIE,
38 – POLE ŽÁROVEK,
41 – ZDÍŘKA PRO KONTROLU KABELU



Repro: araut



Repro: arred

NĚKOLIK POHLEDŮ NA ŠIFROVACÍ PŘÍSTROJ TAK, JAK JE NABÍZEJÍ NĚKTERÉ Z MNOHA INTERNETOVÝCH STRÁNEK O ENIGMĚ