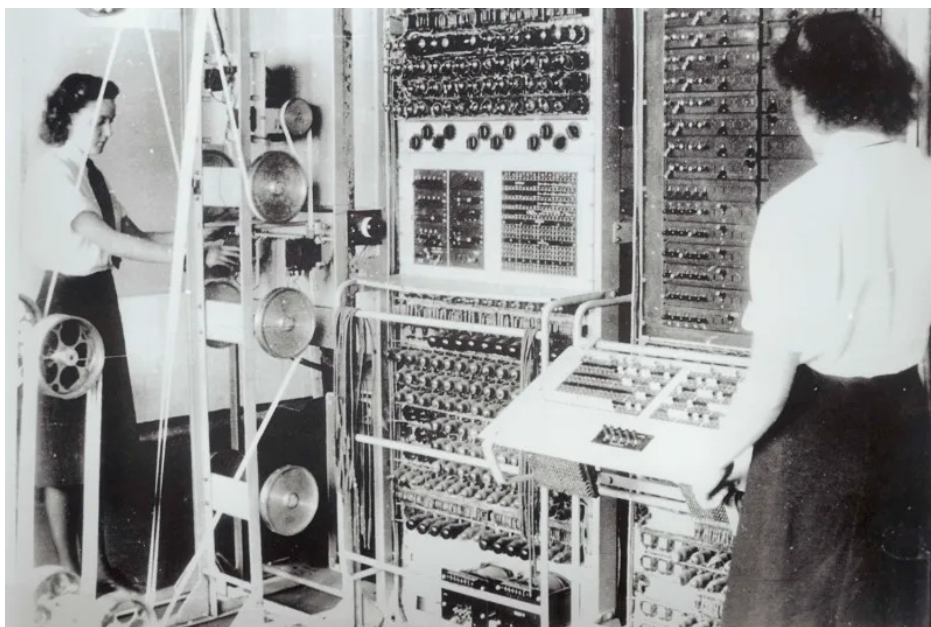




Kryptografie za II. světové války

Západočeská Univerzita V Plzni
Katedra Kybernetiky
Semestrální práce - HKUI

Ivana Roteenbornová
1. semestr
10. února 2026

1 Úvod

Tato *krátká* seminární práce se zaměří na roli kryptografie během II. světové války. Cílem je poukázat na to, jak vědecké pokroky v této oblasti zásadně ovlivnili vývoj tohoto globálního konfliktu a důležitost boje o informace ve válce.

2 Kryptografie

2.1 Definice

Kryptografie je nauka o metodách utajování smyslu zpráv převodem do podoby, která je srozumitelná pouze se speciální znalostí.

Někdy je pojem používán jako alternativa k pojmu **kryptologie**. Kryptologie je věda o čemkoli spojeném se šiframi a zahrnuje kryptografii a kryptoanalýzu, neboli luštění zašifrovaných zpráv.

2.2 Etymologie

Slovo kryptografie pochází z řečtiny:

- *kryptós* znamená skrytý
- *gráphein* znamená psát

2.3 Historie

Doklady o využití primitivních kryptografických technik se dochovaly z většiny antických civilizací. Jedná se především o zéměnu symbolů v dochovaných textech. Nejstarším známým příkladem je šifra v hrobce egyptského šlechtice jménem Khnumhotep II., který žil okolo 1 900 let př.n.l.. Jejím účelem s největší pravděpodobností nebylo utajení informací, ale zvýšit jazykovou přitažlivost hrobky. Nejstarší známý příklad využití kryptografie k utajení informací je okolo 1 500 let př.n.l. z Mezopotámie na utajení receptu na keramickou glazuru.

Za pozdní antiky byla kryptografie běžně využívána na ochranu vojenských informací, k čemuž se využívá dodnes. Z tohoto období pochází také velice známá Caesarova šifra.

Díky rozšíření počítačů se kryptografie v nedávné době vyvinula daleko za omezení analogických zařízení. 128-bitové matematické šifrování je dnes standardem pro ochranu citlivých zařízení a systémů. Kryptografie také umožnila (se vším dobrým i špatným) tvorbu kryptoměn.

3 U.S.A.

3.1 Organizace a projekty

3.1.1 Magic

Magic byl spojenecký kryptoanalytický projekt zahrnující armádu a námořnictvo Spojených států. Cílem bylo zahrnout Americké kryptologické projekty pod jedinou organizaci nazývané Research Bureau.

Za jejich nejvýznamnější úspěchy se pokládají prolomení japonských šifer přezdívaných 'RED', 'BLUE' a 'PURPLE'.

3.1.2 Signal Intelligence Service (SIS)

SIS byla vytvořena v roce 1930. Jejím cílem byla výroba vlastních kódů a šifrovacích zařízení pro armádu a pokusy o dešifrování komunikace potenciálních protivníků Spojených států.

3.2 Významné osobnosti

3.2.1 Elizebeth Smith Friedman (1892 - 1980)

Americká kryptoanalytička a autorka, která pracovala na prolamování kódů v obou světových válkách a případech mezinárodního pašování během Prohibice. Byla nazývána "první americkou kryptoanalytičkou".

3.2.2 William Frederick Friedman (1891 - 1969)

Kryptograf americké armády, který ve 30. letech 20. století vedl výzkumnou divizi SIS. V roce 1940 jeho podřízení v čele s Frankem Rowlettem prolomili japonskou šifru PURPLE.

3.2.3 Frank Byron Rowlett (1908 - 1998)

Americký kryptolog. V polovině 30. let vyluštili první japonský čírovací stroj známý jako RED. V letech 1939–40 Rowlett vedl úsilí SIS, které vyluštilo sofistikovanější japonskou šifru s kódovým označením PURPLE. Hrál také klíčovou roli v ochraně americké komunikace během druhé světové války a zásadně přispěl k návrhu šifrovacího stroje SIGABA.

3.2.4 Virginia Dare Aderholdt (1910 - 1997)

Kryptoanalytička z Arlington Hall a překladatelka japonštiny. Dešifrovala zachycenou zprávu o kapitulaci Japonska na konci druhé světové války, 14. srpna 1945.

3.2.5 Genevieve Marie Grotjan Feinstein (1913 - 2006)

Americká matematická a kryptoanalytička. Během druhé světové války pracovala pro SIS, kde sehrála důležitou roli při dešifrování japonského kryptografického stroje PURPLE a později pracovala na projektu Venona z doby studené války.

3.2.6 Leo Rosen (1916 - 1991)

Americký kryptoanalytik, který před začátkem druhé světové války pracoval s Frankem Rowlettem SIS na japonských šifrách. Rowlett našel metodu, jak číst zprávy zašifrované na japonském šifrovacím stroji PURPLE. Rosen správně odvodil mechanismus šifrovacího stroje, přestože mechanismus používaný šifrovacím strojem PURPLE, telefonní krokové přepínače, se podstatně lišil od jiných strojů.

3.2.7 Joseph John Rochefort (1900 - 1976)

Americký námořní důstojník a kryptoanalytik. Byl významnou postavou kryptografických a zpravodajských operací amerického námořnictva v letech 1925 až 1946, zejména v bitvě u Midway. Jeho příspěvky a příspěvky jeho týmu byly klíčové pro vítězství ve válce v Pacifiku.

3.2.8 Joseph Oswald Mauborgne (1881 - 1971)

Společně s Gilbertem Vernamem z Bell Labs vynalezl jednorázovou klávesnici. V roce 1914 publikoval první zaznamenané řešení šifry Playfair. Stal se generálmajorem armády Spojených států a od října 1937 do svého odchodu do důchodu v roce 1941 byl 12. hlavním signálním důstojníkem armády, velitelem signálního sboru.

3.2.9 Agnes Meyer Driscoll (1889 - 1971)

Snámá jako „slečna Aggie“ nebo „Madame X“. Byla americká kryptoanalytička během první i druhé světové války a byla známá jako „první dáma námořní kryptologie“.

3.3 Zařízení

3.3.1 SIGABA

Oficiálním názvem ECM Mark II. Jednalo se o šifrovací stroj používaný Spojenými státy k šifrování zpráv od druhé světové války až do 50. let 20. století. Stroj byl armádou známý jako SIGABA nebo Converter M-134, námořnictvem jako CSP-888/889 a upravená verze pro námořnictvo byla označena jako CSP-2900.

Stejně jako mnoho strojů té doby používal k šifrování zpráv elektromechanický systém rotorů, ale s řadou bezpečnostních vylepšení oproti předchozím konstrukcím. Žádná úspěšná kryptoanalýza stroje během jeho životnosti není veřejně známa.

3.3.2 SIGSALY

Známý také jako X System, Project X, Ciphony I a Green Hornet, byl zabezpečený hlasový systém používaný ve druhé světové válce pro spojeneckou komunikaci na nejvyšší úrovni. Byl průkopníkem v řadě konceptů digitální komunikace, včetně prvního přenosu řeči pomocí pulzně-kódové modulace.

Název SIGSALY nebyl zkratkou, ale krycím názvem, který se podobal zkratce - část SIG byla běžná v názvech armádních signálních sborů (např. SIGABA). Prototyp byl nazván "Green Hornet" podle rozhlasového pořadu The Green Hornet, protože každému, kdo se snažil odposlouchávat konverzaci, zněl jako bzučící sršeň, připomínající znělku pořadu.

3.3.3 SIGTOT

Jednorázový páskový stroj pro šifrování dálkopisné komunikace, který Spojené státy používaly během druhé světové války a po ní pro přenos nejcitlivějších zpráv. Byl vyvinut poté, co byly v dřívějším rotorovém stroji pro stejný účel, nazývaném SIGCUM, objeveny bezpečnostní chyby. SIGTOT navrhl Leo Rosen a používal stejný směšovač Bell Telephone 132B2 jako SIGCUM. Britové vyvinuli podobný stroj s názvem 5-UCO.

Fenomén s kódovým označením TEMPEST, kdy citlivé informace unikaly prostřednictvím nezamýšleného elektromagnetického záření pro obvody používané uvnitř šifrovacího stroje, byl poprvé objeven u směšovačů 131B2 používaných v těchto systémech.

Systém SIGTOT vyžadoval pro nepřetržitý provoz velké množství pásky s klíčem, což bylo nezbytné pro zabezpečení dopravního provozu. V roce 1955 NSA vyrobila přibližně 1 660 000 rolí jednorázové pásky. Logistické problémy spojené s generováním, dodávkami a ničením dostatečného množství pásky s klíčem omezovaly její použití pouze na nejcitlivější provoz. V 50. letech 20. století začala Bezpečnostní agentura americké armády vyvíjet náhradu, kterou později převzala nově vzniklá Národní bezpečnostní agentura (NSA), což vedlo k nasazení systému KW-26 (ROMULUS).

3.3.4 M-209

Označovaný americkým námořnictvem jako CSP-1500 (výrobce C-38. Jednalo se o přenosný mechanický šifrovací stroj používaný americkou armádou především ve druhé světové válce, ačkoli aktivně zůstal v provozu i během korejské války. M-209 navrhl švédský kryptograf Boris Hagelin v reakci na žádost o přenosný šifrovací stroj, který by byl vylepšením dřívějšího stroje C-36.

Ve své konečné podobě měří 83 mm * 140 mm * 178 mm a váží 2,7 kg (plus 0,45 kg na pouzdro).

4 Velká Británie

4.1 Organizace a projekty

4.1.1 Kryptanalýza Lorenzovy šifry ("Tunny")

Proces, který umožnil Britům číst zprávy německé armády na vysoké úrovni během druhé světové války.

V Bletchley Park dešifrovali mnoho komunikací mezi Oberkommando der Wehrmacht (OKW) v Berlíně a jejich armádními veleními v okupované Evropě, z nichž některé byly podepsány jako "Adolf Hitler, Führer". Jednalo se o zachycené rádiové přenosy, které byly zašifrovány pomocí německého zařízení Lorenz SZ. Dešifrování tohoto provozu se stalo důležitým zdrojem "ultra" zpravodajských informací, které významně přispěly k vítězství Spojenců.

Dešifrování zpráv zašifrovaných pomocí strojů Enigma v Bletchley Park odhalilo, že Němci nazývali jeden ze svých bezdrátových dálkopisných přenosových systémů "Sägefisch" (pilatá ryba), což vedlo britské kryptografy k označování šifrovaný německého radiotelegrafického provozu jako "Fish". "Tunny" (tuňák) byl název pro první spojení, které nebylo založeno na Morseově abecedě, a následně byl používán pro šifrovací stroje a jejich provoz.

Problémy s dešifrováním zpráv z Tunny vedly k vývoji "Colossus", prvního elektronického programovatelného digitálního počítače na světě.

4.1.2 FECB a WEC

Dvě zámořské základny Station X, Bletchley Park, britského centra pro analýzu signálů během druhé světové války.

Wireless Experimental Centre (WEC): Wilfred Noyce a Maurice Allen zde v roce 1943 prolomili japonský armádní kód pro vodní dopravu, což byl první prolomený kód japonské armády na vysoké úrovni.

Far East Combined Bureau (FECB): Monitorování japonské, čínské a ruské (sovětské) zpravodajských a rádiových operací.

4.2 Bletchley Park a kryptoanalýza Enigmy

4.2.1 Bletchley Park

Britské vládní kryptologické zařízení v provozu během druhé světové války. V Bletchley Park Alan Turing a další agenti zpravodajského projektu Ultra dešifrovali tajné zprávy, zejména ty, které byly zašifrovány německými šifrovacími stroji Enigma a Tunny.

Na začátku války v roce 1939 měl Bletchley Park pouze 200 pracovníků, ale koncem roku 1944 téměř 9 000, kteří pracovali ve třech směnách nepřetržitě. Mezi najatými byli odborníci na luštění křížovek a šachů, stejně jako matematici a vědci. Asi tři čtvrtiny pracovníků tvořily ženy.

Aby si zaměstnanci usnadnili práci, navrhovali a vyráběli zařízení, zejména objemné elektromechanické stroje na prolamování kódů zvané Bombes. Později, v lednu 1944, navrhli a sestavili Colossus, první elektronický počítač s 1600 elektronkami.

Navzdory zásadnímu významu práce měl Bletchley Park potíže se získáním dostatečných zdrojů. Proto v roce 1941 Turing a další zaměstnanci napsali dopis přímo premiérovi Winstonu Churchillovi, který okamžitě nařídil svému náčelníku štábu, aby „Zajistil, aby měli vše, co chtějí, s nejvyšší prioritou, a aby mi podal zprávu, že se tak stalo.“

Operace byly prováděny pod přísným utajením, které nebylo zrušeno ani po skončení války. Teprve v roce 1974, kdy Frederick William Winterbotham získal povolení k vydání svých pamětí s názvem „The Ultra Secret“, se svět začal dozvídat, čeho bylo v Bletchley Park dosaženo. Objekt je nyní udržován jako muzeum.

4.2.2 Alan Turing (1912 - 1954) a Prolomení Enigmy

Britský matematik a logik, který významně přispěl k matematice, kryptoanalýze, logice, filozofii a matematické biologii a také k novým oblastem později nazvaným informatika, kognitivní věda, umělá inteligence a umělý život.

Po vypuknutí války s Německem v září 1939 se přestěhoval do Bletchley Park. Několik týdnů předtím polská vláda informovala Británii a Francii o polském úspěchu prolomení Enigmy, hlavního šifrovacího stroje používaném německou armádou k šifrování rádiové komunikace. Již v roce 1932 se malému týmu polských matematiků-kryptoanalytiků pod vedením Mariana Rejewského podařilo odvodit vnitřní zapojení Enigmy a do roku 1938 Rejewského tým

vymyslel stroj na lámání kódů, který nazvali "Bomba". Úspěch Bomby závisel na německých operačních postupech a změna těchto postupů v květnu 1940 učinila Bombu nepoužitelnou.

Během podzimu 1939 a jara 1940 Turing a další navrhli podobný, ale velmi odlišný stroj na lámání kódů, známý jako "Bombe". Po zbytek války dodávala "Bombe" Spojencům velké množství vojenských zpravodajských informací. V roce 1942 Turing také vymyslel první systematickou metodu pro lámání zpráv zašifrovaných německým šifrovacím strojem, který Britové nazývali "Tunny". Na konci války byl Turing za svou práci na lámání kódů jmenován důstojníkem Nejvyššího řádu Britského impéria (OBE).

V březnu 1952 byl Turing usvědčen z „hrubé obscénnosti“ (homosexuality, která byla v té době v Británii trestným činem) a byl odsouzen k 12 měsícům hormonální "terapie". S trestním rejstříkem už nikdy nemohl pracovat pro Government Communications Headquarters (GCHQ), poválečné centrum britské vlády pro prolamování kódů.

Turing byl nalezen mrtvý ve své posteli, otrávený kyanidem. Oficiálním verdiktem byla sebevražda, ale při vyšetřování v roce 1954 nebyl zjištěn žádný motiv. Jeho smrt je často připisována jeho hormonální "léčbě". Zemřel však více než rok poté, co mu hormonální dávky skončily, a v každém případě odolný Turing snášel toto kruté zacházení s tím, co jeho blízký přítel Peter Hilton nazýval "pobavenou statečností". Dle záznamů vyšetřování také nebyly předloženy žádné důkazy, které by naznačovaly, že Turing měl v úmyslu vzít si život, ani že by byla narušena jeho duševní rovnováha. Jeho duševní stav se v té době zdál být zcela obyčejný. Ačkoli sebevraždu nelze vyloučit, je také možné, že jeho smrt byla jednoduše nehoda, důsledkem vdechnutí kyanidových výparů z experimentu v malé laboratoři sousedící s jeho ložnicí. Ani vraždu tajnými službami nelze zcela vyloučit, vzhledem k tomu, že Turing věděl tolik o kryptoanalýze v době, kdy byli homosexuálové považováni za hrozbu pro národní bezpečnost.

4.3 Zařízení

4.3.1 Turing-Welchman Bombe

Elektromechanické zařízení používané britskými kryptology k dešifrování tajných zpráv zašifrovaných německým strojem Enigma během druhé světové války.

První stroj založený na této technologii, známý jako "Agnus Dei" nebo

jednoduše "Agnes", byl uveden do provozu v srpnu 1940. Na konstrukci a konstrukci původních Bombe se podílela společnost British Tabulating Machine Company (BTM). Během války bylo v rámci této operace postaveno přibližně 211 strojů Bombe. Po válce jich bylo dočasně ponecháno asi 50 a některé, podle oficiálních dokumentů, pokračovaly v provozu. Zbytek byl demontován.

4.3.2 Počítač Colossus

První elektronický počítač na světě, určený k rozluštění zpráv zašifrované zařízením Lorenz ("Tunny") mezi Hitlerem a jeho generály během druhé světové války.

4.3.3 Typex

Rotorové šifrovací stroje, které byly vyvíjeny ve Velké Británii od roku 1934. Byly založeny na komerčním německém stroji Enigma, ale s několika změnami, pro zvýšení jeho bezpečnosti.

Byly používány k odesílání a přijímání zpráv pro Britskou armádu během druhé světové války, ale také kvůli své kompatibilitě s Enigmou v Bletchley Park k dešifrování zpráv Enigmy poté, co byl denní klíč získán pomocí Bombe.

5 Německo

5.1 Organizace a projekty

5.1.1 Beobachter Dienst

Zkráceně B-Dienst, v překladu "Pozorovatelská služba", byla německá námořní rádiová SIGINT (Signals Intelligence) služba. Kromě rádiového zaměřování a analýzy provozu se B-Dienst zabývala i prolamováním kódů. Německý systém rádiového zpravodajství zahrnoval také síť odposlechových stanic, které přeposílaly šifrované britské rádiové zprávy do velitelství B-Dienst v Berlíně, kde byly zprávy dešifrovány a využívány k zpravodajským účelům na podporu vojenských operací.

5.1.2 Amtsgruppe Wehrmachtnachrichtenverbindungen

V překladu šifrovací oddělení vrchního velení Wehrmachtu (také Oberkommando der Wehrmacht Chiffrierabteilung, nebo OKW/Chi, nebo Chi) bylo signální zpravodajské oddělení nejvyššího velení německých ozbrojených sil před druhou světovou válkou a během ní. OKW/Chi se v rámci formální německé bitevní hierarchie zabývalo kryptoanalýzou a dešifrováním zpráv nepřátelských a neutrálních států a bezpečnostní kontrolou vlastních klíčových procesů a strojů, jako byl rotorový šifrovací stroj ENIGMA. Bylo nástupcem bývalého úřadu Chi (Chiffrierstelle) ministerstva Reichswehru.

5.1.3 Reservehandverfahren

Běžně zkráceně R.H.V., nebo RHV, byla ruční šifra používaná během druhé světové války německou Kriegsmarine (námořnictvo) jako záložní systém, když nebyl k dispozici žádný funkční šifrovací stroj Enigma. Poprvé ji vyřešili britští luštitelé kódů z Bletchley Park v červnu 1941.

Zpráva kódovaná pomocí RHV vypadá přesně jako zpráva Enigma a postup pro její vytvoření je stejně složitý jako vytvoření zprávy kódované pomocí Enigmy. RHV je však mnohem méně bezpečná.

5.2 Významné osobnosti

5.2.1 Gisbert F. R. Hasenjaeger (1919 - 2006)

Německý matematický logik. Nezávisle a současně s Leonem Henkinem v roce 1949 vyvinul nový důkaz věty o úplnosti Kurta Gödela pro predikátovou logiku. Pracoval jako asistent Heinricha Scholze v sekci IVa Oberkommando der Wehrmacht Chiffrierabteilung a byl zodpovědný za bezpečnost stroje Enigma.

5.3 Zařízení

5.3.1 Enigma

V roce 1925 zakoupila německá armáda několik komerčně vyráběných šifrovacích strojů s názvem ENIGMA, který nejprve vyráběla společnost Chiffriermaschinen Aktiengesellschaft, vlastněná Arthurem Scherbiusem, a později společnost Chiffriermaschinen Gesellschaft Heimsoeth und Rinke. Po

určitých úpravách armáda stroj rozsáhle využívala k ochraně obchodní, diplomatické a vojenské komunikace. Během druhé světové války jej nacistické Německo používalo ve všech složkách armády. Stroj Enigma byl považován za tak bezpečný, že se používal k šifrování i těch nejprísněji tajných zpráv.

Navzdory zdánlivé obtížnosti dešifrování zpráv obsahovala Enigma řadu konstrukčních problémů, které v šifrovaném textu zanechávaly určité vzorce. Polsko poprvé prolomilo stroj již roku 1932. Díky tomu, že se podělili o své úspěchy, Spojenci mohli využít zprávy zašifrované Enigmou jako hlavní zdroj zpravodajských informací. Ačkoli nacistické Německo v průběhu let zavedlo do Enigmy řadu vylepšení, která brzdila snahy o dešifrování, kryptoanalýza Enigmy pokračovala po celou dobu války.

5.3.2 "Fish"

Pod obecným názvem Geheimschreiber (tajný pisatel) používali Němci dvě zařízení pro šifrování vysokoúrovňové (armádní a vyšší) komunikace radiotiskárnou. (Pro armádní a nižší úroveň se používala ENIGMA.) Jednalo se o T typ 52-B/C/D/E, vyrobený společností Siemens & Halske, a SZ-40/SZ-42, vyrobený společností Standard Elektrik Lorenz. „SZ“ znamenalo Schlüsselzusatz (klíčové připojení), nazývané tak, protože základní šifrovací mechanismus byl v krabici, kterou bylo možné oddělit od radiotiskárny.

Britové tyto stroje označovali obecným názvem "Fish" a konkrétně "Sturgeon" pro Siemens & Halske T52 a "Tunny" pro Lorenz.

6 Zdroje

https://en.wikipedia.org/wiki/World_War_II_cryptography

6.1 Úvod

Foto: <https://foreignpolicy.com/2021/07/05/geniuses-at-war-david-a-price-book-re>

6.2 Kryptografie

<https://cs.wikipedia.org/wiki/Kryptografie>

<https://www.binance.com/en/academy/articles/history-of-cryptography>

6.3 U.S.A.

<https://codenames.info/operation/magic-a/>
<https://history.army.mil/portals/143/Images/Publications/catalog/70-43.pdf>

6.4 Velká Británie

<https://www.britannica.com/place/Bletchley-Park>
<https://www.britannica.com/biography/Alan-Turing/Computer-designer>
<https://www.tnmoc.org/bombe>
<https://www.tnmoc.org/colossus>
<https://typex.virtualcolossus.co.uk/>

6.5 Německo

<https://warfarehistorynetwork.com/the-codebreakers-war-in-the-atlantic/>
https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/german_cipher.pdf