Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Bakalářská práce

Ondřej Vaverka

Historický vývoj kryptografie v období světových válek

Historical development of cryptography during the World Wars era

Praha 2012

Vedoucí práce: doc. RNDr. Jiří Ivánek, CSc.

Na tomto místě bych chtěl vzdát dík všem, kteří to se mnou vydrželi až do této chvíle a přes všechny strasti a překážky nade mnou nezlomili hůl. Jmenovitě vedoucímu práce doc. RNDr. Jiřímu Ivánkovi, CSc. za ochotu a cenné rady, svému klanu za trpělivost a nejmilejší Halgerdě za motivaci a pomoc, bez níž by tato práce pravděpodobně nikdy nedospěla ke zdárnému konci.

Věnovat bych však tuto práci chtěl Alanu Mathisonovi Turingovi k 100. výročí jeho narození a zároveň všem mužům i ženám, bez jejichž účasti na historických událostech zde popisovaných by dnešní svět nebyl takový, jaký ho známe.

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, že jsem řádně citoval všechny použité prameny a literaturu a že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze dne...

podpis

Vysoká škola: Univerzita Karlova | Fakulta: Filozofická fakulta

Součást: Ústav informačních studií a knihovnictví | Školní rok: 2007/2008

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta:	Ondřej Vaverka
Datum narození:	9.12.1985
Kontaktní adresa:	Sluneční 264, Vysoké nad Jizerou, PSČ 512 11
Obor studia:	Informační studia a knihovnictví
Název práce v češtině:	Historický vývoj kryptografie v období světových válek
Název práce v angličtině:	Historical development of cryptography during the World Wars era
Vedoucí práce:	Doc., RNDr. Jiří Ivánek, CSc.

Pokyny pro vypracování:

Cílem práce je zmapovat a popsat část novodobé historie kryptografického utajování informací. Práce se zaměří na období 1. a 2. světové války, tj. zhruba 1. polovinu 20. století.

Předběžná osnova:

1. Úvod
2. Šifrovací metody a stroje 1. sv. v.
3. Šifrovací metody a stroje 2. sv. v.
4. Shannonovy teoretické závěry
5. Závěr

Bakalářská práce bude připravena v souladu s platnými vnitřními předpisy FF UK a dalšími metodickými pokyny a normativními dokumenty.

Doporučená literatura:

1. KAHN, David. *The codebreakers : the story of secret writing*. 4th ed. New York : Macmillan, 1968. 1164 s.
2. JANEČEK, Jiří. *Gentlemani (ne)čtou cizí dopisy*. 1. vyd. Brno : Books, 1998. 175 s. ISBN 80-85914-90-5.
3. SINGH, Simon. *Kniha kódů a šifer : tajná komunikace od starého Egypta po kvantovou kryptografii*. 1. vyd. Praha : Dokořán ; Argo, 2003. 382 s. Aliter, sv. 9. ISBN 80-7203-499-5.

Vedoucí práce (podpis): Doc., RNDr. Jiří Ivánek, CSc.

Datum zadání práce: 15.5.2008

L.S.

Univerzita Karlova v Praze
Filozofická fakulta (4)
Studijní oddělení
Praha 1, nám. J. Palacha 2, 11638

PhDr. Richard Papík, Ph.D.

.....
Vedoucí základní součásti

.....
Děkan

V Praze dne 15.5.2008

Identifikační záznam

VAVERKA, Ondřej. *Historický vývoj kryptografie v období světových válek [Historical development of cryptography during the World Wars era]*. Praha, 2012-07-27. 77 s. Bakalářská práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí bakalářské práce Jiří Ivánek.

Abstrakt

Bakalářská práce se zabývá popisem kryptografických a kryptoanalytických metod období první a druhé světové války a historických okolností s tím souvisejících. V úvodu je stručně popsán vývoj kryptologie před 1. sv. válkou. První hlavní kapitola se věnuje aplikaci kryptologie v průběhu 1. sv. války. Další kapitola stručně překlenuje meziválečné období a poté se zaměřuje na druhoválečnou kryptologii. Detailně rozebrán je především program Ultra a problematika stroje Enigma. Závěrečná kapitola je věnována kryptografickému odkazu 2. sv. války v podobě díla Clauda E. Shannona.

Klíčová slova

kryptologie, kryptografie, kryptoanalýza, šifra, první světová válka, druhá světová válka

Abstract

This bachelor thesis deals with the description of cryptographic and cryptanalytic methods during the First and Second World Wars and related historical circumstances. The introduction briefly describes the development of cryptology prior to WWI. The first major chapter examines the application of cryptology during WWI. The next chapter concisely bridges the interwar period, and then focuses on WWII cryptology. The Ultra programme and the problem of Enigma machine is analyzed here in detail. The final chapter is a dedicated to the aftermath of WWII cryptographic efforts in the form of papers by Claude E. Shannon.

Keywords

cryptology, cryptogryphy, cryptanalysis, cipher, First World War, Second World War

Obsah

Předmluva

V předkládané bakalářské práci se věnuji vývoji kryptografických a kryptoanalytických metod v průběhu první a druhé světové války. Toto období je z hlediska kryptologie obzvláště zajímavé, neboť jak známo, válka bývá často motorem technického pokroku. Zcela v souladu s tím i oba velké konflikty 20. století vnesly na pole utajování informací velké množství změn a nakonec i jednotný teoretický základ, který kryptologii do plnohodnotné vědní disciplíny dlouho chyběl.

K výběru tématu mě inspirovala především výběrová přednáška Kódování informací, kde pozdější vedoucí této práce doc. RNDr. Jiří Ivánek, CSc. podstatně rozšířil mé povědomí o obecné problematice kódování i jeho speciální kategorii, šifrování. Má původní představa tématu práce bylo průřezové zpracování celých dějin kryptologie od prvních dochovaných zmínek až po současnost. Období do počátku novověku však již bylo v podobné práci rozebráno a z možných zúžení tématu díky své přelomovosti a poutavosti nejlépe vyšla právě éra světových válek.

V této práci si zdaleka nekladu za cíl popsat detailně všechny dobové metody šifrování a prolamování šifer. Existuje několik publikací, které se o toto snaží, a všechny mají jedno společné - rozsah rovný menší encyklopedii. Na omezeném rozsahu této závěrečné práce se chci věnovat spíše zajímavým a historicky významným případům a poskytnout tak čtenáři přehledné podání problematiky. Proto se nezabývám pouze samotnými principy šifrování, ale podstatnou část rozsahu práce tvoří popis historických událostí, které za vývojem šifer i jejich prolamováním stály. Nebudu se tajit tím, že při výběru kryptoanalytických metod, které rozebírám hlouběji, jsem se řídil i tím, zda jsem byl vůbec schopen dané metodě plně porozumět. Některé postupy prolamování zvláště druhoválečných strojů jsou natolik komplikované, že jejich studium by bylo třeba doplnit též studiem vysoké školy matematického zaměření.

Těžiště práce spočívá v popsání situace z pohledu stran Dohody a západních Spojenců; soustředí se tedy až na několik výjimek především na kryptoanalytické útoky vítězných stran a kryptografické metody stran poražených. Důvodem je především špatná dostupnost zdrojů, nabízejících pohled ze strany poražených.

Terminologie užívaná v této práci vychází z následujících publikací:

- *Encyclopedia of cryptography and security*, 2005
- RITTER, 2007
- SINGH, 2003

Veškeré bibliografické záznamy jsou zpracovány v souladu s citační normou ČSN ISO 690:2010. Záznamy jsou řazeny abecedně podle vstupního prvku. Pro citace je použit harvardský citační systém.

1. Úvod

Snaha utajovat některé informace byla vždy nedílně spojena s bojem. Komunikace antických vojevůdců pomocí skytale, nebo steganografie se dochovala v mnoha pramenech a použití Caesarovy šifry je dostatečně známo. Ne vždy muselo jít o vojenský konflikt. Šifry našly využití i v konkurenčním boji indických obchodníků nebo zápolení novověkých milenců o vdané ženy. Vždy však jde o to samé. Na jedné straně stojí snaha informace utajit a v zabezpečené podobě je dodat adresátovi, který jim porozumí, na druhé pak snaha nepřátelské zprávy zachytit, rozluštit a jejich znalost využít k vlastnímu prospěchu. Tyto protichůdné síly nápadně připomínají např. závody ve zbrojení a stejně jako zbrojní průmysl je i utajování informací velmi dynamickým oborem.

S postupným vývojem vědních oborů, zvláště lingvistiky a matematiky, se zdokonalovaly postupy jak šifrování, tak prolamování šifer. Nejranější šifry využívaly především jednoduchou substituci či transpozici. V devátém století však dosavadní metody rázem zastaraly, když arabský učenec al-Kindí publikoval metodu kryptoanalýzy monoalfabetické substituce pomocí frekvenční analýzy. Dalším krokem byly nejrůznější kombinace starších šifrových systémů a především polyalfabetická substituce. Její první podoba je připisována Leonu Battistovi Albertimu, avšak nejznámější a na dlouhou dobu nejpoužívanější se stala tzv. Vigenérova šifra[1], vynalezená v druhé polovině 16. století. Ta byla až do poloviny 19. století považována za neprolomitelnou šifru. V roce 1854 však Charles Babbage vypracoval postup její kryptoanalýzy na základě nalézání shodně zašifrovaných částí textu a z nich odvozené délky klíče. Metodu však nepublikoval a později byla připsána Friedrichu Kasiskému, který ji nezávisle objevil devět let po Babbageovi. Zda k zamlčení objevu Babbage vedly britské státní zájmy v Krymské válce, nebo přelétavost, s níž opouštěl většinu svých projektů v rozpracovaném stavu, není známo [Cypher Research Laboratories, 2006].

[1] viz. kapitola 2.4.3

2. Kryptologie 1. světové války

První světová válka vnesla do praktik vojenské špionáže zcela nový fenomén. Tím bylo masové rozšíření rádiové komunikace a od něho samozřejmě odvisející potřeba přenášené zprávy šifrovat a na straně nepřítele naopak snaha šifry rozluštit [JANEČEK, 1998, s.31]. Nejznámějším příkladem využití informací získaných za pomoci rádiového odposlechu se stala Bitva u Tannenbergu, o níž bude pojednávat jedna z následujících kapitol.

Před válkou měly pouze dva státy vybudovaný funkční systém zachytávání a luštění tajných depeší - Francie a Rakousko-Uhersko [PIEKALKIEWICZ, 2004, s.266]. Se začátkem konfliktu měly i ostatní státy eminentní zájem na budování vlastní zpravodajské sítě. Nejdále v tomto závodě dospěla Velká Británie s dešifračním oddělením tajné služby britské admirality[2], které vešlo do dějin pod jménem Room 40.

2.1 Vznik a úspěchy britské kryptoslužby

4.8.1914, tedy přesně týden po vypuknutí války, splnil britský člun poblíž německého města Emdenu sabotážní úkol přerušení podmořských komunikačních kabelů spojujících Německo se zámořskými zeměmi. Tento strategický tah donutil Německo po zbytek války používat pro přenos zpráv téměř výhradně rádiovou komunikaci. Jako hlavní vysílač byla využívána 200kW rádiová stanice v městečku Nauen poblíž Postupimi [WOOD, 2000, s.57].

V listopadu 1914 zřídilo vedení NID zvláštní oddělení pro zachytávání a dešifraci nepřátelské komunikace, které dostalo krycí název podle čísla dveří ve staré budově admirality na Whitehallu, kde sídlilo. Room 40 vyrostl na základech dřívějších "poloprofesionálních" aktivit Jamese Alfreda Ewinga, který se kryptologií zabýval spíše jako koníčkem s několika svými přáteli [KAHN, 1968, s.266-276]. Vedením nově vzniklého oficiálního oddělení byl zprvu pově-

[2] Naval Intelligence Department, neboli NID

řen admirál Henry Oliver, který byl však vzápětí nahrazen kapitánem Williamem Reginaldem Hallem. Kapitán, později admirál Hall se budování nového úřadu ujal vskutku svědomitě. To, co začínalo jako skromné oddělení v jedné místnosti, se do konce války proměnilo v pracoviště čítající na jeden tisíc Hallových podřízených - radistů, kryptologů, tlumočníků a dalších profesí. Hall pro Room 40 získal takové odborníky jako Alfreda Dillwyna Knoxe, Nigela de Greye, Williama Montgomeryho a mnohé další, z nichž mnozí o 25 let později zúročili své zkušenosti v Mekce druhoválečné kryptoanalýzy, Bletchley Parku.

Zachycenými zprávami zásobovaly Room 40 odposlouchávací stanice ve východní Anglii. Konkrétně se jednalo o 44 zaměřovacích stanic ve vlastnictví královského námořnictva, doplňovaných 6 stanicemi společnosti British Marconi Company. Tyto sloužily mimo jiné i k zachytávání komunikace mezi přístavy ve Wilhelmshavenu a Kielu a ke sledování pozice německých lodí na základě jejich komunikace. Denně bylo takto odposlechnuto až 2000 depeší, z nichž mnohé, zvláště zpočátku válečného konfliktu, nebyly ani šifrovány [PIEKALKIEWICZ, 2004, s.267].

Mnohé zprávy však šifrovány byly a bez patřičných kódových knih bylo jejich luštění velmi obtížné. Zde Hallovi několikrát pomohla šťastná náhoda. První z nich bylo zajetí německého parníku Hobart u australských břehů a ukořistění kódové knihy kódu HVB. Jen o několik dní později, 26.8.1914, ztroskotal poblíž Rusy ovládaného Estonska při záškodnické akci křižník Magdeburg. Ruské námořní síly zajaly kompletní posádku spolu s kódovou knihou SKM. Kapitán Magdeburgu udělal takřka školáckou chybu, když navzdory vidině zajetí přikázal spálit všechny tajné dokumenty "... s výjimkou těch, které by ještě mohly být potřeba." [PIEKALKIEWICZ, 2004, s.267] Ruská admiralita posléze v zájmu tehdy velmi dobrých rusko-anglických vztahů kódovou knihu předala Winstonu Churchillovi, tehdy ministru námořních sil, s tím, že Británie jakožto námořní velmoc tuto kořist využije nejlépe.

Díky těmto šťastným náhodám mohlo královské loďstvo začít slavit konkrétní bojové úspěchy. Prolomení nepřátelské šifrované komunikace vedlo ke zmaření plánu, podle kterého měly čtyři německé torpédové čluny v říjnu 1914 zaminovat ústí Temže [HALPERN, 1995, s.125-131]. Včasné varování z Room 40 poskytlo britskému loďstvu dostatek času na zosnování a následné úspěšné provedení přepadu. O několik dní později navíc rybářská loď nahlásila nález bedny obsahující další signální knihu s kódem VB a pocházející z jednoho z potopených minových člunů.

Se znalostí těchto kódů byl Hallův tým schopen zásobovat admiralitu aktuálními zprávami o pohybech a záměrech německého loďstva a nezřídka znali Britové zprávu dříve než její legitimní adresát. Německé velitelství navíc v prvních dvou letech války měnilo klíče jen velmi zřídka, případně vůbec, takže jednou získaná kniha mohla sloužit Britům velmi dlouhou dobu [PIEKALKIEWICZ, 2004, s.268].

Nezřídka však muselo být šťastné náhodě pomoženo, tak jako po německé anexi Belgie, kdy Němci začali využívat bruselský vysílač. NID se dozvěděla, že radistou na stanici je britský rodák Alexander Szek. Dohledat jeho příbuzné v Anglii nebylo nijak těžké a donutit je, aby Alexandra přemluvili ke spolupráci, také ne. Tak s příslibem pomoci v útěku Szek během tří měsíců ručně opsal celou signální knihu přísně tajného diplomatického kódu 13042 a předal ji Britům. Pomoci se samozřejmě nedočkal, protože jeho zmizení by na německé straně vyvolalo podezření a učinilo celou akci zbytečnou. Podle jedné verze ho později Němci odhalili a popravili, podle jiné ho v tichosti zlikvidovali sami Britové [BOROVIČKA, 1982, s.25-28].

Další velmi nečestnou a nesportovní akcí bylo získání kódových knih z německého konzulátu v Persii[3] a jemu předcházející hon na Wilhelma Wassmusse. Wassmus, někdy též po vzoru známějšího T.E. Lawrence přezdíván Wassmuss z Persie, byl německým diplomatem působícím na středním východě. Po vy-

[3] dnešní Írán

puknutí války dostal za úkol získat na stranu Německa pomocí propagandy šířené mezi domorodými kmeny dosud neutrální Persii, oblast strategicky důležitou především díky tamním obrovským zásobám ropy. Po cestě byla však jeho expedice přepadena anglickými jednotkami. Jeho pobočníkovi se sice podařilo zachránit tajné dokumenty včetně kódových knih, které si s sebou výprava vezla, a samotný Wassmuss se spasil téměř filmovým útěkem. Britové však neváhali a knihy si vyzvedli přímo z německého konzulátu v Persii spolu s tamním konzulem. Toto hrubé porušení mezinárodního práva muselo být nějak zakryto. V oficiální verzi příběhu tak knihy byly celkem prozaicky nalezeny ve Wassmussově zavazadle, které za sebou zanechal při útěku [PIEKALKIEWICZ, 2004, s.270-272]. Kód, který takto Hall získal, se však později projevil jako zcela nedocenitelný. Jednalo se o diplomatický kód 13040, jehož derivát byl v roce 1917 použit k zašifrování zprávy, která zvrátila průběh celého konfliktu.

2.2 Tannenberg - bitva vyhraná odposlechem

Na východní frontě naopak na počátku konfliktu slavily úspěchy síly Centrálních mocností. Bitva u Tannenbergu je dobrým příkladem toho, kam může vést nedůsledné použití kódování při utajované komunikaci.

V průběhu válečných příprav vedení ruského šifrovacího střediska ze strachu před zrádci ve vlastních řadách pozdrželo přidělování kódových knih jednotlivým plukům a naivně, spoléhavše na to, že nepřítel neposlouchá, se rozhodlo prozatím vysílat rozkazy v otevřené řeči [KAHN, 1968, s.622-627].

Rusové se ihned po vyhlášení války v srpnu 1914 rozhodli zaútočit na německou 8. armádu jistící oblast Východního Pruska. Tento úkol měly provést dvě ruské armády, známé jako Něvská a Narevská, obě velením spadající pod generála Zilinského. Něvská armáda měla zaútočit s dvoudenním předstihem a Němce zdržet, zatímco Narevská by od jihu nepříteli odřízla ústupovou cestu na západ a nakonec by ho dostala do kleští. Ruské jednotky nebyly dosud zvyklé v masové míře používat rádiové spojení a ještě menší ochotu projevovaly ke kó-

dování přenášených zpráv. Němci, kteří ruskou komunikaci bedlivě sledovali, měli dokonce zpočátku dojem, že jde spíše o vskutku ubohý zastírací manévr, než o reálné rozkazy. Nakonec však uvěřili a vypracovali strategii, podle níž měla celá 8. armáda zaútočit na dosud se přesouvající Narevskou armádu u vesničky Tannenberg[4]. Něvskou armádu mělo zdržet jen několik slabých oddílů jezdectva a domobrany. Ruský postup na jihu byl zpomalen špatným terénem i nedostatkem zásob a v komunikaci mezi jednotlivými divizemi vládl doslova chaos. Není tak divu, že se hlavní německé síle podařilo 26.9.1914 zaskočit Rusy zcela nepřipravené, obklíčit je a během čtyřdenní bitvy zcela zdecimovat [PIEKALKIEWICZ, 2004, s.272-275].

2.3 Zimmermannův telegram

Situace v západní Evropě začala na počátku roku 1917 houstnout. Spojené státy byly stále ještě neutrální velmocí, klonící se sice spíše na stranu Dohody, ovšem udržující dobré diplomatické vztahy i s Centrálními mocnostmi. Tato pozice nejlépe vyhovovala jejich obchodním zájmům - jako neutrální mohli bez obav zásobovat svářící se evropské státy nedostatkovými potravinami, zbraněmi i kapitálem. Důsledkem toho byl i poválečný desetimiliardový dluh Evropy vůči americkým bankám [BOROVIČKA, 1982, s.29]. Velká Británie tohoto obchodního spojenectví využívala nejvíce, neboť jako izolovaný ostrov mohla také nejvíce pocítit případný nedostatek zásob. Německé politické špičky si byly této zranitelnosti svého úhlavního nepřítele dobře vědomy a rozhodly se jí využít k rychlému ukončení vlekoucího se konfliktu.

17.1.1917 se dostal dvěma členům Room 40, Nigelu de Greyovi a Williamu Montgomerymu, do rukou text depeše kódované pomocí před nedávnem získaného a bedlivě střeženého kódu 13042. Jako první rozpoznali jméno odesílatele, jímž byl německý ministr zahraničí Arthur Zimmermann, a adresáta, německého velvyslance ve Washingtonu hraběte Johanna von Bernstorffa. Již z toho

[4] dnešní polský Stębark

bylo zřejmé, že jde o zprávu velmi vysoké důležitosti, což se potvrdilo jejím dalším zkoumáním. Celý telegram, který bylo však nejdříve nutné poskládat ze tří samostatných zpráv odeslaných různými kanály, sděloval následující: za několik dnů Německo oficiálně vyhlásí totální ponorkovou válku a tím prakticky blokádu Británie. Vzhledem k tomu, že útoky budou logicky vedeny především na americká zásobovací plavidla, dá se v nejhorším ze strany USA očekávat vyhlášení války. Pro tuto eventualitu se má von Bernstorff pokusit již předem získat na stranu Německa v revolucích se zmítající Mexiko za příslib pomoci v dobytí jižních států USA. Stejně tak má požádat o podobnou pomoc i Japonské císařství.

Německý plán téměř neměl trhlinu - pokud by Spojené státy nijak nereagovaly, Velká Británie bude muset do několika měsíců kapitulovat, a pokud přece jen Amerika do války vstoupí, bude alespoň zpočátku zaměstnána především bojem na vlastním území. Jediná, avšak fatální chyba Němců tkvěla v neznalosti faktu, že Room 40 prolomil jejich nejtajnější kód.

Hall měl nyní unikátní příležitost ke konečnému získání Spojených států na stranu Dohody. Jediným problémem bylo, jak tuto příležitost využít, aniž by Němci pojali podezření, že jejich kód byl kompromitován. Jedinou možností bylo fingované zachycení zprávy v otevřeném textu, tedy buď původní depeše u von Bernstorffa, nebo von Bernstorffovy nabídky spojenectví mexické vládě. Britským agentům se v Mexiku podařilo obstarat kopii telegramu obsahujícího von Bernstorffovu nabídku a tuto verzi Hall předal americkému velvyslanci W.H. Pageovi, který ji dále tlumočil své vládě. Zpráva zprvu neměla takový účinek, v jaký Hall doufal. Prezident Wilson považoval celou aféru za britský trik k vlákání USA do války, avšak v reakci na německé ponorky alespoň přerušil s Německem diplomatické styky. Aby Hall Američany přesvědčil a zároveň ještě více odvrátil pozornost Němců od svého oddělení, nechal v Kanadě zadržet nyní již vyhoštěného von Bernstorffa vracejícího se do vlasti a v jeho zavazadlech fingovaně nalezl původní text telegramu. Tato depeše již byla oficiálně

předána tisku, a když nakonec i sám Zimmermann potvrdil její pravost, nezbývalo vládě USA, než se podvolit tlaku veřejnosti a vyhlásit Německu válku.

Mexický prezident si včas spočítal, že vyhlášení války USA by jeho zemi nemohlo přinést nic dobrého, a stejně tak Japonsko i přes některé neshody s Ruskem raději setrvalo na straně Dohody. Ubohý von Bernstorff se vrátil domů s pověstí neschopného zrádce vlastního národa a Britové nadále nerušeně luštili nejtajnější německé zprávy [PIEKALKIEWICZ, 2004, s.275-281; FREEMAN, 2006].

2.4 Principy šifer 1. světové války

Šifry první světové války vesměs nepřinášely nic nového a šlo pouze o různé variace ručních šifer 19. století, které již byly dávno prolomeny [SINGH, 2003, s.106].

V následujících podkapitolách budou stručně rozebrány tři principy šifrování. Jeden, který během první světové války již spíše dožíval, další, který byl pro prvoválečné účely vyvinut a aktivně používán, a třetí, který sice splňuje charakteristiky neprolomitelné šifry, avšak nebyl nikdy v boji nasazen. Krátce je též pojednáno o použití kódů.

2.4.1 Playfairova šifra

Playfairova šifra byla zkonstruována roku 1854 Charlesem Wheatstonem, který ji pojmenoval po svém příteli a největším propagátorovi šifry, baronu Lyon Playfair [PIPER, 2006, s.39-42]. Zprvu byla britskými úřady odmítána pro svou zdánlivou složitost, avšak později došla uplatnění v druhé búrské válce a v období první světové války [SINGH, 2003, s.352].

Principem jde o bigramovou symetrickou substituční šifru, jejímž klíčem je tabulka o pěti řádcích a pěti sloupcích. Počet všech možných klíčů získáme součtem přes všechny možné řetězce o 25 znacích bez opakování, což ve výsledku dává 25!, tedy přibližně $1{,}55\times10^{25}$ [PIPER, 2006, s.40].

Před samotným šifrováním je zapotřebí upravit otevřený text a připravit si tabulku s klíčem. Z levého horního rohu začneme postupně do políček vepisovat písmena předem dohodnutého klíče, přičemž pokud se písmeno již v tabulce vyskytuje, vynecháme jej a pokračujeme následujícím. Po vepsání klíče doplníme zbylá políčka písmeny abecedy, která ještě nebyla použita. Protože tabulka má 25 políček a standardní anglická abeceda 26 písmen, je nutné jedno nejméně používané písmeno konstantně nahrazovat jiným. V angličtině se nejčastěji zaměňuje J za I a například pro češtinu je výhodné použít zaměňování Q za K. Jak písmena klíče, tak zbývající mohou být do tabulky zapisována jakýmkoliv jiným předem dohodnutým způsobem.

Otevřený text rozdělíme do skupin po dvou písmenech, tzv. bigramů, přičemž provádíme nahrazování vynechaného písmena. Pokud se vedle sebe v bigramu vyskytla dvě stejná písmena, je třeba je oddělit jiným znakem, nejčastěji X nebo Z. Pokud vyjde počet znaků otevřeného textu lichý, doplníme také poslední znak o závěrečné X nebo Z.

Takto upravený otevřený text šifrujeme podle následujících pravidel:

1) Leží-li obě písmena na stejném řádku tabulky, nahradíme každé z nich písmenem nacházejícím se o jednu pozici vpravo. Pokud bychom se dostali mimo tabulku, nahradíme prvním písmenem řádku.
2) Leží-li obě písmena ve stejném sloupci tabulky, nahradíme každé z nich písmenem nacházejícím se o jednu pozici níže. Pokud bychom se dostali mimo tabulku, nahradíme prvním písmenem sloupce.
3) Leží-li písmena v různých řádcích i sloupcích, nahradíme každé z písmen tím, které leží v průsečíku jeho řádku a sloupce zbývajícího písmene.

Nejlépe ilustrujeme postup na následujícím příkladu.

Otevřený text: PREPARE TO ATTACK ON ALL FRONTS

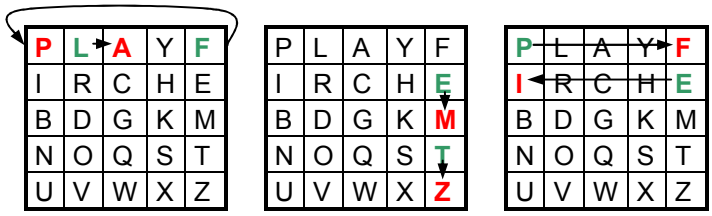
Klíč: PLAYFAIRCIPHER

Otevřený text rozdělený do bigramů s vloženými pomocnými znaky X a nahrazeným J za I: PR EP AR ET OA TX TA CK ON AL LF RO NT SX

Tabulka s vepsaným klíčem, doplněná o zbývající písmena abecedy

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

Příklad šifrování bigramů LF (stejný řádek), ET (stejný sloupec) a EP (různý řádek i sloupec)



Šifrový text: LI IF LC MZ QL SZ QF HG QO YA AP DV ON XY

Dešifrovaní probíhá aplikací modifikovaných pravidel pro šifrování, kdy nahrazujeme písmena na stejných řádcích písmeny ležícími o jedno vlevo a písmena ve stejných sloupcích písmeny ležícími o jedno výše. Výsledný text zbývá již jen očistit od pomocných znaků X a případně zaměnit zpět nepoužité písmeno abecedy J.

Kryptoanalýza šifry může být založena na hrubé síle pomocí frekvenční analýzy bigramů šifrového textu a bigramů v jazyce otevřeného textu. Oproti klasické substituční šifře však při analýze bigramů musíme počítat s 600 různými bigramy namísto 26 písmen. Jiná metoda aplikovatelná při částečné znalosti otevřeného textu využívá identifikaci inverzních bigramů (např. DE a ED)

a z nich vycházející rekonstrukci možného slova v otevřeném textu (např. slovo ***DE***FEND***ED*** zakódované jako ***MR***LREM***RM***) [LYONS, 2009].

2.4.2 Šifra ADFGX

Na konci války nejrozšířenější německá polní šifra byla vyvinuta plukovníkem Fritzem Nebelem v posledním roce války.

Byť se použitím tabulky o 5x5 písmenech podobá Playfairově šifře, jde o zcela odlišný kryptosystém doplňující frakcionovanou substituci[5] následnou transpozicí. Jedná se o implementaci klasického Polybiova čtverce, kde však souřadnice jednotlivých písmen nejsou zaznamenány čísly, nýbrž písmeny A, D, F, G a X. Vlastností šifrového textu je samozřejmě dvojnásobná délka, ovšem možnost soustředit se na vysílání pouhých pěti různých znaků výrazně snižuje možnost chyby při kódování. To podporuje i fakt, že použitá písmena nejsou v Morseově abecedě snadno zaměnitelná.

Princip šifry spočívá v rozmístění písmen abecedy do čtverce o 5x5 polích podobně jako u Playfairovy šifry. Opět je třeba jedno písmeno nahrazovat. Toto rozmístění může být zcela libovolné, je však nutné, aby pro obě strany komunikace bylo totožné. Jednotlivé sloupce a řádky jsou poté označeny písmeny A, D, F, G a X. Otevřený text zašifrujeme tak, že každé jeho písmeno nahradíme bigramem skládajícím se z písmena řádky a písmena sloupce [BURTON, 1985].

Otevřený text:

HALTEN SIE IHRE POSITION

Náhodně zvolený ADFGX čtverec:

	A	D	F	G	X
A	c	k	d	p	r
D	n	v	h	y	w
F	u	a	o	g	i/j
G	f	l	s	b	z
X	m	t	e	q	x

[5] tzn. každý znak otevřeného textu je nahrazen několika znaky šifry

Text v bigramech:

DF FD GD XD XF DA GF FX XF FX DF AX XF AG FF GF FX XD FX FF DA

Vzniklý řetězec poté po jednotlivých písmenech vepíšeme do tabulky o tolika sloupcích, kolik písmen má předem zvolený transpoziční klíč, zde slovo SCHANZE:

S	C	H	A	N	Z	E
D	F	F	D	G	D	X
D	X	F	D	A	G	F
F	X	X	F	F	X	D
F	A	X	X	F	A	G
F	F	G	F	F	X	X
D	F	X	F	F	D	A

Sloupce tabulky seřadíme tak aby písmena transpozičního hesla byla podle abecedy:

A	C	E	H	N	S	Z
D	F	X	F	G	D	D
D	X	F	F	A	D	G
F	X	D	X	F	F	X
X	A	G	X	F	F	A
F	F	X	G	F	F	X
F	F	A	X	F	D	D

Výsledný šifrový text připravený k odvysílání dostaneme čtením tabulky po sloupcích:

DDFXFF FXXAFF XFDGXA FFXXGX GAFFFF DDFFFD DGXAXD

V praxi se osvědčilo vysílat delší zprávy po kratších úsecích s použitím více různých transpozičních klíčů.

Dešifrování zpráv probíhalo jednoduchým obrácením celého postupu, tedy seřadit sloupce podle původního transpozičního klíče a nalezení písmen otevřeného textu pomocí souřadnic ADFGX čtverce.

Systém byl později rozšířen ještě o písmeno V, čímž vznikla šifra ADFGVX. Dodatečné písmeno umožňovalo zařadit do tabulky všech 26 písmen abecedy bez nahrazování, spolu s číslicemi 0-9.

Kryptoanalýza ADFGX a ADFGVX byla poněkud tvrdším oříškem, který rozlouskl v červnu 1918 francouzský kryptolog Georges Painvin. Jeho první metoda spočívala v nalézání podobných vzorů v delších zprávách se stereotypním počátkem a následné složité statistické analýze. Druhá metoda těžila z faktu, že každý sloupec obsahuje pouze písmena z řádkových, nebo sloupcových souřadnic ADFGX čtverce, avšak nikdy jejich kombinaci. Každé písmeno řádkové nebo sloupcové souřadnice tak bylo pevně svázáno se skupinou pěti písmen otevřeného textu. Frekvenční analýzou těchto pětic byl Painvin schopen rozpoznat, které sloupce se skládají z řádkových a které ze sloupcových souřadnic čtverce. Poté již zbývalo jen sloupce správně spárovat a provést jednoduchou frekvenční analýzu nahrazením bigramů písmeny otevřeného textu.

Bez zajímavosti není, že tento výkon Painvina fyzicky i nervově natolik zmohl, že v průběhu prolamování šifry onemocněl a zhubl o 15kg [SINGH, 2003, s.106].

2.4.3 Vernamova šifra

Na sklonku první světové války přišli dva američtí kryptologové, Gilbert Vernam, zaměstnanec telekomunikačního giganta AT&T Bell Laboratories, a major Joseph Mauborgne, vedoucí kryptografického výzkumu americké armády, s myšlenkou, že již více než padesát let prolomená Vigenérova šifra by za určitých předpokladů mohla posloužit ke konstrukci nové, snad již opravdu nerozluštitelné šifry. Základní myšlenka byla jednoduchá: celá síla Vigenérova systému závisí na délce klíče. Čím je klíč kratší, tím více se šifra blíží triviálnímu Caesarovu posunu, který rozlouskne i malé dítě. Proč tedy nepoužít klíč co nejdelší, tedy tak dlouhý jako sama zpráva? Tento prostý předpoklad se ve vý-

sledku ukázal být jediným dodnes známým kryptosystémem, který při správném použití odolává všem myslitelným útokům.

Protože šifra, která vešla v obecné povědomí jako Vernamova, principiálně staví na Vigenérově systému, nebude na škodu jej zde krátce představit. Základní pomůckou pro konstrukci šifrového textu je tzv. Vigenérův čtverec (viz příl. 1), tedy tabulka o 26x26 polích, kde každý sloupec i řádek je nadepsán jedním písmenem abecedy. Samotnou tabulku pak tvoří 26 abecedních řad posunutých vždy o jeden znak oproti předchozímu řádku. Šifrování probíhá vyhledáním znaku otevřeného textu v nadpisech sloupců a znaku klíče v nadpisech řádků. V průsečíku příslušného sloupce a řádku pak leží znak šifrového textu. Klíč můžeme zvolit libovolně dlouhý a po vyčerpání všech jeho znaků pokračujeme opět od jeho počátku. Analogicky pak probíhá dešifrování. Jak již bylo zmíněno, základním faktorem pro složitost či jednoduchost kryptoanalýzy je zde délka klíče, kterou lze zjistit metodou analýzy koincidencí, nebo Kasiského testem. Při znalosti délky klíče se problém kryptoanalýzy polyalfabetické substituční šifry rozpadá na triviální frekvenční analýzu tolika monoalfabetických substitučních šifer, kolik znaků má předpokládaný klíč [SINGH, 2003, s.117].

Vernamova a Mauborgnova inovace spočívá ve zvolení takové délky klíče, při níž nedochází k jeho opakování, tedy klíče stejně dlouhého jako zpráva sama. Za klíč můžeme pro jednoduchost zvolit např. text určité předem dohodnuté knihy. V takovém případě mluvíme o metodě běžícího klíče. Tento způsob však není dokonalý, neboť klíč tvořený textem ve známém jazyce přenáší některé charakteristiky tohoto jazyka do šifrového textu a může tedy být kryptoanalytikem zpětně rekonstruován. Stačí zkoušet kombinovat kousky předpokládaného otevřeného textu s šifrovým textem, a pokud výsledek představuje opět srozumitelný text, je pravděpodobné, že jsme nalezli kus klíče. S dostatečně dlouhou takto odhalenou částí klíče je pak již vcelku triviální dohledat jeho původní zdroj.

V ideálním případě by klíč měl být tvořen zcela náhodnou posloupností znaků. Takový klíč pak i do šifrového textu vnáší svou náhodnost a zcela znemožňuje kryptoanalýzu takové zprávy. Dokonce ani útok hrubou silou, kterým je možno alespoň teoreticky prolomit většinu ostatních šifer, zde není použitelný. Pokud např. na zprávu o 34 znacích šifrovanou v 26 znakové abecedě použijeme útok hrubou silou, pak dostaneme pouze balík všech možných zpráv o 34 znacích[6], z nichž vzhledem k náhodnosti klíče nemáme jak vybrat tu správnou. Případný útočník tedy nemá prostředek, kterým by zjistil, zda původní zpráva říkala "utoctezitrazausvituvsemiprostredky", "generalovadceramapozitrinarozeniny", nebo šlo jen o pouhý krutý žert šifranta odvysílavšího náhodnou změť znaků [SINGH, 2003, s.117].

Ani samotná délka a náhodnost klíče však nevede k neproniknutelnosti šifry. Pro tu je třeba splnit ještě třetí předpoklad, díky němuž se Vernamova šifra často označuje také jako "one-time pad". Jednou použitý klíč již nesmí být znovu použit pro zašifrování jiné zprávy. Pokud máme k dispozici jen dvě zprávy zašifrované týmž klíčem, je možné, byť velmi pracné, šifru prolomit.

Jakkoliv se na první pohled může zdát dodržení těchto pravidel jednoduché, opak je pravdou. Délka klíče činí Vernamovu šifru nepoužitelnou při běžné vojenské komunikaci, kdy se vyměňují i tisíce dlouhých zpráv denně. Způsob, jak rychle a bezpečně dopravovat ke všem stranám komunikace nově vygenerované klíče, se zdá být prakticky řešitelný až v dnešních dnech za pomoci kvantové kryptografie. Navíc je třeba zajistit synchronizaci klíče mezi jednotlivými účastníky, tedy aby jeden účastník komunikace nevědomky neodesílal zprávu v klíči, který již některý jiný účastník před ním použil. Ani samotné generování náhodných hodnot, ať už písmen nebo bitů, není jednoduché. Většina běžně dostupných způsobů vytváří pouze pseudonáhodné řady, které se řídí určitými, byť často složitými zákonitostmi. Jako použitelná se jeví metoda měření fyzikálních jevů, které zákonitosti postrádají - např. radioaktivního vyzařování, na-

[6] tedy 26^{34} zpráv

pěťového šumu, atp. Konečný předpoklad použití jednoho klíče pouze jednou pak již plně závisí na šifrové disciplíně jednotlivých účastníků komunikace.

Všechny výše zmíněné problémy činí Vernamovu šifru použitelnou pouze tam, kde jsou komunikující ochotni vynaložit velké finanční i časové prostředky na zajištění absolutně bezpečné komunikace, rozhodně tedy ne do polních podmínek bojiště [GOEBEL, 2010].

2.4.4 Polní kódy

S tím, jak se hranice válčících států postupně ustálily v mezích několika kilometrů zdevastované fronty a nastala poziční zákopová válka, začaly se jako výhodnější forma utajování komunikace nežli šifry prosazovat kódy. Na rozdíl od šifry nestaví kód svou bezpečnost na utajení klíče. Jde vlastně o substituci, avšak nikoli jednotlivých znaků, nebo jejich skupin, nýbrž celých slov či frází. Pro takovou komunikaci je nutné, aby obě strany měly totožnou kódovou knihu obsahující kódovací a dekódovací tabulku. Tyto knihy je nutno vždy v předstihu distribuovat jednotlivým stranám komunikace a posléze svědomitě chránit. Z toho plyne zranitelnost systému, kdy získání kódové knihy nepřítelem znamená naprostou kompromitaci kódu a znemožňuje jeho další efektivní použití. Pro minimalizaci následků případného ukořistění knihy byly tyto, stejně jako klíče šifer, pravidelně měněny. Navíc byly kódové knihy často úmyslně tištěny na nekvalitní papír, který snadno hořel a po krátkém čase sám podléhal degradaci.

Pro příklad použití kódu můžeme sáhnout ke známé cimrmanovské hře, kde špiónka Kuncová dává britské tajné službě na vědomí, že „salonní vůz Františka Josefa dorazil“, pomocí zprávy „přijel vagón s francovkou, první třída.“ [CIMRMAN, 2001, s.39-39]. V reálu však bylo používáno nahrazení každého slova či ustáleného slovního spojení sérií písmen, případně číslic. Typická kódová kniha se tedy podobala více či méně obsáhlému slovníku, kde pro zakódování stačilo dohledat podle abecedy požadované slovo a nahradit jej odpovídají-

cím kódem. Pro dekódování sloužila druhá část kódové knihy obsahující seřazenou tabulku kódů a jim odpovídající slova otevřeného textu.

Kódy bývají ze své podstaty užší, co do tematického zaměření své slovní zásoby. Většinou není efektivní tvořit příliš složitý kód, který by pokrýval vyjadřovací schopnosti celého jazyka, a nejlépe se služby dobrého kódu využijí v oblastech, kde se dá předem předpokládat charakter otevřeného textu. S pomocí kódu určeného pro potřeby dělostřelectva se tedy jen velmi obtížně povede filozofická debata o Kantově pojetí etiky. Naproti tomu šifra, která nepracuje se slovy, nýbrž se znaky, má vyjadřovací schopnosti prakticky neomezené.

Kryptoanalýza kódu vyžaduje spíše lingvistické než statistické a kombinatorické znalosti a podobá se tak v mnohém např. rekonstrukci zaniklého jazyka [KAHN, 2004, s.xv]. Pokud máme k dispozici dostatečné množství materiálu zakódovaného stejným kódem a alespoň rámcovou představu o obsahu jednotlivých zpráv, případně i o stylistických zvyklostech jejich odesílatele, může být prolomení některých jednodušších kódů možné. Většinou zde však přicházejí ke slovu praktiky špionáže: opisování, či přímo krádeže kódových knih.

3. Kryptologie 2. světové války

3.1 Meziválečný stav britské kryptologie

Až do posledních měsíců první světové války panovala téměř kontraproduktivní řevnivost mezi armádní kryptoslužbou MI1b, vedenou majorem Malcolmem Hayem, a již zmíněným námořním oddělením Room 40 pod taktovkou admirála Halla. Jen zřídka probíhala mezi odděleními jakákoliv spolupráce a komunikace mezi nimi byla omezena na nutné minimum. S koncem války však logicky přišly škrty v armádním rozpočtu, které nakonec vedly až ke sloučení obou konkurenčních pracovišť pod společným názvem Government Code and Cypher School (GC&CS). Vedením nově vzniklého oddělení byl pověřen veterán Room 40 Alfred Denniston. GC&CS narozdíl od Room 40 nebyla oficiálně neexistujícím oddělením, ovšem její jméno bylo i tak spíše zástěrkou. Navenek se oddělení mělo tvářit coby pouhý konzultant pro vývoj kryptosystémů pro potřeby britské vládní garnitury, nicméně hlavní činností zůstávalo i v době míru luštění zahraniční utajené komunikace.

Prakticky bezedný zdroj odposlechů pro GC&CS zajistila britská vláda, když roku 1920 schválila zákon nařizující kabelovým společnostem na vyžádání poskytovat přenášené zprávy. Tento zdroj doplňovaly rádiové zachytávací stanice v Pembroke a Scarborough a stanice z prvoválečných let mimo britské území, zejména na Maltě, středním východě a nově zřízená v Hong-Kongu [COPELAND, 2006, s.19].

I přes veškeré válečné zásluhy obou dešifrovacích služeb však mírová léta učinila z GC&CS pouze chudou sestru tajné služby, které se každé oddělení, pod něž byla převedena, rádo brzy zbavilo. Tak se z jurisdikce admirality, pod

níž byla zpočátku zařazena, přesunula nejprve pod ministerstvo zahraničních věcí a posléze skončila jako jedno z oddělení MI6[7].

GC&CS slavila po dobu své meziválečné existence hned několik úspěchů, které se však často ukázaly být poněkud dvojsečnými. Třikrát, v letech 1920, 1923 a 1927, vedlo zachycení a dešifrování sovětských zpráv k překažení plánů bolševické revoluce ve Velké Británii. Poslední případ však již nebylo možné ututlat a britská strana byla nucena odposlech sovětské komunikace přiznat. To vedlo k mezinárodnímu skandálu a rozhodnutí Sovětů používat nadále pro zprávy nejvyšší citlivosti výhradně kódy superšifrované[8] Vernamovou šifrou [ALDRICH, 2010, s.18; COPELAND, 2006, s.20].

V roce 1936 s celkovým vyostřením mezinárodních vztahů a hrozbou dalšího konfliktu většího rozsahu začala luštitelská práce opět nabývat na významu. GC&CS se tak rozrostla o menší, dosud samostatné kryptooddělení letectva a především jeho zachytávací radiostanice.

3.2 Enigma - matka mechanických šifrovacích strojů

První světová válka byla zenitem, avšak zároveň i labutí písní ručních šifer. Práce spojená s jejich šifrováním a dešifrováním ve výsledku neodpovídala jejich bezpečnosti proti luštění ze strany nepřítele. Již poslední rok války však přinesl inovaci, která měla ovlivnit kryptologické zápolení po několik následujících desetiletí. 23.2.1918 podal německý inženýr Arthur Scherbius první z řady žádostí o patent na "Chiffrierapparat", mechanickou pomůcku pro utajování zpráv [BAUER, 1991]. Spolu s kolegou Richardem Ritterem se snažil vzbudit zájem u potenciálních zákazníků ze soukromého i armádního sektoru, avšak většinou byl zdvořile odmítnut. To vedlo k odprodání všech dosavadních paten-

[7] britská tajná služba dnes oficiálně známá pod názvem Secret Intelligence Service (SIS). V době druhé světové války spadala pod Directorate of Military Intelligence a to pak přímo pod Ministerstvo války

[8] superšifrování - použití další odlišné metody k sekundárnímu zašifrování již jednou zašifrované nebo zakódované zprávy

tů akciové společnosti Chiffriermaschinen AG, s tím, že jak Scherbius tak Ritter dostanou místo v její správní radě. Konečně v roce 1923 byla na kongresu Mezinárodní poštovní unie v Bernu představena první komerčně dostupná verze šifrovacího stroje pod obchodním názvem Enigma. Po počátečních rozpacích a nezájmu ze strany soukromého sektoru, na nějž byl vynález především cílen, bylo uvedeno několik dalších vylepšených verzí. Ty postupně slavily větší úspěch a Scherbius uzavřel kontrakty na prodej svého stroje do zemí jako Švédsko, Japonsko, Polsko, USA i Velká Británie. Kromě soukromého sektoru vyjádřily zájem o Enigmu také armády několika zemí. Největším podporovatelem a uživatelem Enigmy se stala německá vláda a ozbrojené síly. I vláda Velké Británie zvažovala zařazení Enigmy jako platformy pro utajenou komunikaci na nejvyšší úrovni, avšak po konzultaci s GC&CS svůj zájem přehodnotila. Již tehdy kryptologové z GC&CS rozpoznali v konstrukci Enigmy několik drobných chyb, které později vedly k jejímu úspěšnému luštění. Scherbius nicméně svou inovativní myšlenkou nastartoval novou éru kryptografie - éru mechanických šifrovacích strojů. Na základě Enigmy posléze vznikla celá řada odvozenin - britský Typex, německé Lorenz SZ40 a Siemens und Halske T52, americký SIGABA, či již poválečný sovětský stroj Fialka.

3.2.1 Součásti Enigmy a jejich funkce

Enigma od svého prvního modelu prošla několika konstrukčními změnami, které postupně zvyšovaly její efektivitu [REUVERS, 2012]. Základem stroje však ve většině verzí byly následující součásti:

1) Klávesnice - klasická klávesnice à la psací stroj s kontinentálním rozložením QWERTZU, na níž se zadával otevřený text. Nejčastější počet kláves byl 26, avšak některé verze měly 29, či naopak pouze 10 kláves.

2) Vstupní stator - na něj byly připojeny na vstupu kontakty z klávesnice a na výstupu kontakty pravého rotoru[9].

3) Rotory - samotný šifrovací mechanismus a srdce celého stroje. Rotor je kotouč skládající se z několika částí (viz příl. 2 a 3).

Z kryptologického hlediska je hlavní funkcí rotoru substituovat abecedu na vstupní straně jinou abecedou na výstupní straně pomocí pevně daných drátových propojení mezi kontakty. Jeden samotný rotor tak má účinnost klasické monoalfabetické šifry. Většina verzí Enigmy využívala naráz tři různé rotory, přičemž po každém stisknutí klávesy se pravý rotor pootočil o jeden krok dopředu. Po jedné kompletní otáčce (tj. 26 krocích) pravého rotoru se o jednu pozici posunul rotor střední a obdobně, po jedné otáčce prostředního se o jednu pozici posunul levý rotor. Tím průběžně při každém stisku klávesy vznikalo nové zapojení, které vedlo elektrický impulz jinou cestou. Rotory byly ručně nastavitelné do libovolné pozice, čímž se určovala jedna ze složek klíče přenášené zprávy. Navíc bylo možné rotory vyjmout a změnit jejich pořadí, případně vybrat jiné rotory ze sady[10].

Prstenec s abecedou (příl. 2, č.3) je oproti jádru rotoru libovolně nastavitelný a nemění jeho vnitřní funkci. Využití najde při nastavování klíče zprávy, kdy je třeba celý rotor i s abecedním prstencem ručně nastavit tak, aby skrze průzor v krytu Enigmy bylo vidět správné písmeno. K prstenci byl připevněn kroužek se zářezem (příl. 2, č.1), který řídil posun dalšího rotoru. Z osmi možných rotorů, které byly k dispozici na konci války, měly rotory 1-5 pouze jeden zářez. Rotory 6-8, přidané později jako součást námořních verzí Enigmy, měly zářezy dva, což zdánlivě přispívalo k nepravidelnosti chodu stroje, avšak ve skutečnosti pouze zkracovalo periodu klíče na polovinu.

---

[9] Pojmy "vstup" a "výstup" jsou u systému rotorů Enigmy poněkud složitější. Díky reflektoru, který obrací směr propojení skrze rotory, můžeme obě strany rotoru nazvat zároveň vstupem i výstupem. Stejně tak vstupní stator funguje zároveň jako výstupní. Pro jednoduchost tyto pojmy používám z pohledu elektrického proudu procházejícího elektrickým obvodem stroje.

[10] Před druhou světovou válkou byly k dispozici pouze tři rotory, později došlo k přidání dalších dvou a ke konci války bylo k dispozici až osm různých rotorů.

4) Reflektor - obdoba vstupního statoru, která doléhala na výstupní kontakty levého rotoru. Reflektor obsahoval 13 spojení mezi 26 dvojicemi kontaktů, čímž vracel impulz z levého rotoru opět do levého rotoru, avšak jako jiný znak. Impulz byl tak podruhé jinou cestou poslán skrze všechny tři rotory zpět a z kontaktů vstupního statoru putoval do žárovkové desky. Ve většině verzí byl reflektor statický, nechoval se tedy jako čtvrtý rotor.

5) Žárovková deska - "displej" přístroje sestávající z průsvitného filmu s 26 písmeny, přičemž pod každým se nacházela žárovka. Po stisku klávesy a uzavření elektrického obvodu skrze soustavu stator/rotory/reflektor došlo k rozsvícení jedné z žárovek, která indikovala odpovídající znak šifrového textu.

6) Zdroj napájení - k chodu rotorů nebylo napájení zapotřebí, protože byl řízen stiskem kláves. Žárovková deska však potřebovala napájení, které bylo realizováno standardní a po celou válku dobře dostupnou 4,5V baterií.

Podstatným vylepšením bezpečnosti armádní Enigmy oproti civilním modelům bylo zařazení tzv. rozvodné desky[11]. Šlo o 26 párů písmeny nadepsaných kontaktů manuálně propojitelných kabely. Tato součást byla v elektrickém obvodu Enigmy zařazena před a za soustavu stator/rotory/reflektor. Byla-li například propojena písmena S a D a písmeno S bylo stisknuto na klávesnici, rozvodná deska jej substituovala písmenem D a jako takové jej poslala do statoru. Obdobně, pokud by nastal případ, kdy by se na výstupu statoru objevilo písmeno S, rozvodná deska by jej před vstupem do žárovkové desky substituovala písmenem D. V konečném efektu se tedy rozvodná deska chovala jako další sice statický, avšak plně konfigurovatelný rotor. Počet použitých kabelů se časem měnil. Před vypuknutím druhé světové války bylo nařízeno používat 5-8 a později 7-10 kabelů, v závislosti na konkrétní komunikační síti.

[11] něm. "Steckerbrett", angl. "plugboard"

3.2.2 Vývojové stupně Enigmy

Enigma A - první komerční verze z roku 1923. Postrádala reflektor, rozvodnou desku a funkci žárovkové desky zastával mechanismus psacího stroje, který tisknul šifrový text na papír. Stroj byl kvůli tiskovému mechanismu těžký a často se zasekával. Klávesnice kromě 26 znakové abecedy obsahovala také znaky Ä, Ö, Ü. Rotory však měly jen 28 kontaktů, protože písmeno X neprocházelo šifrovacím procesem.

Enigma B - uvedena roku 1924. Enigma A s vylepšeným tiskovým mechanismem

Enigma C - uvedena roku 1924. První verze s reflektorem a žárovkovou deskou. Jednalo se o první vpravdě přenosnou verzi, zabudovanou v dřevěné krabici, která stala pro další modely Enigmy typickou. Ve standardní verzi měla 26 kláves v netypickém rozložení ABCDEFG, avšak vyráběla se i ve verzi pro německé válečné loďstvo a pro vývoz do Švédska, shodně s 29 klávesami.

Enigma D - uvedena roku 1926. Vylepšená verze C. První verze s vyměnitelnými rotory a reflektorem nastavitelným do 26 pozic. Tato verze se dá považovat za základ pro většinu dalších modelů.

Enigma G - uvedena roku 1927. Narozdíl od ostatních modelů není otáčení rotorů řízeno zářezem na prstenci s abecedou, nýbrž pomocí soustavy ozubených kol řízených počítadlem[12]. Pohyb rotorů byl díky tomu nepravidelný a prolomení šifry mnohem složitější. Derivát modelu G používala za války pro interní komunikaci německá tajná služba Abwehr.

Enigma H - uvedena roku 1929. Poslední z řady tiskových strojů[13]. Obsahovala osm rotorů, přičemž na šifrování se podílely pouze čtyři z nich, zbylé čtyři pak řídily jejich otáčení. Stejně jako verze A a B byla i H těžká a náchylná k zasekávání.

[12] odtud oblíbené pojmenování pro tento model Zählwerk Enigma

[13] Především pro komerční účely byly odlišovány řady Schreibende Enigma, tj. modely A, B, H, a Glühlampenmaschine, tj. modely které používaly zobrazení pomocí žárovkové desky.

Enigma Z - uvedena roku 1930. Netypický model pouze s 10 klávesami obsahující číslice 0-9. To ji předurčovalo k použití při superšifrování kódovaných depeší. Existovala verze jak s pravidelným pohybem rotorů, tak s počítadlem po vzoru modelu G.

Enigma I[14] - uvedena roku 1932. První verze vyráběná výhradně pro německé ozbrojené síly. Prvním uživatelem se stala armáda (Wehrmacht), zanedlouho se připojilo letectvo (Luftwaffe) a nakonec i námořnictvo (Kriegsmarine). Námořnictvo později vedlo vlastní vývoj odvozených modelů M1, M2 a M3, které přinesly mnoho vylepšení. Za všechny jmenujme zvýšení počtu možných rotorů, plně konfigurovatelný reflektor, nebo rotor s libovolně nastavitelnými zářezy pro posun. Největší devizou tohoto modelu a všech jeho následných odvozenin se však stala již zmíněná rozvodná deska.

Enigma M4 - další vývojový krok odvozený od Enigmy I. Výhradním uživatelem M4 bylo ponorkové námořnictvo, odtud přezdívka U-Boot Enigma. K již zavedeným osmi možným rotorům přibyl jeden další ve dvou verzích. Tento čtvrtý rotor se však neotáčel, nýbrž pouze předřazoval reflektoru v jedné z 26 možných pozic, z nichž jedna byla zpětně kompatibilní s předcházejícími modely [REUVERS, 2012; SCHUCHMANN, 1983].

3.2.3 Práce s Enigmou

Klíč k zakódování zprávy před odesláním a jejímu dekódování na straně příjemce je tvořen několika na sobě nezávisle nastavitelnými parametry.

1) Výběr a seřazení rotorů - většina verzí stroje používala v jednu chvíli tři rotory, nejdříve ze tří, poté z pěti, později až z osmi možných. K prostoru možných klíčů přispívá tento faktor při osmi možných rotorech 336 možnostmi.[15]

2) Startovní pozice jader rotorů - nastavitelné operátorem pomocí volících kroužků (příl. 2, č.9). Přispívá 26^3, tedy 17576 možnostmi.

[14] Označení I v tomto případě znamená římskou číslici.
[15] (8×6×7)

3) Nastavení prstenců s abecedou vůči jádrům rotorů - tzv. Ringstellung. Rovněž nastavitelné operátorem. Přispívá pouze 26^2, tedy 676 možnostmi, protože levý rotor žádným dalším neotáčí a na nastavení jeho prstence tak nezáleží.

4) Propojení rozvodné desky - teoreticky při použití 0-13 kabelů přispívá až $5{,}3\times10^{14}$ možnostmi. Nařízení pro používání Enigmy při zde popisovaném šifrování však jasně předepisovala použití přesně 10 kabelů, což zúžilo prostor možných klíčů na $1{,}5\times10^{14}$, podle vzorce $\frac{26!}{n!\times(26-2n)!\times2^n}$, kde n značí počet současně použitých kabelů [MILLER, 1995].

Celý prostor možných klíčů tak ve výsledku dává přibližně 6×10^{23} možností nastavení stroje. To pro srovnání přibližně odpovídá 2^{79}, tedy 79 bitovému šifrování. To ovšem platí pouze za předpokladu, že případný útočník, který by se pokoušel šifru prolomit, zná vnitřní zapojení všech rotorů. Pokud není zapojení známo, vzroste prostor možných klíčů na přibližně 10^{114}.

Změny parametrů 1 a 3 byly prováděny obvykle jednou za dva dny, parametr 4 byl měněn každý den a parametr 2 se lišil pro každou zprávu. Změny probíhaly v souladu s knihami denních nastavení. Tato nastavení byla pro každou komunikační síť odlišná. Například Luftwaffe se svým nastavením nemohlo dekódovat zprávy ponorkové Enigmy a naopak[16] [COPELAND, 2004b, s.227].

[16] Jednotlivé komunikační sítě byly britskými kryptology v Bletchley nazývány "klíče" a každá měla vlastní krycí jméno, např. Lufrwaffe - Red, ponorky - Shark, atlantické námořnictvo - Dolphin, atd.

Postup bezpečného přenosu klíče zprávy se v průběhu doby i v jednotlivých komunikačních sítích lišil. Pravděpodobně nejkomplikovanější, avšak zároveň nejbezpečnější postup byl využíván od roku 1940 německým námořnictvem [COPELAND, 2004b, s.271-273]. Postup spoléhal na dvojici knih, první se seznamem denních nastavení a druhou zvanou Kenngruppenbuch, neboli K-Buch. Ta sestávala z několika částí:

1) Spaltenliste - seznam 17576 trigramů náhodně seřazených do 733 sloupců. Každé komunikační síti byl přidělen určitý blok sloupců.

2) Gruppenliste - abecedně seřazené trigramy se souřadnicemi určujícími sloupec a řádek, na němž se trigram vyskytuje ve Spaltenliste. De facto jde o rejstřík ke Spaltenliste.

3) Devět tabulek, každá sestávající z 676 bigramů jimž jsou náhodně, avšak recipročně, přiřazeny jiné substituční bigramy.

4) Kalendář určující, která z devíti bigramových tabulek má být který den použita.

Přenos klíče zprávy probíhal následovně:

1) operátor náhodně vybral jeden trigram z prostoru přiřazeného jeho komunikační síti ve Spaltenliste a další zcela náhodný trigram.

2) Pokud vybral např. trigramy HNH a PGB, zapsal je posléze způsobem:

HNH

PGB

a doplnil dvěma náhodnými písmeny do podoby:

QHNH

PGBL

3) Takto zapsané dvě čtveřice substituoval po sloupcích podle aktuální bigramové tabulky. Odpovídal-li bigram QP např. bigramu IN, HG odpovídalo DS atd., vznikly substitucí odlišné dvě čtveřice, např.:

IDYB

NSOI

Tyto čtveřice se nazývají indikátor zprávy.

4) Operátor navolil na přístroji příslušné denní nastavení, na klávesnici zadal druhý zvolený trigram PGB a výsledek, který přístroj zobrazil na žárovkové desce, použil jako počáteční pozici rotorů pro odesílanou zprávu. S tímto novým nastavením zašifroval samotnou zprávu.

Šifra byla poté odvysílána v Morseově kódu. Indikátor zprávy IDYB NSOI jí bezprostředně předcházel a často býval pro eliminaci chyb řazen ještě za ni.

Příjemce zprávy nejdříve provedl podle seznamu bigramů sloupcovou substituci a eliminoval dva náhodně přidané znaky. Pomocí prvního trigramu si mohl v Gruppenliste ověřit, zda je zpráva v denním klíči, který má k dispozici, a zda ji tedy bude schopen správně dešifrovat. Pokud ano, zadal druhý trigram na klávesnici přístroje a výsledek, který přístroj zobrazil na žárovkové desce, použil jako počáteční pozici rotorů. S tímto nastavením již mohl zprávu bez problémů dešifrovat.

Je třeba podotknout, že několikrát použité slovo operátor v případě Enigmy ve skutečnosti neoznačovalo jednu osobu. Ve většině případů tvořila obsluhu Enigmy hned trojice operátorů. Pouze jeden z nich s přístrojem přímo pracoval, tj. nastavoval jej a zadával znaky na klávesnici, další odečítal a zapisoval znaky zobrazené na žárovkové desce a konečně třetí obsluhoval přidělenou rádiovou stanici. V celém procesu tak byla velká pravděpodobnost lidské chyby, což vedlo k časté nutnosti zprávu opakovat, a jak známo, jakékoliv opakování či pravidelnost nutně vede k degradaci bezpečnosti šifry [RITTER, 2007].

3.2.4. Polská kryptoanalýza Enigmy

Němci považovali Enigmu za dokonale neprolomitelný systém a vinu na případném vyzrazení zprávy často svalovali na práci špionů ve vlastních řadách nebo porušení pravidel bezpečnosti. Jakkoliv však byla Enigma rafinovaná, neprolomitelná rozhodně nebyla.

Již dávno před válkou, roku 1928, započali polští kryptologové Marian Rejewski, Henryk Zygalski a Jerzy Różycki z oddělení tajné služby Biuro Szyfrów s kryptoanalýzou Enigmy. Nejprve se zacvičili na komerční verzi, a když se polské tajné službě podařilo získat a okopírovat tehdy používanou německou armádní verzi, brzy začali úspěšně luštit první armádní šifry [COPELAND, 2004b, s.235-245].

Hlavní devizou, kterou Poláci získali, byla znalost vnitřního propojení kontaktů v rotorech armádní Enigmy. S tímto základem mohli využít dvou slabin, kterými přístroj trpěl:

1) Pravidelnost pohybu rotorů - s velkou pravděpodobností se vždy na začátku šifrování zprávy pro prvních několik znaků pohyboval pouze pravý rotor a střední a levý zůstával v téže pozici.

2) Raný způsob výměny klíče zprávy - operátor navolil podle knihy denní nastavení, dvakrát po sobě zašifroval náhodně vybraný trigram a ten poslal na začátku zprávy jako indikáror. Pokud byl splněn předpoklad, že střední a levý rotor se v průběhu šifrování indikátoru nepootočil, byl indikátor efektivně zašifrován jednoduchou polyalfabetickou substituční šifrou. Navíc bylo možné těžit ze znalosti, že první a čtvrtý znak šifrového textu v otevřeném textu představuje stejný znak a podobné dvojice tvoří druhý s pátým a třetí s šestým znakem [GAJ, 2003].

Když posléze navíc spolupracující francouzská tajná služba dodala Polákům kódové knihy s tabulkami denních nastavení pro několik týdnů, mohl Rejewski dořešit poslední nejasnosti ohledně fungování systému výměny klíče a v roce 1933 tak polská a francouzská tajná služba četla až 75% německých tajných

zpráv. Zpočátku luštili Poláci s pomocí různých ručních metod vylepšených v roce 1938 použitím tzv. Zygalského archů, což byly archy papíru posouvatelné vůči sobě a perforované v místech, kde bylo možné očekávat tzv. *samice*. Ještě téhož roku však byl princip výměny klíče pozměněn tak, že používání ručních metod se stalo neúměrně časově náročným. To si vyžádalo sestrojení zařízení, kterým by se celý postup zautomatizoval a tím výrazně zrychlil. Zařízení skutečně záhy spatřilo světlo světa a vešlo ve známost jako *bomba* [BAUER, 2000].

Bomba dokázala rekonstruovat klíč zprávy z jejího indikátoru za pomoci tzv. *tahákůů*[17], a při splnění jistých podmínek i bez nich.

1) S tahákem - Tahák je část předpokládaného otevřeného textu. Pro ilustraci zvolme příklad, kdy pro šifrový text začínající znaky NYPN víme, že první a čtvrtý znak odpovídá v otevřeném textu písmenu E. Vyjděme nyní z již dříve zmíněného předpokladu, že se při šifrování těchto čtyř znaků otáčel pouze pravý rotor. Tím můžeme případ zjednodušit na hypotetickou Enigmu s jediným rotorem a v konečném důsledku odvodit pozici tohoto rotoru na začátku šifrování zprávy. Jednoduchou bombu zkonstruujeme spřažením dvou jednoduchých Enigem paralelně k sobě tak, aby rotor druhé z nich byl oproti rotoru první o tři pozice dále[18]. Do obou přístrojů budeme neustále zadávat znak N a ve chvíli, kdy se na displejích zároveň rozsvítí znak E, poznamenáme si pozici rotoru prvního přístroje. Takovýchto stavů může nastat i více než jeden, proto pokračujeme, dokud nedokončíme celou otáčku rotoru. Pokud žádný takový stav nenastal, byl tahák zřejmě chybný. Pokud však jednou nebo vícekrát nastane, vyzkoušíme s těmito nastaveními dešifrovat zbytek zprávy a sledujeme, které z nich produkuje srozumitelný text.

K luštění reálné Enigmy je zapotřebí otáček všech tří rotorů, tedy 26^3 kroků[19], a to při šesti různých pořadích rotorů. Skutečná bomba byla tedy tvořena

[17] angl. "crib"
[18] tj. o vzdálenost mezi prvním a čtvrtým znakem v NYPN
[19] 676 otáček pravého rotoru, 26 otáček prostředního a 1 otáčky levého

třemi paralelně spřaženými páry replik Enigmy. Nešlo samozřejmě přímo o věrné kopie Enigmy, ale o jeden přístroj, který jejich chování emuloval. Všech 26^3 možných nastavení byla bomba schopna projít přibližně za dvě hodiny. Poláci disponovali šesti bombami, a tudíž byli schopni procházet zároveň všech šest možných pozic rotorů.

2) bez taháku s vhodnými indikátory - Tahák nebyl ve skutečnosti potřeba, pokud se v jednom dni podařilo zachytit zprávy s indikátory obsahujícími již zmíněné samice[20]. Jak již bylo řečeno, indikátor zprávy představovalo šest znaků vzniklých zašifrováním opakovaného trigramu.

Vhodně zašifrované indikátory tří zpráv a indikátorové nastavení[21] mohly vypadat například následovně:

indikátor	indikátorové nastavení
WAHWIK	RTJ
DWJMWR	DQY
RAWKTW	HPB

Ač se může zdát zachycení zpráv s takto výhodnými indikátory nepravděpodobné, mezi stovkami zpráv, které byly denně zachytávány, se skutečně běžně nacházely.

Označme nyní pro přehlednost počáteční pozice pravých rotorů na začátku šifrování indikátoru:

P_R - počáteční pozice pravého rotoru při šifrování indikátoru první zprávy

Q_R - počáteční pozice pravého rotoru při šifrování indikátoru druhé zprávy

R_R - počáteční pozice pravého rotoru při šifrování indikátoru třetí zprávy

Víme, že zadání W produkuje stejné písmeno na pozici P_R a P_R+3. Další písmeno[22] je shodně produkováno na pozicích Q_R+1 a Q_R+4. Další pak na R_R+2 a R_R+5.

[20] Z polského "samiczki", pravděpodobně odvozeno od slova "same" tedy "totožné". I britští kryptoanalytici v Bletchley převzali později tento termín, ovšem již bez původní slovní hříčky jako "females".
[21] vysílalo se otevřeně ještě před samotnými indikátory

Dále z pravých písmen indikátorového nastavení můžeme odvodit relativní vztahy mezi P_R, Q_R a R_R. Pokud hodnotu pro P_R, tj. J budeme považovat za základní, pak:

Q_R - P_R+15 (tj. vzdálenost od J do Y)

R_R - P_R+18 (tj. vzdálenost od J do B)

Se znalostí těchto vztahů můžeme konstatovat, že stisk W produkuje dvojice stejný písmen na pozicích P_R a P_R+3, (P_R+15)+1 a (P_R+15)+4, (P_R+18)+2 a (P_R+18)+5; po zjednodušení tedy na P_R a P_R+3, P_R+16 a P_R+19, P_R+20 a P_R+23. Víme tedy, jak nastavit odstupy na jednotlivých pravých rotorech. Správné relativní pozice prostředních a levých rotorů opět získáme z indikátorového nastavení.

Oba prostřední rotory na druhém páru nastavíme o 23 pozic před první pár (tj. vzdálenost od T do Q) a na třetím páru o 22 pozic (tj. vzdálenost od T do P). Podobně levé rotory budou mít odstup 12 na druhém páru a 16 na třetím páru.[23]

Do takto nastavené bomby kontinuálně vkládáme písmeno W a zaznamenáváme pozice, kdy každý ze tří párů produkuje dvojici shodných znaků. Výsledné tři znaky pak odpovídají nastavení jader rotorů na začátku šifrování indikátoru.

Abychom mohli luštit samotný text zprávy, chybí nám však nastavení prstenců s abecedou. To snadno získáme, když prstence při zachování nastavení jader rotorů nastavíme tak, aby se v průzorech zobrazovaly znaky indikátorového nastavení, tj. pro první zprávu RTJ. Správné nastavení prstence rotoru pak přečteme u značky kontaktu vnitřního písmene "A" (příl. 2, č.2).

---

[22] které se může od toho na pozicích P_R a P_R + 3 lišit, protože jde o zcela jinou zprávu pouze se shodným denním nastavením

[23] Rotory v páru oproti sobě nejsou posunuty, jako je tomu u pravých rotorů, protože opět nepředpokládáme, že by se v průběhu šifrování identifikátoru posunuly. Šance tohoto posunu je pouze $\frac{6}{26}$.

Úspěch této metody závisí také na splnění předpokladu, že znaky v indikátorech nebyly pozměněny žádnou substitucí na rozvodné desce. Při předválečném menším množství propojení byla však i tato šance uspokojivá.

Pokud jsme měli štěstí, nastavíme na replice Enigmy údaje, které nám poskytla bomba, a po zadání šifrového textu dostaneme německý otevřený text prokládaný vinou rozvodné desky páry prohozených znaků, jejichž eliminace je s dobrou znalostí němčiny triviální. Pokud kdekoliv v procesu dojde k problému, znamená to buď, že v průběhu šifrování indikátoru došlo k pootočení prostředního nebo i levého rotoru, nebo že do šifrování indikátoru zasáhly substituce skrze rozvodnou desku. Pak nezbývá, než celý proces vyzkoušet s jinou sadou samic, nebo s možným tahákem.

V prosinci 1938 rozšířili Němci počet možných rotorů na 5, čímž se zvýšil počet možných pozic rotorů z 6 na 60. Naštěstí další ukořistěná kniha denních nastavení dovolila Rejewskému rekonstruovat jejich vnitřní zapojení, ovšem i tak šestice bomb, které byly k dispozici, začala za Enigmou zaostávat. Další ranou pro polské bomby bylo zvýšení počtu propojení na rozvodné desce na začátku roku 1939.

Vědomi si toho, že sami již nedisponují proti Enigmě dostatečnými prostředky, svolali Poláci na červen 1939 do vesnice Pyry francouzské a britské kryptology k projednání problému. Poláci jim předali prakticky všechny své poznatky a metody luštění, z nichž některé sice již byly Britům známy, nicméně další se prokázaly být neocenitelnými[24]. Nádavkem předali Poláci zahraničním kolegům i dvě repliky armádní Enigmy s kompletními sadami rotorů [Bletchley Park, 2012].

[24] Například Alfred Dillwyn Knox, který v té době na v britském luštění Enigmy odvedl největší kus práce, nemohl dlouho přijít na to, jak je napojena klávesnice ke vstupnímu statoru. Nejrůznější rafinovaná propojení vycházející z německého rozložení klávesnice nefungovala a britská kryptoanalýza tak na nějakou dobu ustrnula na mrtvém bodě. Až v Pyry se Britové dozvěděli, že kontakty jsou napojeny podle očividného, a tudíž nikým nepředpokládaného vzoru A-A, B-B, C-C atd. [BATEY, 2008].

Po vypuknutí války Rejewski s několika kolegy uprchl do Francie, kde, dokonce i po jejím obsazení, pokračoval ve svém výzkumu a konec války strávil ve Velké Británii.

3.2.5 Britské průlomy Enigmy

Government Code and Cypher School byla v srpnu 1939 přestěhována do prostor bývalé šlechtické usedlosti Bletchley Park, nacházející se přibližně 50 km severozápadně od Londýna. Poloha měla zajistit klid od bombových útoků v nadcházející válce a díky blízkosti obou největších univerzitních komplexů Anglie, Oxfordu a Cambridge, také stálý přísun nových vysoce specializovaných pracovních sil. Čtyři dny po začátku války přibyla do Bletchley první nová krev - Alan Turing, který již rok pro GC&CS pracoval na částečný úvazek, Gordon Welchman, Hugh Alexander a Stuart Milner-Barry [GREY, 2008; DAY, 2004].

S vypuknutím války prudce vzrostl hlad po německých tajných depeších a s tím se rozrostla i veškerá aktivita v Bletchley. Kapacita původních budov byla rychle naplněna, pročež bylo rozhodnuto na přilehlých pozemcích vybudovat několik prefabrikovaných dřevěných staveb. Ty vešly ve známost jako boudy[25] a bylo jich postaveno celkem osmnáct. V roce 1941 k nim přibylo dalších osm zděných budov. Nejdůležitějšími pro průběh války se staly boudy označené čísly 3, 4, 6 a 8. V boudě 6 pracoval tým kryptologů pod vedením Gordona Welchmana na luštění denních klíčů armádní a letecké Enigmy a výsledek svého snažení posílali do sousední boudy 3, kde byly s pomocí klíče dešifrovány zachycené zprávy. Podobný vztah panoval mezi boudou 8, jejíž personál včetně Alana Turinga prolamoval námořní a ponorkovou Enigmu a rutinní práci dešifrování zpráv ponechával na boudě 4 [COPELAND, 2006, s.26; BURNS, 1994]. V průběhu války bylo vypracováno několik způsobů urychlujících předávání zpráv mezi boudami, od posouvání krabice od bot skrze provizorní tunel až po plnohodnotný systém potrubní pošty [DAY, 2004].

[25] angl. "hut"

Všechno úsilí v Bletchley by přišlo vniveč, pokud by Němci pojali podezření, že jejich šifry jsou pravidelně prolamovány. Všichni zaměstnanci byli povinni podepsat a dodržovat Zákon o utajení, který mimo jiné zakazoval mluvit o práci v Bletchley s kýmkoliv mimo vlastní oddělení. Přísaha mlčenlivosti neztratila svou účinnost ani po válce, což vedlo k tomu, že první informace o aktivitách v Bletchley se dostaly na veřejnost až s oficiálním odtajňováním dokumentů v sedmdesátých letech [JANEČEK, 1998, s.43].

Práce na luštění nepřátelské komunikace dostala souborné kódové jméno Ultra, odvisející právě od vysokého stupně utajení.

Britové po poradě v Pyry začali na polském základě vyvíjet systém útoku přímo na šifrový text. Pod vedením Alana Turinga vznikla vylepšená verze polské bomby[26]. Šlo o přibližně dva metry širokou i vysokou skříň obsahující 108 rotujících bubnů emulujících rotory 36 Enigem. Ty byly z druhé strany propojeny složitým systémem kabelů. Na pravé straně konstrukce se nacházelo menu umožňující zadání parametrů [PLIMMER, 1998; Code-breakers, 2011].

Útok byl opět založen na použití taháků, ovšem tentokrát v otevřeném textu zprávy. Turing si správně uvědomil, že vojenská rutina po čase i svědomitého operátora přetvoří ve stereotypní, předvídatelnou bytost, která tíhne nejen k používání lehce odhadnutelných klíčů, ale především ke stereotypní formulaci zpráv. Protože každá zpráva musela obsahovat v nešifrované podobě volací znak odesílajícího i adresáta a vysílací frekvence se měnily pouze sporadicky, bylo možné mít svého operátora dokonale "přečteného". Například pokud bylo známo, že operátor rádiové stanice lodi sledující počasí začínal každou první zprávu daného dne slovy "Wettervorhersage für heute", bylo pro kryptoanalytiky vybavené bombou zjištění klíče pouhou otázkou času.

[26] Zde je třeba rozlišovat polský stroj "bomba" a britský "bombe". Ze stylistických důvodů však budu i britský stroj nadále nazývat jednoduše bomba.

Trvanlivost taháku však nebyla nijak garantovaná a získávání nových se vyvinulo ve svébytné umění provozované především veterány s velkým počtem rozluštěných zpráv na kontě.

Tahák se nemusel vždy nacházet pouze na začátku zprávy. Zde luštitelům pomohla reciprocita Enigmy. Nezávisle na jakýchkoliv nastaveních a vylepšeních Enigma nikdy nedokázala zašifrovat písmeno jako sebe samé. S dostatečně dlouhým tahákem tak bylo možné nalézt pouze několik pozic, na nichž se mohl vyskytovat, prostým porovnáním oproti šifrovému textu.

Pokud jsme si tahákem i jeho polohou dostatečně jisti, můžeme nastavit bombu a počkat si na výsledek. Nastavení a práce s bombou probíhaly následovně:

1) porovnáme otevřený text taháku s šifrou

Pozice:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
OT:	W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E
ŠT:	X	G	P	E	W	T	F	H	E	S	C	Q	C	R	X	S

2) Vytvoříme graf znázorňující vztahy jednotlivých znaků. W je na 1. pozici šifrováno jako X, E na 2. místě jako G, atd. (viz příl. 4). V kroužcích jsou vepsána písmena taháku i šifrového textu a ve čtvercích pozice, na níž se substituce jednoho písmene za druhé odehrává. Díky reciprocitě Enigmy platí vztah vždy oboustranně. Všimněme si, že v grafu se nám vytvořilo několik smyček, jmenovitě RTE, WEGX, ESC. Tyto smyčky dokáží výrazně přispět k rychlé eliminaci mnoha nevyhovujících nastavení rotorů.

3) Z grafu vytvoříme zapojení na menu bomby a stroj spustíme. Pokud jsou všechny podmínky dané grafem splněny, bomba zaznamená nastavení rotorů, které k tomu vedlo, a pokračuje dál.

4) Nastavení rotorů, která bomba vyhodnotila jako vyhovující, jsou ručně přezkoušena na celém textu zprávy, přičemž jedno z nich nakonec vyjde jako správný denní klíč.

Závěrečný problém představuje rozvodná deska. Její vinou nemusí výsledky, které bomba poskytne, odpovídat skutečnému dennímu nastavení. Proto Turing zakomponoval do celého procesu dodatečnou abstraktní vrstvu, která nepracuje přímo s písmeny, nýbrž s jejich propojkovými hodnotami. Propojková hodnota písmene může být kterékoliv z 26 písmen abecedy, avšak pokud vezmeme v úvahu relativní vztahy mezi znaky, dané opět především smyčkami v grafu, můžeme s trochou snahy zpětně rekonstruovat zapojení celé rozvodné desky [ELLSBURY, 2007].

Bomby však na počátku války nemohly být vyráběny v dostatečných počtech, které by odpovídaly nárůstu komunikace na německé straně a průběžným inovacím Enigmy. Na výrobu miniaturních mechanických součástek, které byly k jejich konstrukci zapotřebí, nebyly továrny Spojenců uzpůsobeny. Švýcarsko, které naopak bylo na tomto poli specialistou, bylo co do dodávek jemné mechaniky v područí Německa. Bylo tedy nutné vytvořit rozsáhlou pašeráckou síť, která byla pod taktovkou Johna Lomaxe schopna ze Švýcarska dodávat mikrošrouby, ložiska i nástroje k jejich výrobě [PIEKALKIEWICZ, 2004, s.382; URNER, 2002, s.124]. Do roku 1943, kdy již byly bomby vyráběny a provozovány po desítkách, bylo tedy zapotřebí ušetřit co nejvíce strojového času. To zajistila Turingova ruční metoda zvaná Banburismus[27]. Ta vycházela ze starších polských ručních metod a snažila se porovnáváním zpráv s podobnými indikátory určit správné nastavení pravého a prostředního rotoru.

Práce kryptologů by byla o mnoho složitější, pokud by se tu a tam neopakovaly šťastné náhody, ne nepodobné těm z první světové války. Způsob výměny klíče zprávy popsaný v kapitole 3.2.3 se dal díky použití náhodně uspořádaných bigramů považovat za velmi bezpečný. Pokud chtěli kryptologové v Bletchley luštit námořní Enigmu, bylo třeba tyto tabulky za každou cenu získat. To se

[27] Odvozeno od města Banbury, kde se vyráběly archy potřebné pro tuto metodu.

podařilo v dubnu 1940, kdy byla zajata německá loď poblíž norského Narviku, a o rok později další u břehů Lofot. Obě nesly na palubách aktuální verzi K-Buch a manuály, jejichž analýza potvrdila Turingovu představu o fungování celého systému [ERSKINE, 2008].

Na počátku roku 1942 však německé ponorky začaly používat čtyřrotorovou Enigmu M4, známou v Bletchley jako Shark. Luštění ponorkové komunikace bylo pro Británii záležitostí rozhodující o přežití. Konvoje zásobovacích plavidel proudící z USA byly v Atlantiku "vlčími smečkami" německých ponorek vytrvale decimovány již v letech 1940 a 1941. Poté, co Britové začali Spojence na základě informací z ponorkové Enigmy informovat o poloze ponorek, mohly být konvoje průběžně odkláněny mimo nebezpečnou zónu. Nechat znova vypuknout ponorkovou blokádu tedy vůbec nepřipadalo v úvahu. Pomohla opět až šťastná náhoda - zajetí ponorky U-110 u Islandu, které poskytlo nový manuál a dostatečnou zásobu taháků pro luštění M4 [KAHN, 1991, s.125-131; COPELAND, 2004b, s.259-261; BURNS, 1994].

Se zažehnanou ponorkovou hrozbou už Turing jako teoretik neměl v Bletchley dostatek problémů, kterými by se mohl zabývat. V prosinci 1942 odcestoval do USA, kde pomáhal s konstrukcí rychlejších čtyřrotorových bomb. V Bletchley ještě vyvinul ruční metodu prolamování stroje Lorenz SZ40 a v roce 1943 odešel do Hanslope Park pracovat na automatickém šifrování řeči. Jeho bomba však žila dál vlastním životem a na konci války bylo v provozu 152 třírotorových a 180 čtyřrotorových bomb v USA a Velké Británii [ALEXANDER, 1945, s.56; LEE, 2000].

3.3. Dálnopisné stroje

Odhlédneme-li od faktu, že Enigma byla za války nepřítelem vcelku pravidelně luštěna, byla pro původní strategii Třetí říše, tj. bleskovou válku, jako stvořená. Malý přenosný aparát, který nevyžadoval po obsluze žádné zvláštní znalosti, se ukázal být výborným řešením tajné komunikace přímo v poli. Větši-

nou dvou- až třísetznakové zprávy pro taktické účely bohatě postačovaly. Jakkoliv měli Němci Enigmu za neprolomitelnou, pro komunikaci na vyšší strategické úrovni se rozhodli používat jiné, bezpečnější stroje. Německou důvěru v nové stroje odráží i jejich domácí označení - Geheimschreiber.

3.3.1 Lorenz SZ40 vs. Colossus

Ve větší míře byly nasazeny dva typy strojů, kombinující některé charakteristiky Enigmy s dálnopisem. Prvním z nich byl Lorenz SZ40, v Bletchley známý jako Tunny. Stroj měl 12 rotorů, které se však nepodílely na samotném šifrování, nýbrž pouze na vytváření pseudonáhodného klíče, který byl později binárně přičten k otevřenému textu zprávy.

Celý stroj narozdíl od Enigmy pracoval s binární reprezentací znaků v Baudot-Murrayho kódování používaného v dálnopisné komunikaci. To reprezentuje každý znak pomocí pětice bitů zaznamenaných do děrné pásky (viz příl. 5). Lorenz byl pouze přídavným nástavcem k dálnopisu, který přebral pásku s otevřeným textem, přičetl k ní klíč vygenerovaný na rotorech a hotovou šifru poslal skrze radiostanici do éteru.[28] Klíč se ke zprávě přičítal prostřednictvím logické funkce výlučného logického součtu známé jako XOR, či též modulo 2. Tato metoda, zamýšlená již Vernamem pro one-time pad, má opět výhodu v reciprocitě. Pokud ke zprávě přičteme klíč, vznikne šifra. Pokud stejný klíč přičteme k šifře, vznikne původní zpráva.

Rotory SZ40 byly rozděleny do tří skupin - ψ-rotory, χ-rotory a μ-rotory[29]. Všechny měly vůči sobě navzájem nesoudělné počty pozic[30], což maximalizovalo nejdelší možnou periodu klíče. Každá pozice na rotoru měla vlastní vačku nastavitelnou do dvou poloh reprezentujících jeden bit. Pět χ-rotorů se společně otočilo o jednu pozici po každém zadaném znaku. Otočení pětice χ-rotorů závi-

[28] Z toho plyne další rozdíl oproti Enigmě - potřeba pouze jednoho operátora, a tím i minimalizace možnosti lidské chyby.
[29] Tedy psí, chí a mí - označení pomocí písmen řecké abecedy ovšem zavedli až v Bletchley
[30] 43,47,51,53,59,37,61,41,31,29,26,23 - navíc tedy viditelně vyšší počty než Enigma

selo na dvou μ-rotorech, z nichž pohyb jednoho byl závislý na aktuální pozici druhého. Výsledný klíč pak byl vypočítán jako XOR pěti bitů na ψ-rotorech s pěti bity na χ-rotorech.

Nastavení vaček na rotorech bylo měněno podle knih denních nastavení, na ψ- a χ-rotorech jednou měsíčně a na μ-rotorech denně. Klíč zprávy tvořilo podobně jako u Enigmy počáteční nastavení všech dvanácti rotorů [GOOD, 1945, s.5-15; ZORPETTE, 1987].

Lorenz SZ40 byl vyhrazen pro komunikaci na nejvyšší úrovni strategického plánování, tedy především mezi vrchním velením v Berlíně a lokálními velitelstvími jednotlivých armád. Proto počet aktivních komunikačních linek v průběhu války nepřesáhl 26 [COPELAND, 2004b, s.40]. Každá z linek dostala v Bletchley krycí jméno podle druhu ryby (viz příl. 6), přičemž celá komunikace pomocí dálnopisných strojů obdržela jméno Fish.

První zpráva zachycená Brity v červnu 1941 pocházela z experimentální linky Berlín-Atény. Nezvyklý typ rádiového provozu ihned upoutal pozornost kryptologů. Zpočátku zdánlivě neprolomitelný systém poprvé selhal v srpnu 1941, kdy německý operátor poslal dvě podobné zprávy se stejným počátečním nastavením.[31] Z nich dokázal kryptoanalytik John Tiltman rekonstruovat klíč, z něhož se na počátku roku 1942 jeho kolegovi Williamu Tuttovi podařilo rekonstruovat systém tvorby klíče. Se znalostí principu pohybu rotorů vypracoval Turing ruční metodu odhalování nastavení vaček rotorů, tedy denního klíče. Pro Tunny byla vyhrazena celá sekce pod vedením majora Ralpha Testera, nazvaná

[31] Tento kryptografický prohřešek je znám jako "zprávy v hloubce". Na začátku máme otevřené texty M_1, M2, šifrové texty E_1, E_2 a stejný klíč K.
$M_1 \oplus K=E_1$; $M_2 \oplus K=E_2$
Klíč je možné díky charakteru funkce XOR eliminovat a pracovat pouze s otevřenými a šifrovými texty.
$M_1 \oplus M_2=E_1 \oplus E_2$
Zkoušením taháků na otevřený text M_1 a sledováním čitelnosti textu M_2 můžeme jednoznačně určit původní zprávy.
$(M_1 \oplus M_2) \oplus M_1=M_2$
Při znalosti M_1 a E_1 je pak jednoduché zrekonstruovat klíč jako
$K= M_1 \oplus E_1$

Testery, kde probíhalo luštění výhradně za pomoci ručních metod. Z Testery pocházely i patrně nejužitečnější rozluštěné zprávy týkající se plánů německé ofenzivy, která vedla k bitvě u Kurska. Ta měla pro Němce znamenat obrat ve válce a znovuzískání kontroly nad východní frontou. Britské informace však zajistily Rusům dostatečný čas na přípravy a pro Němce se bitva stala fatálním debaklem.

S narůstajícím provozem a několika bezpečnostními vylepšeními vyvstala potřeba část práce Testery automatizovat. Za tímto účelem byla v červenci 1943 vytvořena sekce Newmanry pod vedením matematika Maxe Newmana. První stroj, který stavěl na Tuttových teoriích, byl pojmenován Heath Robinson, avšak nebyl příliš spolehlivý. Jeho zdokonalení se ujal inženýr Thomas Flowers, který pak během 11 měsíců navrhl a zkonstruoval první elektronický digitální programovatelný počítač v historii [SALE, 1995; SALE 2004]. Stroj dostal jméno Colossus a byl spuštěn v prosinci 1943. Colossus pracoval bez problémů a pětkrát rychleji než Heath Robinson. Skládal se z čtecího mechanismu, kterým rychlostí 5000 znaků za sekundu procházela děrná páska s šifrovým textem, 1500 elektronek tvořících logický obvod programovatelný pomocí menu, a žárovkového displeje zobrazujícího průběžný výsledek programu [ANDRESEN, 2001; PLIMMER, 1998]. Byť museli zaměstnanci Testery stále odvádět velkou část práce ručně, Colossus poskytl natolik výrazné zefektivnění celého procesu, že bylo rozhodnuto o výrobě dalších čtyř strojů. Ty měly být hotovy do 1. června následujícího roku - předpokládaného data počátku spojenecké invaze na evropský kontinent. To se sice ukázalo jako nereálné, avšak jeden další zdokonalený model byl opravdu do tohoto data dokončen [COPELAND, 2004a].

Den D znovu dokázal neocenitelnost zpráv z Tunny. Nejenže Spojenci měli přesné informace o rozložení německých sil v Normandii, ale navíc se potvrdil úspěch operace Fortitude - klamného manévru, který měl Němce přesvědčit, že vylodění proběhne v Norsku a v Calais [CARTER, 1997].

3.3.2 Siemens und Halske T52 vs. Arne Beurling

Dalším dálnopisným strojem používaným pro utajenou komunikaci byl Siemens und Halske T52. Byl používán především při komunikaci s okupovanými územími, což byl i případ Dánska a Norska, které Němci obsadili 9.4.1940. Švédsko, které nadále zůstávalo neutrální, bylo požádáno o pronajmutí kabelu, který by umožnil dálnopisný provoz mezi Berlínem a Norskem. Švédi, vědomi si toho, že záporná odpověď by mohla mít dalekosáhlé důsledky, souhlasili, avšak při první příležitosti začali německé zprávy odposlouchávat. Z odposlechů se dozvěděli o chystaném nasazení Geheimschreiberu a zanedlouho se komunikace skutečně stala nečitelnou. Švédsko, země náhle obklíčená ze všech stran rozpínající se Třetí říší, si nemohlo dovolit neznat plány potenciálního nepřítele.

T52 byl vyvinut v letech 1929-1932. Narozdíl od SZ40 nešlo pouze o přídavné zařízení, nýbrž o řešení "vše v jednom" - přístroj obsahoval jak dálnopis, tak šifrovací mechanismus. To si vyžádalo daň v podobě 100kg hmotnosti, které přístroj předurčovaly k stacionárnímu použití; i tak však dosáhl daleko většího rozšíření než SZ40. Vyrobeno bylo přibližně 600 kusů, které používaly jak velitelství všech složek ozbrojených sil, tak konzuláty v okupovaných a neutrálních zemích. Stroj obsahoval deset rotorů, z nichž pět generovalo klíč přičítaný k otevřenému textu podobně jako SZ40, ovšem zbylých pět výsledek navíc na bitové úrovni transponovalo. Po každém stisku klávesy se všechny rotory, každý s jiným počtem pozic, o jeden krok otočily. Nastavení probíhalo pomocí tzv. QEK a QEP čísel. V knize denních nastavení byla pro pět z rotorů předvyplněna povinná QEK čísla a výběr zbylých pěti, QEP čísel, byl ponechán na operátorovi. Ten pak zvolená QEP čísla zaslal otevřeně před začátkem šifrování. Výměna klíče nebyla třeba pro každou jednotlivou zprávu. T52 fungoval duplexně, tzn. po navázání kontaktu se přístroje na obou stranách udržovaly synchronizované a celá komunikace se nevítanému naslouchajícímu jevila jako jediná nepřerušovaná zpráva [BECKMAN, 2002, s.65-86; DAVIES, 1994].

O zachytávání zpráv se staral švédský Telecom, který jimi zásoboval kryptoanalytiky v jednom z oddělení Obranného štábu[32]. Zde jako poradce pracoval i Arne Beurling, profesor matematiky na uppsalské univerzitě. Poté co si na nové německé šifře vylámalo zuby několik jeho kolegů, byl úkol přidělen jemu. Beurling měl bohaté zkušenosti s prolamováním superšifrovaných sovětských kódů. Brzy si uvědomil komplexnost mechanismu produkujícího šifru a rozhodl se spolehnout na pomoc ze strany operátorů přístroje, tedy na jejich případné kryptografické prohřešky. Zachycené zprávy obsahovaly i nešifrované hovory operátorů sloužící k ověření prostupnosti linek před začátkem šifrování. Linky byly nespolehlivé a komunikace trpěla silným šumem, který přístroj často sám interpretoval jako přepnutí do registru číslic (viz příl. 5). Operátoři si proto zvykli vkládat do zpráv množství redundantních znaků pro přepnutí na registr písmen, obzvláště často ve spojení se znakem mezery. Dále často opakovali frázi "QRV?", obdobu "jak mě slyšíte?", kterou Beurling znal z nešifrovaných hovorů. Ani při volbě QEP čísel nebyli operátoři příliš svědomití. Přístroj obsahoval páku, která resetovala QEK rotory do jejich startovních pozic, a operátoři brzy přišli na to, že pokud všechny rotory označí jako QEK, nemusí je pokaždé nastavovat ručně. To zajistilo Beurlingovi bohatý přísun zpráv v hloubce. S pomocí dvou univerzitních kolegů, Bertila Nymana a Hanse Ruberga, během dvou týdnů pouze s použitím ručních metod rekonstruoval princip T52 a sepsal podklady ke konstrukci stroje, který dokázal T52 emulovat. Přesný charakter tohoto výjimečného kryptoanalytického výkonu Beurling nikdy neprozradil. Dokonce ani naléhání švédské tajné služby v sedmdesátých letech nedostalo z Beurlinga, tehdy profesora na Princetonu, nic víc, než že "Kouzelník své triky nikdy neodhaluje". Prozradil pouze, že "roli hrály trojky a pětky", což byly švédské ekvivalenty pro znaky mezery a přechodu na rejstřík písmen. Z toho je možné usuzo-

[32] Försvarsstaben - jedno z oddělení ministerstva obrany, dnes známé jako FRA

vat, že právě přehnaná snaha operátorů o čitelnost textu u legitimního adresáta nevědomky způsobila degradaci šifry[33] [BECKMAN, 2002, s.xi].

Jakýkoliv však byl postup, důležité byly výsledky. Švédi po tři roky četli tajné německé depeše proudící do Norska i Finska a zčásti i díky správnému využití získaných informací si mohli dovolit zůstat po celou válku neutrální zemí. Naneštěstí bezpečnostní opatření nedosahovala britské úrovně a tento fakt se nakonec donesl Němcům. Proto byl v roce 1943 uveden nový typ T52d, který se lišil především nepravidelností chodu rotorů a na nějž byly metody vypracované Beurlingem krátké.

3.4 Spojenecké šifry

Spojenci rovněž spoléhali na elektromechanické šifrovací stroje. Ty stavěly z velké části na principech Enigmy, ovšem netrpěly většinou jejích chyb.

Britský Typex využíval pět rotorů a reflektor. První dva rotory byly statické a plnily podobnou funkci jako propojovací deska Enigmy. Operátor mohl vybírat z deseti rotorů, které měly různý počet zářezů pro posun. Navíc byly některé rotory rozložitelné, takže bylo možné vyjmout jádro a vložit jej do jiného prstence. V průběhu války se vyrábělo několik typů: stacionární Typex Mark II, Typex 22 a 23, které byly napájeny ze sítě a disponovaly dvěma tiskárnami, jednou pro otevřený a druhou pro šifrový text. Přenosné varianty Typex Mark III a VI byly poháněny klikou a tiskly pouze šifrový text. Od roku 1937 do 1945 bylo vyrobeno okolo 12000 strojů [ERSKINE, 1997; ERSKINE 2002].

Američané rovněž uvedli do provozu vlastní stroj v roce 1937. Hlavní devizou zařízení pojmenovaného ECM Mark II s kódovým jménem SIGABA byl nepravidelný pohyb rotorů. První verze, navržená Williamem Friedmanem, ředitelem armádní kryptoslužby, využívala k řízení chodu rotorů děrnou pásku,

[33] To prezentuje zajímavý psychologický problém. Např. u Enigmy, kde operátor viděl šifrový text, byla větší šance, že si uvědomí svou případnou chybu při jeho tvorbě. Pokud však celá práce operátora spočívá pouze v psaní a čtení otevřeného textu a o celý proces šifrovaní a dešifrování se stará stroj, má operátor větší tendenci porušovat kryptografickou morálku a chovat se v utajované zprávě stejně jako v běžné nešifrované komunikaci.

která se však často trhala. S řešením přišel jeho kolega Frank Rowlett, který navrhl řízení šifrovacích rotorů pomocí další sady rotorů. Finální verze stroje obsahovala 15 rotorů ve třech skupinách - 1.-5. a 6.-10. shodně o 26 pozicích a 11.-15. pouze o 10 pozicích. Prvních pět obstarávalo samotnou substituci, podobně jako tři rotory Enigmy, avšak nevyužívaly reflektor. Rotory 6-10 při každém stisku klávesy dostaly impulzy do čtyř kontaktů. Tyto rotory byly na třetí sadu napojeny v 10 skupinách po 1-6 kontaktech. Z třetí sady se vynořilo 1-4 elektrických impulzů, které pak otočily příslušnými rotory z první sady. Všechny rotory byly plně nastavitelné a první a druhá sada byla vzájemně zaměnitelná. Tento komplexní krokovací mechanismus zajišťoval natolik dokonalou ochranu, že systém nebyl až do svého vyřazení ze služby v roce 1959 nikdy prolomen. Podobně jako Typex i SIGABA obsahoval tiskový mechanismus a byl vzhledem ke své hmotnosti používán především stacionárně nebo na bitevních lodích [PROC, 2012].

Brzy vyvstala potřeba vzájemné komunikace mezi Británií a Amerikou, avšak detaily konstrukce ECM podléhaly přísnému utajení. Bylo tedy rozhodnuto o výrobě přídavných zařízení řešících nekompatibilitu ECM a Typexu. Modifikované přístroje byly pak známy pod společným názvem CCM[34] [MACKINNON, 2005].

Podobně jako Němci, i Američané vycítili potřebu šifrovat dálnopisnou komunikaci. V roce 1943 bylo uvedeno do služby dálnopisné přípojné zařízení M-228, přezdívané SIGCUM, které bylo opět dílem Friedmana a Rowletta. Šlo o méně komplikovanou variaci na Lorenz SZ40, která obsahovala pouze pět rotorů s poměrně pravidelným chodem, což bylo kompenzováno využitím více vodičů v jednom kroku a jejich následným dělením do skupin podobně jako u ECM.

Kromě dosud zmíněných rozměrných a tedy stacionárních strojů byly i spojenecké jednotky v poli vybaveny šifrovacími zařízeními. Nejjednodušším byl

[34] Combined Cypher Machine

M-94, sestávající z 25 hliníkových disků na společné ose. Každý disk měl na obvodu vyrytu jinak uspořádanou 26-znakovou abecedu. Šifrování probíhalo prostým otočením disků tak, aby na jednom z řádků byla zobrazena 25 znaků dlouhá zpráva a jako šifrový text byl použit jakýkoliv jiný řádek. Příjemce nastavil disky na svém zařízení do polohy specifikované šifrovým textem a otevřený text se zobrazil na některém jiném řádku.

Poněkud sofistikovanějším přístrojem byl M-209, vyvinutý švédským kryptografem Borisem Hagelinem. Šlo o ručně poháněný čistě mechanický stroj s šesti rotory o nesoudělném počtu pozic. Každá pozice na rotoru byla podobně jako u SZ40 osazena nastavitelnou vačkou. Další součástí byl otočný válec sestávající z 27 posuvných táhel s nastavitelnými zarážkami. Vačky v aktivní poloze interagovaly se zarážkami v aktivní poloze, načež válec zafungoval jako ozubené kolo o 0-27 zubech a pootočil kolem, které tisklo znak šifrového textu. Znak otevřeného textu se volil pomocí otočného knoflíku a rotory se po každém zašifrovaném znaku otočily o jednu pozici. Celkem bylo vyrobeno přibližně 140000 strojů [REUVERS, 2012]. Navzdory kompaktním rozměrům 8×14×18cm, hmotnosti nepřevyšující 3kg a relativně jednoduché obsluze nabízel M-209 výbornou bezpečnost plně postačující pro taktickou komunikaci [CHURCHHOUSE, 1993].

Kromě šifer bylo využíváno nespočet kódů, z nichž nad ostatní vyčnívá koncept obecně známý díky kódu Navajo. Kvůli izolovanosti indiánských jazykových rodin a absenci jejich psané podoby bylo prakticky nemožné, aby nepřítel disponoval jejich znalostí. Americké ozbrojené síly využívaly hned několik indiánských jazyků v roli kódů, avšak jazyk kmene Navajo se ukázal být co do komplikovanosti gramatiky a dostupnosti rodilých mluvčích ideálním. Kód sestával z přibližně 600 výrazů, které substituovaly termíny neznámé pro původní jazyk pomocí opisů[35]. Výrazy neobsažené v kódu byly hláskovány pomocí kó-

[35] Např. "tank" byl označován jako "želva", "artilerie" jako "velká zbraň", "samopal" jako "malá rychlá zbraň", atd.

dové abecedy podle prvního písmene anglického překladu navažského slova.[36] Bez znalosti kódových označení a principu abecedy se i rodilému mluvčímu navažštiny zpráva jevila pouze jako nesrozumitelný proud slov [Navajo Code Talkers Foundation, 2012]. Podobné uplatnění našli například i rodilí Baskové sloužící v americké armádě. Jak bylo řečeno, kryptoanalýza kódu se podobá rekonstrukci neznámého jazyka. Pokud je však jazyk natolik odlišný od všeho, co je kryptoanalytikovi známé, je i otevřeně vysílaná zpráva nerozluštitelná.

3.5 Německá kryptologie a její srovnání se spojeneckou

Z předchozích kapitol by bylo možné usoudit, že německá kryptologie byla na nižším stupni než spojenecká. Do jisté míry je toto tvrzení pravdivé, avšak v průběhu války nevypadala situace z německého úhlu pohledu nijak tragicky. Enigma fungovala, a byť se občas objevilo podezření stran jejího prolamování, nebylo až do odtajnění materiálů dlouho po válce plně potvrzeno. Také na německé straně byly konstruovány první složitější stroje, které můžeme označit jako počítače. Hlavním konstruktérem byl Konrad Zuse, který již v polovině třicátých let sestrojil binární čistě mechanický počítač Z1. Z2, Z3 a Z4 následovaly již ve válečných letech a využívaly elektrických obvodů sestavených z relé. Jejich nemalý potenciál však nebyl soustředěn na kryptoanalýzu, nýbrž na problémy leteckého inženýrství.

Byla to zvláště německá kryptoanalýza, která nedosahovala úrovně Spojenců, a to hned z několika důvodů, které sumarizoval ve své přednášce David Kahn [National Security Agency, 1995]:

1) Třetí říše po celou válku nevybudovala jednotnou kryptologickou agenturu. V USA fungovaly dvě agentury (armádní SIS[37] a námořní OP-20-G[38]), v Británii se vše odehrávalo v režii Government Code and Cypher School. V Ně-

[36] pro zakódování písmene A se tak daly použít výrazy "Wo-La-Chee" (ant), "be-la-sana" (apple), "tse-nill" (ax) a mnohé další.
[37] Signals Intelligence Service
[38] Office of Chief Of Naval Operations (OPNAV), 20th Division of the Office of Naval Communications, G Section / Communications Security

mecku existovalo hned několik agentur zabývajících se kryptografií a kryptoanalýzou. Každá složka ozbrojených sil spravovala přinejmenším jedno vlastní kryptoodělení a další podléhaly například poštám. Málokdy probíhala výměna informací či dokonce spolupráce. Naopak, každé oddělení si před ostatními své případné úspěchy chránilo, aby se jimi mohlo samo zavděčit pohlavárům. Větší úspěchy slavila pouze námořní služba známá jako B-Dienst[39]. Jejím zaměstnancům se podařilo prolomit britský námořní kód a několik dalších méně důležitých kódů a šifer. Luštění strojů formátu Typexu však po šesti týdnech snažení vzdali s odůvodněním, že jde o neproveditelný úkol [FLICKE, 1994, s.145-161].

2) Spojenci mohli soustředit síly na dva německé stroje, které nesly největší díl zásadních zpráv. Němci naproti tomu museli luštit mnoho různých spojeneckých šifer a kódů.

3) Narozdíl od Enigmy, která byla před válkou volně komerčně dostupná, podléhaly všechny informace o spojeneckých strojích od počátku přísnému utajení.

4) Spojenecké stroje byly oproti Enigmě vývojově o generaci dále. Mohly proto stavět na jejích základních principech a zároveň se vyvarovat slabin.

5) Systém spojeneckých indikátorů využíval pokročilejší postupy. Útok se znalostí taháku, nebo délky zprávy komplikovaly často používané klamače.

6) Celková populace spojenců byla větší. Státy Osy byly v roce 1940 domovem přibližně 260mil. obyvatel, kdežto spojenecké území[40] obývalo 990mil. lidí. Tím byla větší i šance výskytu geniálních odborníků typu Turinga, Tutta, Shannona atd.

7) O velkou část odborníků se sami Němci připravili vyloučením Židů a dalších skupin z veřejného života. Max Newman jako žid nebo Alan Turing jako homosexuál by v podmínkách Třetí říše byli bez ohledu na své schopnosti ne-

[39] Beobachtungsdienst
[40] včetně tehdy ještě neválčících USA a Sovětského svazu

zaměstnatelní. Nacistická ideologie v tomto smyslu pracovala proti nacistům a je možné, že potenciální "německý Turing" zemřel nepovšimnut v koncentračním táboře.

8) Německá doktrína bleskové války spíše než na znalosti protivníka získané z dešifrované rádiové komunikace spoléhala na překvapivé nasazení masivní síly. Pro Spojence jakožto zpočátku defenzivní stranu bylo otázkou přežití vědět, kdy a odkud nepřátelský útok čekat. S postupným ustálením front na přelomu let 1941-1942 a vstupem USA do války neměla již nedorostlá německá kryptoanalýza šanci dohnat spojenecký náskok.

9) V posledních letech války začali spojenci budovat čistě elektronické, tedy rychlejší a univerzálnější kryptoanalytické stroje, zatímco Němci stále spoléhali na elektromechanickou kryptografii. Zuseho stroje, které snad měly potenciál se nakonec oprostit od mechanické části, zůstávaly kryptologicky nevyužité [DAVIES, 1993].

Kahn věnuje pozornost i samotné otázce Enigmy. Proč Němci nebyli schopni vzít vážně v úvahu, že by jejich nejrozšířenější šifra mohla být prolamována? Pokud existovala podezření, proč nebyly učiněny patřičné kroky?

1) Podezření existovala hlavně na nižší úrovni, především mezi operátory, kteří se strojem denně pracovali, a nikdy se nedostalo k lidem, kteří by mohli na věci cokoliv podstatného změnit. V totalitním režimu mají lidé zodpovědní za funkčnost systému tendenci zamlčovat jeho případné chyby před vedením, protože chyba je může snadno dovést před popravčí četu.

2) Nahrazení Enigmy bylo pro Němce zcela nepředstavitelné z důvodu jejího rozšíření. Při celkovém množství vyrobených přístrojů odhadovaném na 100000 [Cipher machines, 2012] by jejich nahrazení novým systémem bylo logisticky takřka nemožné. Výměna by musela proběhnout ve velmi krátkém čase, aby nebyl nový systém kompromitován přeposíláním zpráv pomocí Enigmy.

3) V průběhu války byla postupně zaváděna vylepšení, která měla zabránit kompromitaci šifry s nárůstem počtu zpráv (viz závěr kapitoly 4). Konstruktéři měli tato opatření za dostatečná a stroj tak měl zůstat neprolomitelný.

4) Němci si se zkušeností ze svých kryptoanalytických služeb nedokázali představit, že by spojenci vytvořili natolik silnou spolupráci mezi svými službami, aby mohli vést dostatečně soustředěný útok proti německým šifrám. Americko-britská spolupráce na bombách a dalších pomůckách pro luštění by německé kryptology uvyklé vzájemné řevnivosti a tajnůstkářství velmi překvapila.

5) Němcům se nikdy nedostalo žádného přímého důkazu, že by byly šifry prolamovány. Spojencům se vždy podařilo vykonstruovat jiný důvod, na nějž mohl nepřítel svalit vinu. Pokud například byla pomocí dešifrace Enigmy lokalizována ponorka, bylo před odkloněním konvojů na místo vysláno "náhodné" hlídkové letadlo, které v očích nepřítele získalo polohu ponorky standardním způsobem.

4. Shannonovy teoretické závěry

Druhá světová válka přinesla do kryptologie nový trend. Zatímco předtím našli při luštění šifer využití spíše lingvisté a jednotlivé šifry byly luštěny případ od případu, v průběhu války se začala vynořovat nutnost položit kryptologii jako vědě obecné teoretické základy. To byl úkol pro matematiky, kteří mohli stavět na základech položených např. Georgem Boolem, nebo Kurtem Gödelem. Jednou z cest se vydal i Alan Turing, který po válce dále rozvíjel myšlenku tzv. univerzálního Turingova stroje, tedy počítače schopného provádět jakékoliv spočitatelné operace [ATHERTON, 1989; LEAVITT, 2007, s.53-58]. Své koncepty nakonec aplikoval v praxi při návrhu prvního počítače s programem uloženým v paměti. Skutečný základní kámen v podobě teorie informace však přinesl až americký kryptolog a matematik Claude Elwood Shannon.

Shannon v průběhu druhé světové války působil v Bellových laboratořích a ve Výboru pro národní obranný výzkum[41]. Hlavním polem jeho činnosti byl vývoj systémů pro zaměřování střelby a kryptologický výzkum. Na počátku roku 1943 se setkal s Alanem Turingem, s nímž sdílel zájem o problém automatického šifrování řeči. S koncem války žádal NDRC výsledky v podobě shrnující publikační činnosti. Shannon připravil zprávu "A Mathematical Theory of Cryptography", která byla po odtajnění v roce 1949 publikována v Bell System Technical Journal pod názvem "Communication Theory of Secrecy Systems" [ROGERS, 1994]. Roku 1948 publikoval článek "A Mathematical Theory of Communication", který s spolu s výše zmíněným prakticky položil základy moderní teorie informace. Zde jsou poprvé zmíněny fundamentální termíny jako entropie systému, kapacita přenosového kanálu, apod. [SHANNON, 1948].

[41] National Defense Research Committee (NDRC), komise zodpovědná za dohled nad veškerým základním výzkumem s potenciálním válečným využitím

V Communication Theory of Secrecy Systems se Shannon zabývá obecnou matematickou strukturou a vlastnostmi utajovacích systémů. Nejprve charakterizuje základní typy utajovacích systémů:

1) zastírací systémy - snaží se o utajení samotné existence zprávy, tj. steganografie;

2) soukromé systémy - spoléhají na technické vybavení, např. inverze nahrávky hlasu;

3) pravé utajovací systémy - transformují zprávu pomocí šifry nebo kódu do podoby, v níž není nepříteli bez znalosti patřičného klíče čitelná.

Vzápětí předesílá zaměření článku pouze na třetí jmenovanou skupinu systémů. Tuto skupinu dále omezuje na systémy s konečnou množinou diskrétních prvků (tzn. jakoukoliv abecedou s konečným počtem symbolů) pro tvorbu zpráv. Každý z těchto prvků má v jazyce zprávy jistou pravděpodobnost výskytu. Přirozené jazyky mají vlastnost důležitou pro utajovací systémy - redundanci. Redundance jazyka vyjadřuje, jak velká část textu může být vypuštěna, aniž by text ztratil svůj původní smysl, tj. stal se nečitelným.

Pravý utajovací systém definuje jako množinu transformací množiny všech možných zpráv do množiny všech možných jim odpovídajících kryptogramů. Každá z těchto transformací odpovídá šifrování konkrétním klíčem *i*. Kryptogram E je tedy aplikací konkrétní transformace T_i na zprávu M:

$E= T_i(M)$

Transformace musí splňovat podmínku reverzibility, tj. pro každou transformaci T_i musí existovat T_i^{-1} taková, že její aplikací na kryptogram dostaneme původní zprávu:

$M= T_i^{-1}(E)$

To při znalosti konkrétní transformace, tj. klíče, umožňuje jednoznačné dešifrování kryptogramu.

Proces přenosu zprávy v univerzálním utajovacím systému popsal Shannon na diagramu uvedeném v příloze 7. Zpráva od svého původce prochází šifrova-

cím mechanismem, který na ni aplikuje transformaci T_K, tedy konkrétní transformaci podle klíče K. Klíč je generován zdrojem klíče, který však musí být schopen dodat stejný klíč oběma stranám, a to pomocí bezpečného kanálu[42]. Aplikací transformace na zprávu vznikne kryptogram E, který je přenášen nezabezpečeným kanálem, v němž je nutno počítat s možným zachycením nepřátelským kryptoanalytikem. Ten může sice znát princip šifry, tedy množinu všech možných transformací T, avšak bez znalosti klíče K není schopen rozhodnout, kterou transformaci použít. Naproti tomu dešifrovací mechanismus ve vlastnictví legitimního příjemce tento klíč zná, a je tak schopen aplikovat jedinou správnou transformaci T_K^{-1}, která přemění kryptogram zpět na původní zprávu.

Každému klíči můžeme ještě před zachycením kryptogramu *a priori* přiřadit pravděpodobnost jeho vybrání z množiny všech klíčů, a stejně tak můžeme pravděpodobnost přiřadit každé možné zprávě. Bez znalosti klíče je nepřátelský kryptoanalytik nucen jej co nejlépe odhadnout. K tomu je zapotřebí přiřadit všem možným klíčům, a tím i zprávám, *a posteriori* pravděpodobnosti, vyplývající ze znalosti kryptogramu a okolností, za nichž byla zpráva šifrována. Příkladem může být klasická substituce na 26-znakové abecedě. Počet všech možných klíčů takového systému je 26!. Pokud nevíme o zprávě nic bližšího, jsou *a priori* pravděpodobnosti každého jednotlivého klíče $\frac{1}{26!}$. Pokud však jakkoliv zjistíme jazyk zprávy, můžeme aplikovat jeho frekvenční charakteristiky na kryptogram, čímž získáme *a posteriori* pravděpodobnosti různých zpráv, a tím i klíčů. Veškerá práce kryptoanalytika se tak dá v posledku chápat jako snaha o určení těchto *a posteriori* pravděpodobností. Nehraje přitom roli, zda zjišťujeme pravděpodobnosti zpráv nebo klíčů, protože při znalosti jednoho je možné jednoznačně určit druhé. Pokud se po zachycení kryptogramu určené *a posteriori* pravděpodobnosti neliší od *a priori* pravděpodobností, není možné určit, který z klíčů nebo zpráv byl použit. Shannon dokazuje, že jediný systém, který tento

[42] Např. kurýr v případě one-time padu, nebo předem dohodnuté identické nastavení šifrovacího stroje.

předpoklad splňuje, je Vernamova šifra. Každý jazyk má své statisticky určitelné frekvenční charakteristiky, které se přenáší i do kryptogramu. Jediným případem, kdy tomu tak není, je použití zcela náhodného klíče dlouhého jako zpráva sama.

Pokud je zpráva zašifrována jiným systémem, pak s každým zachyceným znakem kryptogramu vzrůstají a klesají pravděpodobnosti jednotlivých klíčů a zpráv, až do stavu, kdy jedna zpráva nebo klíč má pravděpodobnost blížící se jedné a všechny ostatní pravděpodobnosti blížící se nule. Proces přibližování se tomuto stavu je možné popsat tzv. *ekvivokací*:

$$H(N) = \frac{H(K)}{D}$$

H(K) charakterizuje velikost prostoru klíčů. Pokud jsou všechny klíče *a priori* stejně pravděpodobné, je H(K) rovno desítkovému logaritmu počtu klíčů. D představuje redundanci jazyka zprávy. N je počet zachycených znaků kryptogramu. U většiny systémů má H(N) s rostoucím N klesající charakter, tzn. čím více znaků kryptoanalytik zachytí, tím si je jistější řešením. Pro Vernamovu šifru platí, že H(N) je konstantní, a libovolně velké N tedy nedává žádnou dodatečnou informaci o zprávě nebo klíči. Závěrem Shannon dodává, že je možné se i s použitím jiných systémů alespoň přiblížit Vernamově šifře. Toho lze dosáhnout buď dostatečně velkým prostorem klíčů, nebo snížením redundance jazyka [SHANNON, 1949].

5. Závěr

Od počátku 20. století nastaly dva zlomy, které zásadním způsobem přispěly k formování moderní kryptologie. Prvním bylo rychlé rozšíření rádiové komunikace a s ní bezpodmínečná nutnost utajení velkého množství přenášených zpráv. Poté, co se ruční šifry ukázaly jako pomalé a nedostatečně odolné proti moderním kryptoanalytickým útokům, nastal čas pro druhý zlom a začala éra strojového šifrování. Od prvních kroků v podobě Enigmy, která byla spíše pasivní pomůckou typu Albertiho šifrovacího disku, byl postupně eliminován lidský prvek a u strojů jako T52 již člověk nebyl k šifrování a dešifrování zapotřebí. Tento trend se udržel a vedl k masovému použití elektronické kryptografie, jak ji známe dnes. Dnešní člověk si často ani neuvědomuje, jak velká část jeho komunikace je šifrována. A naopak pokud o tom ví, avšak postrádá dostatečný vhled do principů šifer a jejich slabin, má často tendenci považovat šifrovanou komunikaci za absolutně bezpečnou. Právě to se stalo osudným Třetí říši, která spoléhala na chytrost vlastních strojů a málo si uvědomovala potenciální omylnost vlastních lidí[43]. Tento problém pokračuje v mírné obměně i dnes. Ačkoliv moderní kryptosystémy typu AES nebo RSA nabízejí oproti válečným systémům řádově vyšší bezpečnost, neexistuje doposud žádný systém zabezpečený proti svému nejslabšímu článku - chybujícímu uživateli.

Projekt Ultra dokázal, že teoretické vědy, jako matematika a lingvistika, mohou mít při správném použití nemalý vliv na reálný svět. Sir Harry Hinsley, bývalý zaměstnanec Bletchley a pozdější profesor historie mezinárodních vztahů na University of Cambridge, v jedné ze svých přednášek prohlásil, že práce kryptologů v Bletchley zkrátila válku o dva až čtyři roky[44] [HINSLEY, 1993]. Opačný proces, tvorbu teoretických základních kamenů jako podpory předtím spíše aplikovaného oboru, lze sledovat v Shannonových pracích.

---

[43] Případně nebrala v úvahu chytrost některých lidí na druhé straně Lamanšského kanálu.
[44] Tento výrok je často mylně připisován mnoha významným osobnostem - Winstonu Churchillovi, Dwightu D. Eisenhowerovi a dalším. I oni však ve svých memoárech vyjádřili nezpochybnitelné uznání práce lidí v Bletchley.

Jak bylo zmíněno v předmluvě, z důvodu stanoveného rozsahu není tato práce vyčerpávajícím zpracováním tématu. Nabízí se tedy hned několik možných směrů případného pozdějšího rozšíření. Bylo by jistě možné popsat šifrovací a špionážní metody ležící mimo hlavní dějiště kryptologické války: šifry českých partyzánů, italské luštění amerických diplomatických kódů, japonské šifrovací stroje a jejich americkou kryptoanalýzu, sovětskou špionážní síť přezdívanou Rudá kapela a mnohé další. Velkou dávku vlastního výzkumu by jistě vyžadovalo právě téma sovětské kryptografie. Literatura k této problematice je zatím až podezřele skrovná, avšak vždy se dá doufat v odtajnění dalších materiálů, které mohou otevřít živou vědeckou debatu. Dalším možným rozšířením, či spíše příbuzným tématem, je raná fáze vývoje počítačů. Množství britských i amerických strojů rozvíjejících Turingovy a Shannonovy myšlenky by nepochybně vydalo na samostatnou práci.

Seznam použité literatury

- ALDRICH, Richard, 2010. *GCHQ: the uncensored story of Britain's most secret intelligence agency*. London: HarperPress. 448 s. ISBN 978-000-7278-473.
- ALEXANDER, C. Hugh O'D, 1945. Cryptographic History of Work on the German Naval Enigma. Milton Keynes, 120 s. Dostupné z: http://www.ellsbury.com/gne/gne-000.htm
- ANDRESEN, S. L., 2001. Donald Michie: secrets of Colossus revealed. *IEEE Intelligent Systems*. vol. 16, no. 6, s. 82-83. ISSN 1094-7167.
- ATHERTON, W. A., 1989. Alan Mathison Turing (1912-54) : the solitary genius who wanted to build a brain. *Electronics & Wireless World*. vol. 95, no. 1640, s. 582-583. ISSN 0266-3244.
- BATEY, Mavis, 2008. Dilly Knox : a reminiscence of this pioneer Enigma cryptanalyst. *Cryptologia*. vol. 32, no. 2, s. 104-130. ISSN 0161-1194.
- BAUER, F. L., 1991. Scherbius and the Enigma. *Informatik Spektrum*. vol. 14, no. 4, s. 211-214. ISSN 0170-6012.
- BAUER, F. L., 2000. Marian Rejewski-the inventor of the cryptological computer. *Informatik Spektrum*. vol. 23, no. 5, s. 325-333. ISSN 0170-6012.
- BECKMAN, Bengt, 2002. *Codebreakers: Arne Beurling and the Swedish crypto program during World War II*. Providence, R.I.: American Mathematical Society. xviii, 259 s. ISBN 978-082-1828-892.
- Bletchley Park, 2012. *The Polish contribution* [online]. Milton Keynes : Bletchley Park [cit. 2012-05-23]. Dostupné z: http://www.bletchleypark.org.uk/content/hist/history/polish.rhtm
- BOROVIČKA, V. P., 1982. *Přísně tajné šifry*. Vyd. 1. Praha : Naše vojsko. 315 s.
- BURNS, R. W., 1994. Impact of technology on the defeat of the U-boat September 1939-May 1943. *IEE Proceedings-Science, Measurement and Technology*. vol. 141, no. 5, s. 343-55. ISSN 1350-2344.
- BURTON, C. E., 1985. Enhanced ADFGVX cipher system. *Dr. Dobb's Journal*. vol. 10, no. 2, s. 48-70. ISSN: 1044-789X.

- CARTER, F. L., 1997. The breaking of the Lorenz Cipher : an introduction to the theory behind the operational role of "Colossus" at BP. In: DARNELL, M. (ed.). *Cryptography and coding : 6th IMA international conference, Cirencester, UK, 17-19 December 1997 : proceedings*. Berlin : Springer, s. 74-88. ISBN 3-540-63927-6.
- CIMRMAN, Jára da. 2001. *Němý Bobeš, aneb, Český Tarzan*. 4. vyd. Praha : Paseka. 64 s. ISBN 80-7185-368-2.
- *Cipher machines*, 2012. [online]. Last modified 4 Jul 2012 [cit. 2012-07-15]. Dostupné z: http://ciphermachines.com
- Code-breakers : Bletchley Park's lost heroes, 2011. In: *Timewatch* [televizní dokument]. BBC two, 29.10. 20:40.
- COPELAND, B. Jack, 2004a. Colossus: its origins and originators. *IEEE Annals of the History of Computing*. vol. 26, no. 4. s. 38-45. ISSN: 1058-6180.
- COPELAND, B. Jack (ed.), 2004b. *The essential Turing: seminal writings in computing, logic, philosophy, artificial intelligence, and artificial life, plus the secrets of Enigma*. Oxford: Clarendon Press. viii, 613 s. ISBN 978-0-19-825080-7.
- COPELAND, B. Jack, 2006. Colossus: the secrets of Bletchley Park's codebreaking computers. New York: Oxford University Press. xvi, 462 s. ISBN 978-019-2840-554.
- Cypher Research Laboratories, 2006. *A brief history of cryptography* [online]. Cairns : Cypher Research Laboratories. Last updated January 24 2006. [cit. 2012-03-26]. Dostupné z: http://www.cypher.com.au/crypto_history.htm
- DAVIES, D. W., 1993. The transition from mechanisms to electronic computers, 1940 to 1950. In: IMAI, H. (ed.). *Advances in cryptology - ASIACRYPT '91 : international conference on the theory and application of cryptology, Fujiyoshida, Japan, 11-14 November 1991 : proceedings*. Berlin : Springer, s. 1-21. ISBN 3-540-57332-1.
- DAVIES, D. W., 1994, New information on the history of the Siemens and Halske T52 cipher machines. *Cryptologia*. vol. 18, no. 2, s. 141-146. ISSN 0161-1194.

- DAY, Colin, 2004. *Bletchley Park : Britain's best-kept secret of World War II* [online]. [cit. 2012-04-04]. Dostupné z: http://www.colindaylinks.com/bletchley/index.html
- ELLSBURY, Graham, 2007. *The Enigma and the Bombe* [online]. [cit. 2012-03-30] Dostupné z: http://www.ellsbury.com/enigmabombe.htm
- *Encyclopedia of cryptography and security*, 2005. New York : Springer. x, 684 s. ISBN 0-387-23473-X.
- ERSKINE, R., 2008. Captured Kriegsmarine enigma documents at Bletchley park. *Cryptologia*. vol. 32, no. 3, s. 199-219. ISSN 0161-1194.
- ERSKINE, Ralph, 2002. The Admiralty and cipher machines during the Second World War : not so stupid after all. *Journal of Intelligence History*. vol. 2, no. 2. s. 49-68. ISSN 1616-1262.
- ERSKINE, Ralph, 1997. The Development of Typex. *The Enigma Bulletin.* no. 2. s. 69-86. ISSN 0867-8693.
- FREEMAN, Peter, 2006. The Zimmermann Telegram revisited : a reconciliation of the primary sources. *Cryptologia*. vol. 30, no. 2, s. 98-150. ISSN 0161-1194.
- FLICKE, Wilhelm F., 1994. *War secrets in the ether : the use of signals intelligence by the German military in WWII.* [S.l.] : Aegean Park Press. 244 s. ISBN 0-89412-233-9.
- GAJ, K.; ORLOWSKI, A., 2003. Facts and myths of enigma : breaking stereotypes. In: BIHAM, E. (ed.). *Advances in cryptology - EUROCRPYT 2003 : international conference on the theory and applications of cryptographic techniques, Warsaw, Poland, 4-8 May 2003 : proceedings*. Berlin : Springer, s. 106-22. Lecture notes in computer science, vol. 2656. ISBN 3-540-14039-5.
- GOEBEL, Greg, 2010. *Codes, Ciphers, & Codebreaking* [online]. [cit. 2011-12-01]. Dostupné z: http://www.vectorsite.net/ttcode.html
- GOOD, Jack, MICHIE, Donald a TIMMS, Geoffrey, 1945. *General report on Tunny*. Milton Keynes : Bletchley Park. 505 s. Dostupné z: http://www.ellsbury.com/tunny/tunny-000.htm
- GREY, Christopher a STURDY, Andrew, 2008. The 1942 reorganization of the Government Code and Cypher School. *Cryptologia*. vol. 32 no. 4, s. 311-333. ISSN 0161-1194.

- HALPERN, Paul G., 1995. *A naval history of World War I*. London : Routledge. xiii, 591 s. ISBN 1-85728-498-4.
- HINSLEY, Harry, 1993. *The Influence of ULTRA in the Second World War*. [záznam přednášky] Cambridge : University of Cambridge, 19.10.1993. Dostupné z: http://www.cl.cam.ac.uk/research/security/Historical/hinsley.html
- CHURCHHOUSE, R. F., 1993. The M209 cipher machine : a war of words. *IEE Review*. vol. 39, no. 4, s. 173-175. ISSN 0953-5683.
- JANEČEK, Jiří, 1998. *Gentlemani (ne)čtou cizí dopisy*. 1. vyd. Brno : Books. 175 s. ISBN 80-85914-90-5.
- KAHN, David. 1968. *The codebreakers : the story of secret writing*. 4th ed. New York : Macmillan, 1968. 1164 s.
- KAHN, David. 1991. *Seizing the enigma: the race to break the German U-boat codes, 1939-1943*. Boston: Houghton Mifflin Co. xii, 336 s. ISBN 03-954-2739-8.
- KAHN, David. 2004. *The reader of gentlemen's mail : Herbert O. Yardley and the birth of American codebreaking*. 1st ed. New Haven : Yale University Press. xxi, 318 s. ISBN 0-300-09846-4.
- LEAVITT, David. 2007. *Muž, který věděl příliš mnoho*. 1. vyd. Praha: Dokořán. 270 s. ISBN 978-80-7363-086-7.
- LEE, J. A. N., BURKE, C. a ANDERSON, D., 2000. The US Bombes, NCR, Joseph Desch, and 600 WAVES: the first reunion of the US Naval Computing Machine Laboratory. *IEEE Annals of the History of Computing*. vol. 22, no. 3, s. 27-41. ISSN 1058-6180.
- LYONS, James, 2009. *Practical cryptogreaphy:* Playfair cipher [online]. [cit. 2011-07-10]. Dostupné z: http://practicalcryptography.com/ciphers/playfair-cipher
- MACKINNON, Colin, 2005. William Friedman's Bletchley park diary : a new source for the history of Anglo-American intelligence cooperation. *Intelligence & National Security*. vol. 20, no 4, s. 654-669. ISSN 0268-4527.
- MILLER, A. Ray, 1995. The cryptographic mathematics of Enigma. *Cryptologia*. vol. 19, no. 1, s. 65-80. ISSN 0161-1194.

- National Security Agency, 1995. *Allied vs. German Cryptology*. [záznam přednášky]. Fort Meade, NSA, 26.10.1995. Dostupné z: http://www.c-spanvideo.org/program/67946-1
- Navajo Code Talkers Foundation, 2012. *Official site of the Navajo code talkers* [online]. Window Rock : Navajo Code Talkers Foundation. [cit. 2012-07-19]. Dostupné z: http://navajocodetalkers.org/
- PIEKALKIEWICZ, Janusz, 2004. *Historie špionáže : agenti, systémy, akce*. 1. vyd. Praha : Naše vojsko. 565 s. ISBN 80-206-0738-2.
- PIPER, Fred; MURPHY, Sean, 2006. *Kryptografie : průvodce pro každého*. 1. vyd. Praha : Dokořán. 157 s. ISBN 80-7363-074-5.
- PLIMMER, B., 1998. Machines invented for WW II code breaking. *SIGCSE Bulletin*. vol.30, no.4, s. 37-40. ISSN 0097-8418.
- PROC, Jerry, 2012. *Crypto machines home page* [online]. Last updated June 12 2012 [cit. 2012-07-13]. Dostupné z: http://jproc.ca/crypto/
- REUVERS, Paul a SIMONS, Marc, 2012. *Enigma Cipher Machine* [online]. [cit. 2012-06-20]. Dostupné z: http://www.cryptomuseum.com/crypto/enigma
- RITTER, Terry, 2007. *Ritter's Crypto Glossary and Dictionary of Technical Cryptography* [online]. [cit. 2012-06-07]. Dostupné z: http://www.ciphersbyritter.com/GLOSSARY.HTM
- ROGERS, E. M., 1994. Claude Shannon's cryptography research during World War II and the mathematical theory of communication. In: SANSON, L. D. (ed.). *Proceedings of IEEE international Carnahan conference on security technology, Albuquerque, NM, 12-14 October 1994*. New York : IEEE, s. 1-5. ISBN 0-7803-1924-9.
- SALE, T., 1995. The Colossus of Bletchley Park. *IEE Review*. vol. 41, no. 2, s. 55-59. ISSN 0953-5683.
- SALE, Tony; COULTAS, Charles, 2004. Colossus : the world's first electronic digital computer. *Electronics World*. vol. 110, no. 1818, s. 16-20. ISSN: 1365-4675.
- SHANNON, Claude E., 1948. A mathematical theory of communication. *Bell System Technical Journal*. vol. 27(3), s. 379–423. ISSN: 0005-8580.
- SHANNON, Claude E., 1949. Communication theory of secrecy systems. *Bell System Technical Journal*. vol. 28(4), s. 656-715. ISSN: 0005-8580.

- SCHUCHMANN, H.-R., 1983. Enigma variations. In: BETH, Thomas (ed.). *Cryptography, Berg Feuerstein, West Germany, March 29 - April 2, 1982 : proceedings of the workshop*. Berlin : Springer, s. 65-68. Lecture notes in computer science, vol. 149. ISBN 3-540-11993-0.
- SINGH, Simon. 2003. *Kniha kódů a šifer : tajná komunikace od starého Egypta po kvantovou kryptografii*. 1. vyd. Praha : Dokořán. 382 s. ISBN 80-86569-18-7.
- URNER, Klaus. 2002. *"Let's swallow Switzerland": Hitler's plans against the Swiss Confederation*. Lanham, Md.: Lexington Books. xxi, 200 s. ISBN 07-391-0255-9.
- WOOD, James. 2000. *History of international broadcasting*. London : Institution of Electrical Engineers. 2 sv. ISBN 0-85296-920-1.
- ZORPETTE, G., 1987. Breaking the enemy's code. *IEEE Spectrum*. vol. 24, no. 9, s. 47-51. ISSN 0018-9235.

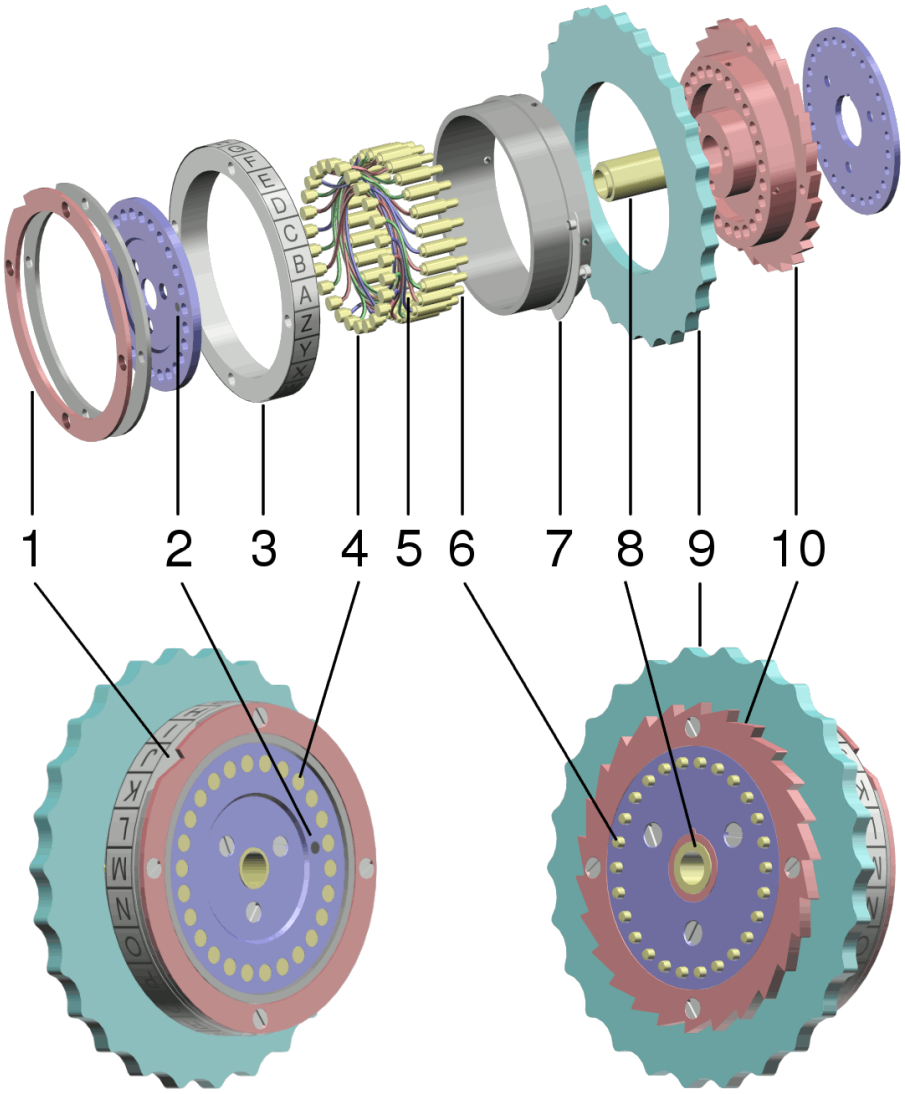
Seznam příloh

Přílohy

1) Vigenérův čtverec

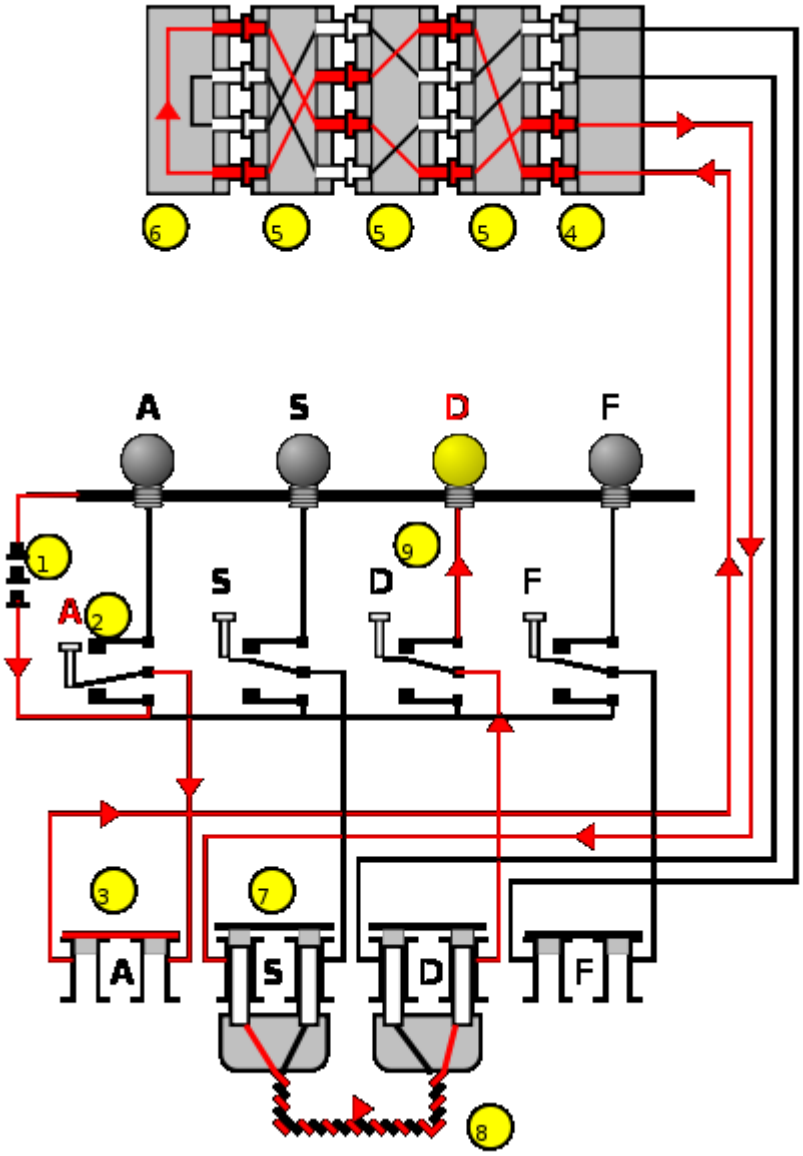
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	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

2) Rotor Enigmy M3 (zvýrazněné zobrazení)



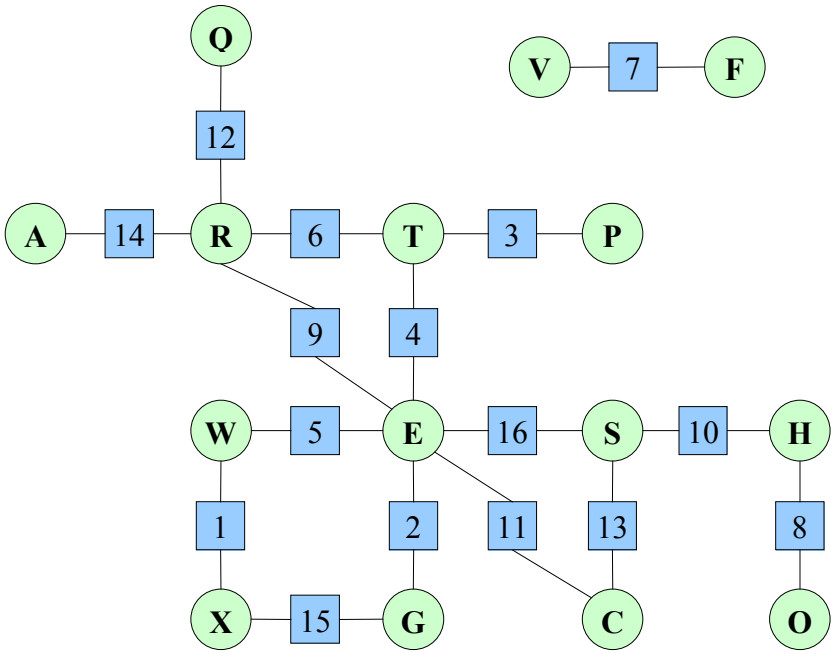
1. kroužek se zářezem
2. značka kontaktu vnitřního písmene "A"
3. prstenec s abecedou
4. kontakty
5. drátová propojení
6. kontakty
7. ustavující páka s pružinou
8. ložisko
9. volicí kroužek
10. zoubkovaný kroužek

3) Zjednodušené schéma elektrického zapojení Enigmy



1. baterie
2. stisknutá klávesa "A"
3. rozvodná deska (nepropojené "A")
4. vstupní stator
5. soustava rotorů
6. reflektor
7. a 8. rozvodná deska ("S" propojené s "D")
9. svítící žárovka "D"

4) Graf zapojení Turingovy bomby s tahákem "Wettervorhersage"

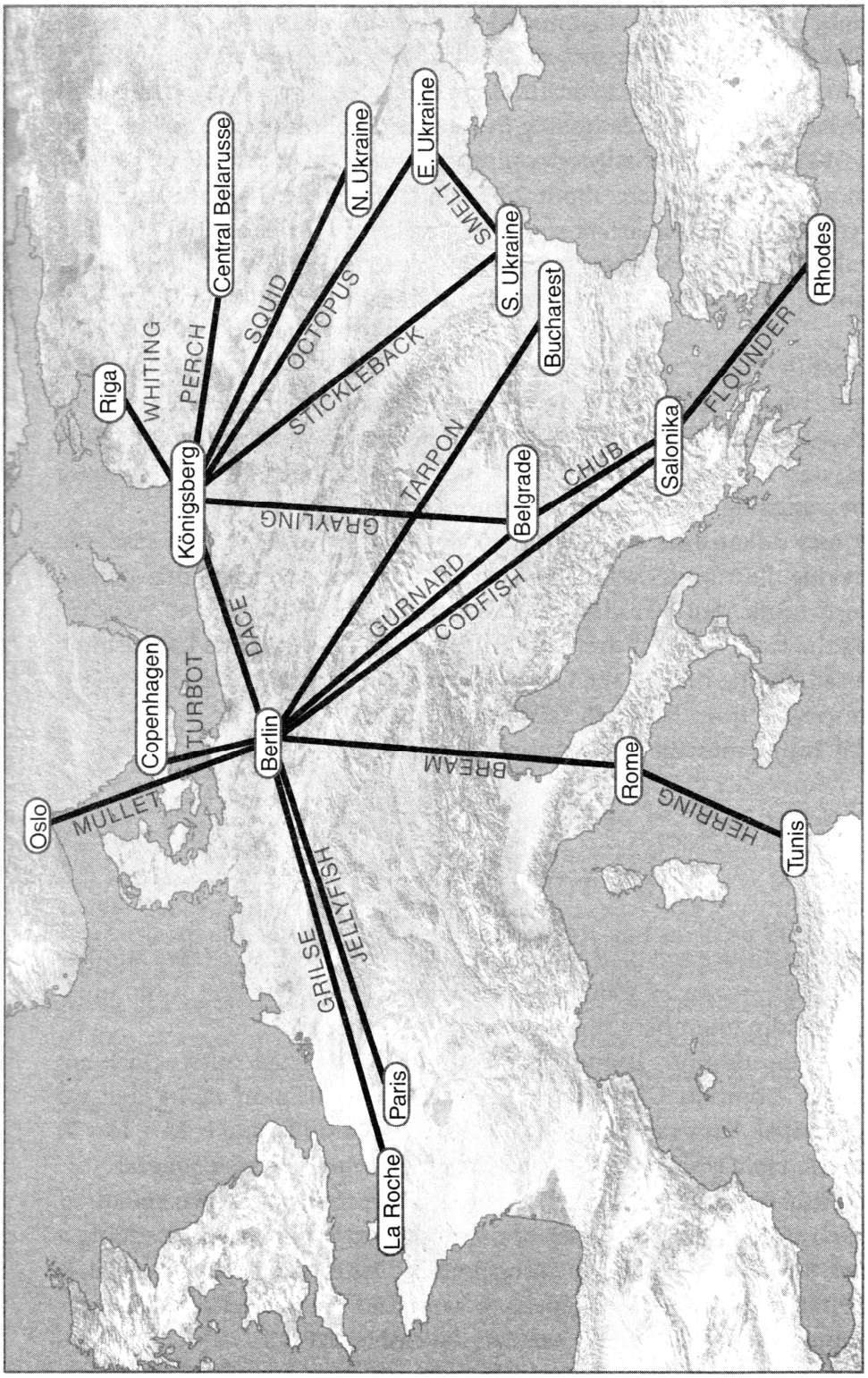


5) Baudot-Murrayho dálnopisné kódování

(díra ● označuje 1, nedíra 0)

1	2	3	4	5	**registr písmen**	**registr číslic**
●	●				A	- (pomlčka)
●			●	●	B	?
	●	●	●		C	:
●			●		D	dotaz (kdo tam?)
●					E	3
●		●	●		F	národní znak
	●		●	●	G	národní znak
		●		●	H	národní znak
	●	●			I	8
●	●		●		J	zvonek
●	●	●	●		K	(
	●			●	L	)
		●	●	●	M	. (tečka)
		●	●		N	, (čárka)
			●	●	O	9
	●	●		●	P	0
●	●	●		●	Q	1
	●		●		R	4
●		●			S	' (apostrof)
				●	T	5
●	●	●			U	7
	●	●	●	●	V	=
●	●			●	W	2
●		●	●	●	X	/
●		●		●	Y	6
●				●	Z	+
			●		návrat vozíku	
	●				posun o řádek	
●	●	●	●	●	změna na registr písmen	
●	●		●	●	změna na registr číslic	
		●			mezera	
					prázdný znak	

6) Mapa linek sítě dálnopisů Lorenz SZ40 (březen 1943 - červenec1944)



7) Shannonův diagram utajovacího systému