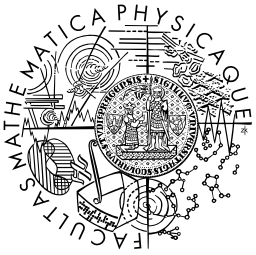


MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Dominika Kubániová

Metody odhalování denních klíčů u Enigmy

Katedra algebry

Vedoucí bakalářské práce:	doc. RNDr. Jiří Tůma, DrSc.
Studijní program:	Matematika
Studijní obor:	Matematické metody informační bezpečnosti

Praha 2018

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Chcela by som sa poďakovať doc. RNDr. Jiřímu Tůmovi, DrSc. za jeho rady, ochotu pri vedení práce a jeho nadšenie do tématu. Ďalej ďakujem rodine a najbližším priateľom za ich podporu.

Název práce: Metody odhalování denních klíčů u Enigmy

Autor: Dominika Kubániová

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. RNDr. Jiří Tůma, DrSc., Katedra algebry

Abstrakt: Počas druhej svetovej vojny bola schopnosť čítať nepriateľové šifrované správy dôležitá k obrane vlastného územia a dokonca ku rýchlejšiemu ukončeniu vojny. Jednou zo šifrovacích strojov bola nemecká Enigma, ktorej zmocnenie sa ale ešte ani zďaleka neznamenalo úspech pri dešifrovaní, keďže počet všetkých jej možných nastavení pre jeden deň predstavoval číslo presahujúce trilióny. V predvojnových a vojnových rokoch sa prelomeniu Enigmy neústupne venovali najlepší poľskí a anglickí matematici, ktorí svoje úspechy museli striktne držať v tajnosti, dokonca aj desiatky rokov po vojne. Náplňou mojej bakalárskej práce je vytvorenie matematického modelu Enigmy a pomocou jeho zistených slabín zrekonštruovať postupy pri odhaľovaní denných kľúčov s dôrazom na ich matematické zdôvodnenie.

Klíčová slova: Enigma, Rejewski, Zygalski, Turing, bomba, denné kľúče

Title: Recovering daily keys for Enigma

Author: Dominika Kubániová

Department: Department of algebra

Supervisor: doc. RNDr. Jiří Tůma, DrSc., Department of algebra

Abstract: During the second world war the ability to read enemy's encrypted messages was important to defence own territory and even to quicken the end of the war. One of the encrypting machines was german Enigma, whose seizing did not yet mean any success of decryption since the number of all possible settings for one day was a number exceeding trillions. In the pre-war and war years the breaking of Enigma was led by the best polish and british mathematicians, while they had to strictly keep their achievements secret, even decades years after the war. The aim of my bachelor thesis is to create a mathematical model of Enigma and to reconstruct its procedures for discovering daily keys with emphasis on their mathematical substantiation.

Keywords: Enigma, Rejewski, Zygalski, Turing, bombe, daily keys

Obsah

Úvod

V období medzi prvou a druhou svetovou vojnou boli poliaci znepokojení nemeckou komunikáciou šifrovanou nemeckým strojom Enigma. Preto najali troch poľských matematikov a kryptológov: Mariana Rejewského, Henryka Zygalského a Jerzyho Różyckého, aby sa pokúsili o prelomenie tohoto šifrovacieho stroja.

Komerčná verzia Enigmy bola voľne dostupná pre verejnosť. Vojenská komunikácia bola ale šifrovaná vylepšenou Enigmou, ktorá obsahovala oproti komerčnej verzii zložitejšiu architektúru a nové komponenty. Ďalej k tomu vojenská Enigma bola každý deň nastavená iným spôsobom podľa presne stanovených inštrukcií (denných kľúčov).

Keďže traja poľský kryptológovia vojenskú Enigmu sami nevlastnili a mali prístup len ku komerčnej verzii, museli na základe odpočutých správ vypočítať architektúru jednotlivých komponent a vyrobiť si vojenskú Enigmu sami. Toto skonštruovanie sa im podarilo a následne sa venovali zisťovaniu denných kľúčov na základe odpočutých správ. Aj v tomto procese boli poliaci úspešní a prišli na niekoľko metód, z ktorých dvom najvýznamnejším sa vo svojej práci budem venovať.

Nemci Enigmu a spôsob šifrovania ale neustále vylepšovali, čím prácu poliakom sťažovali. Neskôr už prelomovanie presahovalo ich možnosti (či už výpočetné alebo finančné), a preto krátko pred napadnutím Poľska nemeckou armádou svoje poznatky prezentovali anglickým kryptológom a matematikom, ktorý už v tej dobe tiež dávno pracovali na prelomovaní.

Angličania sa na problém pozerali viac z technickejšieho hľadiska než z matematického ako poliaci. Architektúru vojenskej Enigmy poznali od začiatku, keďže sa im podarilo Enigmu získať pri napadnutí nemeckej ponorky spolu s dennými kľúčmi pre isté krátke obdobie.

Cieľom mojej práce bude popísať a matematicky dokázať správnosť poľských a anglických metód odhaľovania denných kľúčov. V 1. kapitole sa zoznámime s architektúrou Enigmy, jej jednotlivými komponentami a s používanými protokolmi pre šifrovanie správ. V 2. kapitole predstavím matematický model Enigmy a nastienim slabosť šifrovacích protokolov, ktorá viedla k jej prelomeniu. Hlavnými časťami práce budú 3. a 4. kapitola, v ktorých budem popisovať a matematicky dokazovať princípy poľských a anglických metód odhaľovania denných kľúčov.

Vo svojej práci sa budem snažiť vychádzať z originálných zdrojov, teda z článkov priamo od Mariana Rejewského a Alana Turinga.

1. Architektúra Enigmy a šifrovanie

1.1 Architektúra stroja a jeho komponent

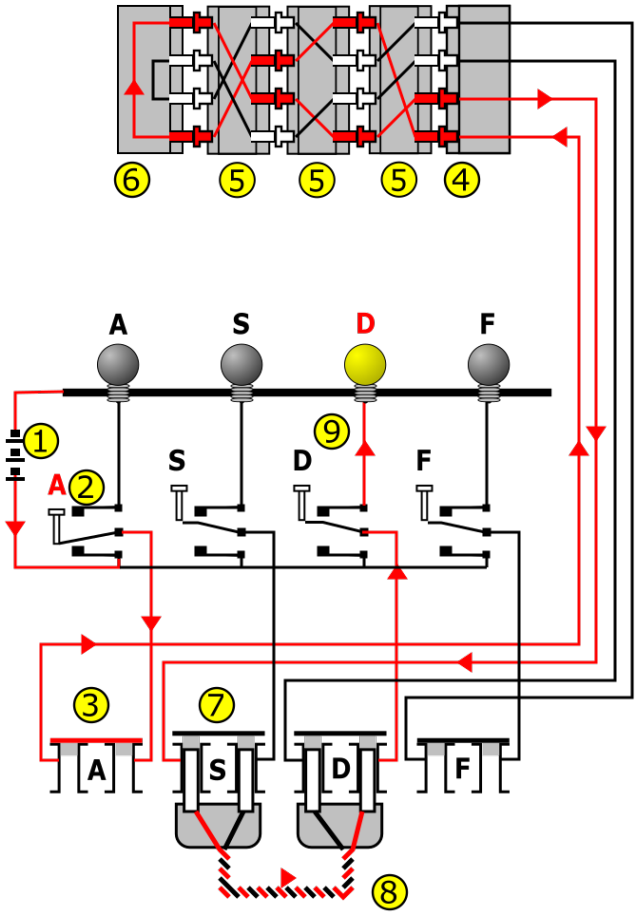
Enigma je elektricko-mechanický šifrovací stroj predstavujúci polyalfabetickú šifru, ktorý pozostáva z komponent prepojených drôtmi vedúcimi elektrický prúd. Stroj sa skladá z batérie, 26-tich stláčacích kláves a 26-tich žiaroviek označných písmenami abecedy, prepojovacej dosky, vstupného rotora, troch bubnov (pravého, stredného a ľavého), reflektoru a krokovacieho mechanizmu.

V Enigme sa v každom momente nachádza 26 elektrických obvodov, ktoré sa kvôli pohyblivým komponentám stroja v každom šifrovaní písmena menia. Schéma priechodu prúdu strojom je znázornená na obrázku 1.1. Stlačením ľubovolnej klávesy sa k nej patriaci obvod uzavrie, čím prúd smeruje od klávesy s písmenom (2), ktoré je zároveň vstupom šifrovacieho algoritmu, do prepojovacej dosky (3), následne cez vstupný rotor (4) a tri bubny (5) do reflektoru (6), ktorý prúd presmeruje a pošle späť cez tri bubny a vstupný rotor do prepojovacej dosky (7,8). Nakoniec prúd prejde doskou so žiarovkami a rozžiari práve jednu (9), ktorá nesie písmeno predstavujúce výstup algoritmu, teda zašifrované vstupné písmeno.

Prvou šifrovacou komponentou je *prepojovacia doska* pozostávajúca z 26-tich zásuviek, kde každá patrí k jednému písmenu abecedy. Prepojovacia doska umožnuje spojiť dve písmená káblom, čím sa pri priechode prúdu doskou písmena navzájom prehodia. Štandardom bolo používanie 6-tich káblov, teda prepojenie 12-tich písmen. Tento štandard bol v októbri 1936 zmenený na päť až osem káblov, a neskôr až na desať a viac (Rejewski, 1981, str. 224). Vidíme, že prepojovacia doska tvorí permutáciu so 6-timi transpozíciami a 14-timi 1-cyklami (podľa prvého štandardu).

Úlohou *vstupného rotora* je prepojiť prepojovaciu dosku s pravým bubnom. Na pravej strane do vstupného rotora vstupje 26 drôtov z prepojovacej dosky a na ľavej strane vystupuje 26, do kruhu zoradených, kolíkov. Naďalej budeme jednotlivé kolíky označovať písmenami abecedy v abecednom poradí. Z prepojovacej dosky vychádzajú drôty vhľadom k písmenu ku ktorému prislúchajú v abecednom poradí, a v rovnakom poradí sa pripájajú ku kolíkom na vstupnom rotore. Inak povedané, vstupný rotor predstavuje identickú permutáciu a preto nemá pre šifrovanie žiaden význam.

Najdôležitejšími a najkomplexnejšími komponentami Enigmy sú tri (v niektorých typoch Enigiem až štyri) *bubny*, z ktorých sa pri každom stlačení klávesy aspoň jeden pootočí. Bubon pozostáva z rotora a abecedného krúžku. Jadro bubna sa nazýva *rotor*, ktorého vnútro obsahuje 26 drôtov nepravidelne spájajúcich do kruhu usporiadaných 26 kolíkov na pravej strane rotora s 26-timi plochými elektrickými kontaktami, usporiadanými do kruhu na ľavej strane rotora (Rejewski, 1981, str. 214). Jadro rotora môžeme vidieť na obrázku 1.4. Rovnako ako pri vstupnom rotore, jednotlivé kolíky a ploché elektrické kontakty budeme označovať písmenami abecedy v abecednom poradí. Kolík a elektrický kontakt, ktoré ležia oproti sebe budeme označovať jedným písmenom abecedy. Po vložení troch bubnov do stroja sa vždy elektrické kontakty jedného rotora dotýkajú kolíkov dru-



Obr. 1.1: Priechod prúdu jedným obvodom pri šifrovaní. Zdroj (Woland, 2007)

hého rotora, čo umožňuje viesť elektrický prúd. Kvôli nepravidelnému pospájaniu sa prúd v každom rotore presmeruje na iné výstupné miesto.

Abecedný krúžok je prstenec, ktorý má na obvode vyrité písmená v abecednom poradí (resp. čísla 00-25), ktoré ako ukážem neskôr v sekcii 1.3 súvisia s nastavením pozícií jednotlivých bubnov. Abecedný krúžok je možné nasadiť a uchytiť na rotor 26-timi spôsobmi. Súčasťou krúžku je vždy jeden *zárez*, nachádzajúci sa pri pevne danom písmene, ktorý súvisí s otáčaním súsedných bubnov.

V neskoršom období existovalo až osem typov rotorov, z ktorých sa vyberalo a v istom poradí sa vkladalo do Enigmy. Každý rotor sa líšil od ostatných nie len v zadrôtovaní kolíkov s plochými kontaktmi, ale aj pozíciou zárezu. V medzivojnovom a vojnovom období existovalo viac komunikačných sietí, z ktorých niektoré šifrovali svoju komunikáciu trochu inak a dokonca aj s vylepšenými Enigmami. Niektoré siete vyberali len z prvých troch typov rotorov a neskôr z piatich, a iné siete mali Enigmy používajúce až štyri rotory. V tomto prípade tieto siete vyberali až z ôsmich typov rotorov. Prepojenie jednotlivých typov rotorov a ich značenie bolo ale pre všetky siete rovnaké (Rijmenants). Ďalej v práci budem uvažovať len Enigmy obsahujúce tri miesta pre rotory a tri typy rotorov, z ktorých sa vyberalo.

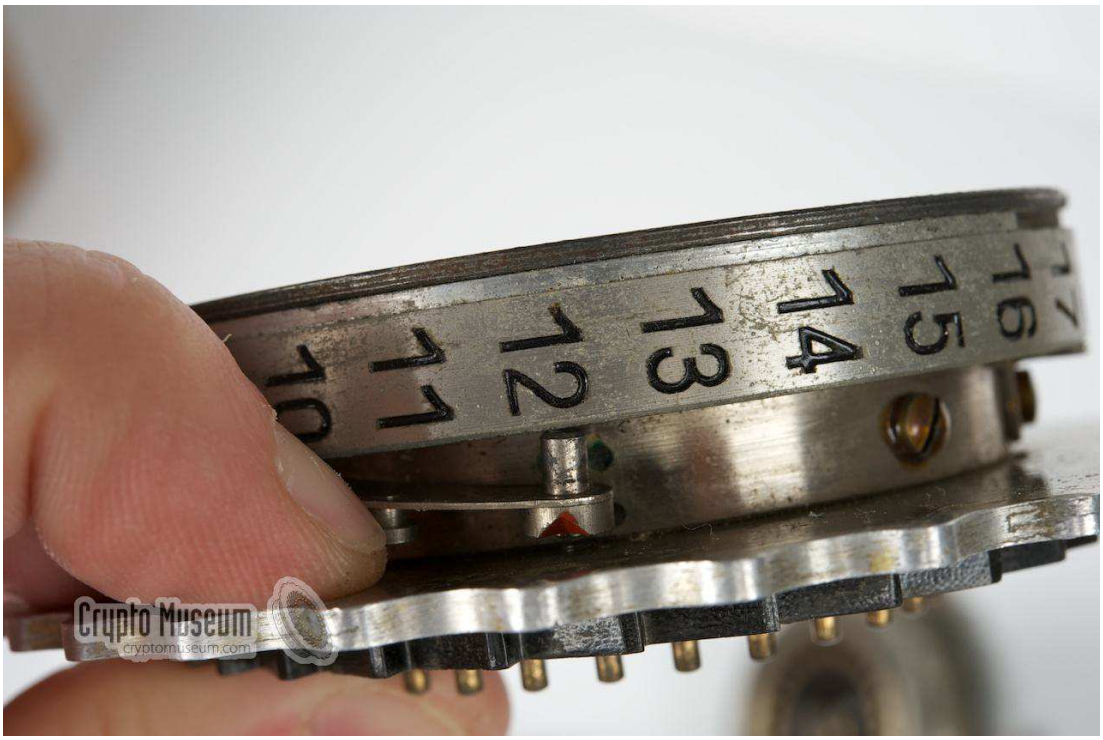
Každý z troch typov rotorov mal vlastný abecedný krúžok, pričom každý typ mal zárez pri inom písmene. Rotor s nasadeným abecedným krúžkom môžeme vidieť na obrázku 1.5 a zárez na abecednom krúžku na obrázku 1.4. Na kryte

Obr. 1.2: Enigma s detailným záberom na prepojovacú dosku. Zdroj (Reuvers a Simons, a)

Obr. 1.3: Enigma s detailným záberom na vnútro a tri bubny. Zdroj (Reuvers a Simons, a)

stroja sa nachádzajú tri okienka, cez ktoré možno vidieť písmena (resp. čísla) z

Obr. 1.4: Záber na jadro bubna. Zdroj (Reuvers a Simons, a)



Obr. 1.5: Detailný záber na abecedný krúžok a pinu. Zdroj (Reuvers a Simons, a)

abecedného krúžku nasadenom na rotore. Neskôr ukážem, že tri písmená ktoré v týchto okienkach vidno sú súčasťou denného kľúča na šifrovanie.

Keď budem naďalej hovoriť o *rotore*, budem tým myslieť *bubon bez abecedného*

krúžku. Pojmom *bubon* budem naďalej myslieť *rotor s abecedným krúžkom*.

O otáčanie bubnov sa stará *krokovací mechanizmus*, ktorému sa v práci nebudem venovať. Pre vysvetlenie viď (Rijmenants, The stepping mechanism). *Obratová pozícia* je pozícia, v ktorej krokovací mechanizmus zapadne do zárezu abecedného krúžku na rotore a tým pootočí súsedný ľavý bubon. Pravý bubon sa pootočí o 1/26 pri každom stlačení klávesy. Keď sa dostane k obratovej pozícii, posunie zároveň aj stredný bubon o 1/26. Rovnako, keď sa stredný bubon dostane k obratovej pozícii, posunie ľavý bubon o 1/26. Podstata toho prečo Enigma predstavuje polyalfabetickú šifru spočíva práve v zmene natočení bubnov pri každom stlačení klávesy, čím každé písmeno v texte je šifrované inou šifrovacou permutáciou. Dôsledkom je, že stláčaním stále rovnakého písmena sa rozsvieti vždy iná žiarovka.

Poslednou nepohyblivou šifrovacou komponentou stroja je *reflektor*, ktorý obsahuje kolíky iba na pravej strane. Vo vnútri reflektora sa všetky kolíky drôtmi spájajú do dvojíc. To znamená, že prúd vstupuje do reflektora prvým kolíkom v dvojici a vystupuje z neho opäť do bubnov druhým kolíkom v dvojici. Úlohou reflektora je teda presmerovanie prúdu späť. Vídíme, že reflektor tvorí permutáciu obsahujúcu 13 transpozíc.

Je dôležité poznamenať, že pri každom nastavení, čím myslím pri každom natočení rotorov, Enigma tvorí substitučnú šifru, ktorá pozostáva z 13-tich transpozíc. Dôvodom je konjugovanosť permutácie predstavujúcej šifrovanie v istom nastavení stroja s reflektorom, ktorý tvorí permutáciu s 13-timi transpozíciami. Neskôr v sekcii 2.2 tento fakt dokážem. Jasným dôsledkom je, že po stlačení ľubovoľnej klávesy s písmenom $\alpha \in \{\texttt{a},...,\texttt{z}\}$ sa nikdy nerozsvieti žiarovka s písmenom α. Ďalším dôsledkom je, že ak sa v istom nastavení stlačí klávesa α a rozsvieti sa žiarovka s písmenom β, potom v tom istom nastavení sa stlačením písmena β rozsvieti žiarovka s písmenom α (Rejewski, 1980, str. 5). Teda Enigma je recipročná.

1.2 Denné kľuče

Pripravenie Enigmy na šifrovanie alebo dešifrovanie spočívalo v určení poradia bubnov, nastavení prepojovacej dosky (*plugboard-setting*), uchytení abecedného krúžku každého rotora (*ring-setting*), a nastavení písmen viditeľných cez okienka v kryte stroja (*ground-setting*). Každý deň boli tieto poradia rotorov a nastavenia stroja jedinečné. Aby Enigmy na oboch koncoch komunikačného kanála boli nastavené rovnakým nastavením, tak každý nemecký operátor dostával každý mesiac tabuľku obsahujúcu vyššie zmienené denné nastavenia (denné kľúče) vygenerované pre každý deň v danom mesiaci.

1.3 Abecedný krúžok

Predstavme si, že máme v stroji len jeden rotor na ktorom sú napísané písmená v abecednom poradí. Každé písmeno vždy patrí jednému kolíku a plochému elektrickému kontaktu na stranách rotora. Každý rotor obsahuje *pinu*, ktorá sa nachádza pri kolíku a plochom elektrickom kontakte patriacim písmenu `a`. Pina slúži na uchytenie abecedného krúžku a môžeme ju vidieť na obrázku 1.5.

Pootočme rotor tak, aby sme na vrchu (teda v okienku na kryte stroja) videli napr. písmeno `a`, a teda vidíme aj pinu na vrchu rotora. Naďalej budem hovoriť, že rotor je *v pozícii napr.* `a`, ak na vrchu rotora vidíme písmeno `a`. Následne na rotor nasaďme abecedný krúžok a uchyťme ho pinou tak, aby sme na vrchu videli napr. písmeno `n`. Pripomínam, že točením bubna sa točí rotor spolu s abecedným krúžkom akoby boli jeden, a preto keďže abecedný krúžok je pri písmene `n` pevne uchytený, tak dvojica písmen `a` a `n` bude vždy nad sebou v akomkoľvek natočení bubna. Úlohou abecedného krúžku je zakrývať pozíciu rotora pod ním. Ďalej otočíme celým bubnom tak, aby sme v okienku na kryte stroja videli písmeno určené *ground-setting*, čo spolu s nastavením rotora budem nazývať *úvodnou pozíciou bubna*.

Vďaka abecednému krúžku kryptológovia nevedeli určiť presné nastavenie rotora aj keď poznali *ground-setting*, keďže na uchytenie piny existuje 26 možností, čo pri troch rotoroch vedie na $26^3 = 17\ 576$ možností.

Vidíme, že natočenie rotorov nezávisí na abecedných krúžkoch, ale vďaka nim nemeckí operátori mohli presne nastaviť rotory tak, aby Enigmy na obidvoch koncoch komunikačného kanálu boli nastavené rovnakým nastavením.

1.4 Šifrovanie

Operátorovou úlohou bolo nájsť v tabuľke kľúčov nastavenie prislúchajúce aktuálnemu dňu, vybrať tri bubny a vložiť ich v správnom poradí do Enigmy, v každom rotore uchytiť abecedný krúžok pinou pri písmenách určenými *ring-setting*, a otáčaním celých bubnov zabezpečiť, aby písmená abecedného krúžku vidiace cez okienka odpovedali písmenám určenými *ground-setting*, a nakoniec spárovať 6 dvojíc písmen v prepojovacej doske podľa *plugboard-setting*. Typy rotorov boli v tabuľkách označené rímskymi písmenami.

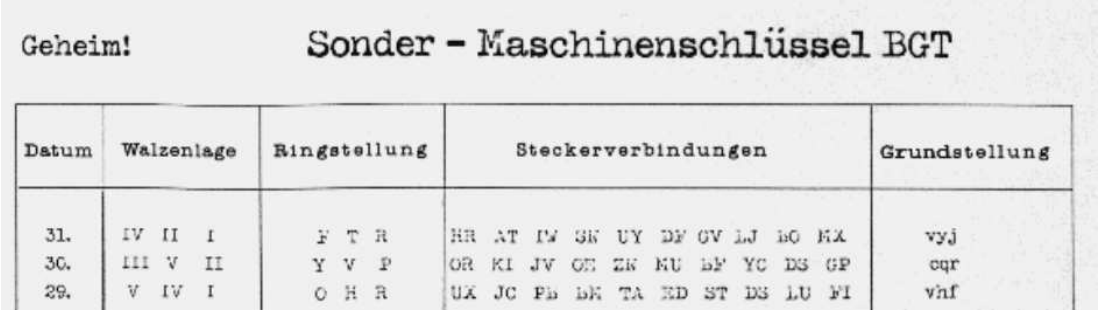
Existovali tri protokoly šifrovania.

1.4.1 Protokol šifrovania do 15.9.1938

- Operátor, vlastniaci tabuľku denných kľúčov, nastavil Enigmu podľa denného nastavenia
- Náhodne zvolil tri písmená, ktoré budem nazývať jeho *individuálny kľúč*
- Trojicu písmen jeho individuálneho kľúča dvakrát zašifroval Enigmou s denným nastavením, a šesť zašifrovaných písmen zapísal na začiatok šifrovanej správy
- Pootočil všetky tri bubny tak, aby okienka ukazovali jeho zvolený nezašifrovaný individuálny kľuč
- Začal šifrovať hlavnú správu a jej písmená postupne písal za zašifrovaný individuálny kľúč
- Rádiom poslal celú zašifrovanú správu pozostávajúcu zo zašifrovaného individuálneho kľúča dvakrát a zašifrovanej hlavnej správy

- Operátor na druhej strane komunikačného kanála, rovnako vlastniaci tabuľku denných kľúčov, nastavil Enigmu denným nastavením
- Denným nastavením dešifroval prvých šesť písmen, čím zistil individuálny kľúč odosielateľa
- Pootočil všetky tri bubny tak, aby okienka ukazovali odosielateľov zvolený individuálny kľúč
- Dešifroval hlavnú správu

Tento protokol sa používal do 15 Septembra, 1938. Zašifrovanie individuálneho kľúča dvakrát slúžilo ako prevencia proti zlému prenosu správy rádiom. Ak pri prenose došlo k chybe v prvých šiestich písmenách, prijímateľ to zistil tým, že pri dešifrovaní zašifrovaného individuálneho kľúča nedostal dvakrát po sebe rovnakú trojicu písmen. V tom prípade celú správu ignoroval (Rejewski, 1981, str. 216). Na obrázku 1.6 je fotografia tabuľky obsahujúcej denný kľúč k 31., 30. a 29. dňu v nejakom mesiaci. `Steckerverbindungen`, teda *plugboard-setting*, obsahuje až desať prepojených dvojíc, a teda sa jedná o tabuľku už z obdobia používania desiatich káblov.



Geheim! Sonder - Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Grundstellung
31.	IV II I	F T R	HR AT IW SN UY DF GV LJ BO MX	vyj
30.	III V II	Y V P	OR KI JV GZ ZN MU BF YC DS GP	cqr
29.	V IV I	O H R	UX JC PB BK TA ND ST DS LU FI	vhf

Obr. 1.6: Fotografia tabuľky denných kľúčov. Zdroj (Sale, The difficulties in breaking German Naval Enigma)

Príklad 1.4.1. Uvediem príklad predávania individuálneho kľúča a šifrovania správy `ENIGMA` prvým protokolom, ktorý si môžete vyskúšať sami na simulátore Enigmy na stránke `http://enigma.louisedade.co.uk/enigma.html` s typom Enigmy `M3` a reflektorom (*umkehrwalze*) `B`. Nastavíme Enigmu podľa denného kľúča: poradie rotorov - `I II III`, *ring-setting* - `AAA`, *ground-setting* - `KLM`, *plugboard-setting* - `AH CX DK ER MZ OP` (uvedených je šesť prepojených dvojíc). Zvolím si individuálny kľúč, napr. `nal`. Nezašifrovane správa teda podľa protokolu vyzerá `nal nal enigma`. S denným nastavením sa `nal nal` zašifruje na `wpv jjf`. V tomto momente zmeníme *ground-setting* na `nal` a ďalej zašifrujeme správu na `mdkcvc`. Zašifrovane teda poslaná správa je `wpv jjf mdkcvc`. V simulátore môžete skúsiť správu podľa protokolu dešifrovať.

1.4.2 Protokol šifrovania od 15.9.1938

Predošlý protokol šifrovania bol zmenený 15 Septembra, 1938, keď *ground-setting* prestal byť súčasťou denných kľúčov. Zmenený bol aj spôsob predávania individuálneho kľúča.

- Operátor nastavil Enigmu podľa denných kľúčov (tentokrát bez *ground-setting*)
- Náhodne vybral tri písmená, ktoré nezašifrovane vložil na začiatok správy, a pootočil všetky tri bubny tak, aby okienka ukazovali tri ním zvolené písmená. Tieto tri písmená predstavovali jeho *individuálny ground-setting*
- Vybral ďalšiu trojicu náhodných písmen, predstavujúcu jeho individuálny kľúč, ktorú dvakrát zašifroval, a šesť zašifrovaných písmen zapísal do správy za jeho individuálny *ground-setting*
- Pootočil všetky tri bubny tak, aby okienka ukazovali jeho nezašifrovanú trojicu individuálneho kľúča
- Začal šifrovať hlavnú správu a jej písmená postupne písal za zašifrovaný individuálny kľúč
- Rádiom poslal celú zašifrovanú správu pozostávajúcu z prvej trojice nezašifrovaných písmen individuálneho *ground-setting*, zašifrovaného individuálneho kľúča dvakrát a zašifrovanej hlavnej správy
- Operátor na druhej strane komunikačného kanála, rovnako vlastniaci tabuľku denných kľúčov, nastavil Enigmu denným nastavením
- Bubny pootočil tak, aby v okienkach videl prvé tri písmená prijatej správy, teda odosielateľov individuálny *ground-setting*
- Dešifroval ďalších šesť písmen, čím zistil individuálny kľuč odosielateľa
- Pootočil všetky tri bubny tak, aby okienka ukazovali odosielateľov zvolený individuálny kľuč
- Dešifroval hlavnú správu

Prvých deväť písmen poslanej správy (teda individuálny *ground-setting* a dvakrát zašifrovaný individuálny kľúč) budem ďalej nazývať *indikátor* (Rejewski, 1981, str. 225-226).

Príklad 1.4.2. Uvediem opäť príklad predávania individuálneho kľúča a šifrovania správy `ENIGMA` druhým protokolom s rovnakým nastavením bez *ground-setting* ako v príklade prvého protokolu, ktorý si môžete skúsiť cez simulátor. Zvolím si individuálny *ground-setting*: `YKE` a individuálny kľúč `nal`. Nezašifrovane správa teda podľa protokolu vyzerá `YKE nal nal enigma`. S denným nastavením a individuálnym *ground-setting* sa `nal nal` zašifruje na `hfi iji`. V tomto momente zmeníme *ground-setting* na `nal` a ďalej zašifrujeme správu na `mdkcvc`. Vidíme, že sa správa zašifrovala rovnako ako v predošlom príklade. Zašifrovane teda poslaná správa je `YKE hfi iji mdkcvc`. Opäť si v simulátore môžete skúsiť správu podľa protokolu dešifrovať.

Poznámka. Všimli sme si, že druhý protokol nám dáva informáciu o okamžiku, kedy dochádza ku pootočeniu ľavého a stredného bubna, v prípade ak poznáme ktoré typy rotorov boli použité, resp. predpokladáme ktoré boli použité. Keďže

presne poznáme kde sa zárezy nachádzajú v abecednom krúžku každého typu rotora, tak z prvých troch písmen indikátora (individuálneho *ground-setting*) vieme určiť, či sa v priebehu šifrovania dvakrát individuálneho kľúča otočil stredný, ľavý, alebo oba bubny. Napríklad rotor I má zárez pri písmene `y`, a teda rotor naľavo od neho sa pootočí pri následujúcom stlačení klávesy keď v okienku na kryte stroja vidíme písmeno `q`. To je príčinou toho, že klapky *stepping-mechanizmu*, ktoré pootáčajú rotory sa nachádzajú za rotormi a nižšie ako sú okienka (Rijmenants). Pri prechode písmena `q` na `r` v okienku sa rotor naľavo od rotora I pootočí o jedna (resp. nepootočí ak rotor I je na ľavo).

Neskôr ukážem, že metódy odhaľovania denných kľúčov boli založené na predpoklade, že počas šifrovania dvakrát individuálneho kľúča sa nepootočil ľavý a stredný rotor. Preto pred aplikovaním týchto metód vyfiltrovali z odpočutých správ tie, ktoré tento predpoklad splňovali pre nejaké skúmané poradie rotorov.

Príklad 1.4.3. Na jednoduchom príklade ukážem ako zistíme či sa aspoň jeden z ľavého a stredného rotora pootočil. Nech denné nastavenie Enigmy je rovnaké ako v predošlom príklade, až na nové poradie rotorov - `III II I` a individuálny *ground-setting* - `WBO`. Individuálny kľúč je naďalej `nal nal`. A teda zaslaná správa má indikátor

```
WBO uit pwe
```

Predpokladajme, že sme túto správu odpočuli, a že sme správne uhádli poradie rotorov III, II, I. Z predošlej poznámky ale vieme, že po šifrovaní tretieho písmena individuálneho kľúča na `t` sa stredný rotor pootočí keďže pri tomto šifrovaní vidíme v okienkách písmená `WBQ`. A teda vieme, že prvé písmeno individuálneho kľúča sa následne zašifrovalo na `p` s písmenami v okienkach už `WCR`. Táto správa teda nebude použitá k odhaleniu denného kľúča. Príklad si opäť môžete skúsiť na simulátore a pozorovať ako sa písmená v okienkach (*grundstellung*) menia.

1.4.3 Protokol šifrovania od Mája 1940

Od Mája 1940 sa naďalej používal druhý protokol, ale s tým rozdielom, že už individuálny kľúč nebol šifrovaný dvakrát. Teda na začiatku odoslanej správy prvé tri nezašifrované písmená predstavovali individuálny *ground-setting* a ďalšie tri písmená už predstavovali operátorom zvolený individuálny kľúč zašifrovaný raz (Reuvers a Simons, b).

2. Matematický model

V náledujúcej kapitole zadefinujem permutácie predstavujúce jednotlivé komponenty Enigmy a vytvorím matematický model šifrovania v každom nastavení stroja. Ďalej ukážem ako tento matematický model odkrýva chyby a nedostatky šifrovacích protokolov, ktoré viedli k prelomeniu šifry.

Pripomeňme, že druhá časť indikátora zašifrovanej správy druhým protokolom, teda šesť písmen zapísaných po troch písmenách individuálneho *ground-setting*, vždy obsahuje dvakrát po sebe zašifrovanú rovnakú trojicu písmen, to znamená, že prvé a štvrté písmeno v šestici patrí k rovnakému nezašifrovanému písmenu. Tak isto to platí pre druhé a piate písmeno, a tretie a šieste písmeno.

V celej práci budem skladať permutácie zľava, tzn. zápisom $DA\mathtt{a}$ uvažujem najprv aplikovanie permutácie A na písmeno `a`, a následne aplikovanie permutácie D na písmeno $A\mathtt{a}$. Písmená abecedy `a,...,z` budem stotožnovať a počítať s nimi ako s prvkami okruhu $\mathbb{Z}_{26}$.

2.1 Matematický model Enigmy

Značenie:

- S – permutácia predstavujúca prepojovaciu dosku
- H – permutácia predstavujúca prepojenie medzi prepojovacou doskou a vstupným rotorom
- *R, M, L* – permutácie predstavujúce pravý, stredný a ľavý bubon
- Q – permutácia predstavujúca reflektor
- $P := (\mathtt{A\ B\ C\ D\ E\ F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z})$

Permutácie *R, M, L* sa nikdy nemenia keďže odpovedajú presným prepojeniam kolíkov a elektrických kontaktov drôtmi v rotoroch, a to sa nemenilo. Rotory sú ale pri každom stave Enigmy pri šifrovaní v inom natočení. Permutácia ktorá bude popisovať i-té natočenie rotora bude P^i.

Vidíme, že

$$P^1 = (\mathtt{A\ B\ C\ D\ E\ F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z})$$
$$P^2 = (\mathtt{A\ C\ E\ G\ I\ K\ M\ O\ Q\ S\ U\ W\ Y})(\mathtt{B\ D\ F\ H\ J\ L\ N\ P\ R\ T\ V\ X\ Z})$$
$$P^3 = (\mathtt{A\ D\ G\ J\ M\ P\ S\ V\ Y\ B\ E\ H\ K\ N\ Q\ T\ W\ Z\ C\ F\ I\ L\ O\ R\ U\ X})$$
$$\ldots$$

a teda P^i permutuje každé písmeno z množiny `{A,B,...Z}` na i-té nasledujúce, čím zloženie $P^{-i}RP^i$ charakterizuje rotor R otočený o $i/26$ od základnej pozície (Rejewski, 1980, str. 6). Základnú pozíciu uvažujeme ako pozíciu bubnov keď v okienkách vidíme *ground-setting*.

Ďalej je dôležité podotknúť, že otočenie rotorov nastáva bezprostredne po stlačení klávesy. To znamená, že ak je pravý rotor natočený v pozícii i, stlačením klávesy sa písmeno šifruje pravým rotorom už v pozícii $i + 1$.

Ešte pripomeňme, že prepojovacia doska je každý deň nastavená inak podľa denného kľúča, a teda permutácia S, ktorá prepojovaciu dosku predstavuje, závisí na tomto nastavení.

S vyššie definovaným značením môžeme permutáciu predstavujúcu šifrovanie Enigmou s ľavým, stredným a pravým rotorom v z-tej, y-tej a x-tej pozícii popísať ako zloženie permutácií

$$S^{-1}E_{z,y,x}S \tag{2.1}$$

kde

$$\begin{aligned} E_{z,y,x} = (&H^{-1}P^{-(x+1)}R^{-1}P^{(x+1)}P^{-y}M^{-1}P^{y}P^{-z}L^{-1}P^{z})Q \\ &(P^{-z}LP^{z}P^{-y}MP^{y}P^{-(x+1)}RP^{(x+1)}H) \end{aligned} \tag{2.2}$$

Bez újmy na obecnosti môžeme permutáciu H naďalej v zápise vynechávať, keďže predstavuje identitu, ako som už zmienila v 1.1.

2.2 Permutácie definujúce indikátor

Budeme sa zaoberať druhým šifrovacím protokolom. Majme indikátor tvaru $X_1X_2X_3\ p_1q_1r_1\ p_2q_2r_2$, kde $X_1X_2X_3$ je individuálny *ground-setting* a $p_1q_1r_1\ p_2q_2r_2$ dvakrát zašifrovaná trojica písmen neznámeho individuálneho kľúča $k_1l_1m_1$, teda zašifrované $k_1l_1m_1\ k_1l_1m_1$. Nakoniec nech z, y a x je pozícia rotorov pred šifrovaním indikátora (teda pod písmenom abecedného krúžku X_1 ľavého bubna sa nachádza na ľavom rotore z, pod X_2 sa na strednom rotore nachádza y, a pod X_3 sa na pravom rotore nachádza x).

Predpokladajme, že pri šifrovaní individuálneho kľúča dochádza iba k otáčaniu pravého bubna o 1/26 pri každom stlačení klávesy. Ľavý a stredný zostávajú v rovnakej pozícii.

Zadefinujme permutácie, ktoré určujú šifrovanie dvakrát individuálneho kľúča s pozíciou rotorov z, y a x:

$$\begin{aligned} A = S^{-1}(&P^{-(x+1)}R^{-1}P^{(x+1)}P^{-y}M^{-1}P^{y}P^{-z}L^{-1}P^{z})Q \\ &(P^{-z}LP^{z}P^{-y}MP^{y}P^{-(x+1)}RP^{(x+1)})S \\ B = S^{-1}(&P^{-(x+2)}R^{-1}P^{(x+2)}P^{-y}M^{-1}P^{y}P^{-z}L^{-1}P^{z})Q \\ &(P^{-z}LP^{z}P^{-y}MP^{y}P^{-(x+2)}RP^{(x+2)})S \\ C = S^{-1}(&P^{-(x+3)}R^{-1}P^{(x+3)}P^{-y}M^{-1}P^{y}P^{-z}L^{-1}P^{z})Q \\ &(P^{-z}LP^{z}P^{-y}MP^{y}P^{-(x+3)}RP^{(x+3)})S \\ D = S^{-1}(&P^{-(x+4)}R^{-1}P^{(x+4)}P^{-y}M^{-1}P^{y}P^{-z}L^{-1}P^{z})Q \\ &(P^{-z}LP^{z}P^{-y}MP^{y}P^{-(x+4)}RP^{(x+4)})S \\ E = S^{-1}(&P^{-(x+5)}R^{-1}P^{(x+5)}P^{-y}M^{-1}P^{y}P^{-z}L^{-1}P^{z})Q \\ &(P^{-z}LP^{z}P^{-y}MP^{y}P^{-(x+5)}RP^{(x+5)})S \\ F = S^{-1}(&P^{-(x+6)}R^{-1}P^{(x+6)}P^{-y}M^{-1}P^{y}P^{-z}L^{-1}P^{z})Q \\ &(P^{-z}LP^{z}P^{-y}MP^{y}P^{-(x+6)}RP^{(x+6)})S \end{aligned} \tag{2.3}$$

(Rejewski, 1980, str. 6)

Vidíme, že $P^{-y}M^{-1}P^{y}P^{-z}L^{-1}P^{z}QP^{-z}LP^{k}P^{-y}MP^{y}$ sa v každej permutácii opakuje keďže predpokladáme, že ľavý a stredný bubon sa neotáčajú, a teda označením $T := P^{-y}M^{-1}P^{y}P^{-z}L^{-1}P^{z}QP^{-z}LP^{k}P^{-y}MP^{y}$ môžeme písať

$$\begin{aligned}
A &= S^{-1}(P^{-(x+1)}R^{-1}P^{(x+1)})T(P^{-(x+1)}RP^{(x+1)})S \\
B &= S^{-1}(P^{-(x+2)}R^{-1}P^{(x+2)})T(P^{-(x+2)}RP^{(x+2)})S \\
C &= S^{-1}(P^{-(x+3)}R^{-1}P^{(x+3)})T(P^{-(x+3)}RP^{(x+3)})S \\
D &= S^{-1}(P^{-(x+4)}R^{-1}P^{(x+4)})T(P^{-(x+4)}RP^{(x+4)})S \\
E &= S^{-1}(P^{-(x+5)}R^{-1}P^{(x+5)})T(P^{-(x+5)}RP^{(x+5)})S \\
F &= S^{-1}(P^{-(x+6)}R^{-1}P^{(x+6)})T(P^{-(x+6)}RP^{(x+6)})S
\end{aligned} \tag{2.4}$$

Potom z indikátora máme

$$\begin{aligned}
p_1 &= Ak_1 \\
q_1 &= Bl_1 \\
r_1 &= Cm_1 \\
p_2 &= Dk_1 \\
q_2 &= El_1 \\
r_2 &= Fm_1
\end{aligned} \tag{2.5}$$

Definícia 1. *Dve permutácie π a ρ na konečnej množine sú konjugované, ak existuje permutácia σ na rovnakej konečnej množine taká, že $\pi = \sigma^{-1}\rho\sigma$.*

Tvrdenie 1. *Dve permutácie na konečnej množine sú konjugované práve vtedy keď majú rovnaký počet cyklov každej dĺžky.*

Dôkaz. viď. (Tůma, 2003, str. 34-38)

□

Definícia 2. *Dve permutácie majúce rovnaký počet cyklov každej dĺžky nazývame permutácie majúce rovnakú štruktúru cyklov.*

Z rovnosti 2.2 máme, že

$$\begin{aligned}
S^{-1}E_{z,y,x}S = (&S^{-1}P^{-(x+1)}R^{-1}P^{(x+1)}P^{-y}M^{-1}P^{y}P^{-z}L^{-1}P^{z})Q \\
&(P^{-z}LP^{z}P^{-y}MP^{y}P^{-(x+1)}RP^{(x+1)}S)
\end{aligned} \tag{2.6}$$

a teda vidíme, že permutácia $S^{-1}E_{z,y,x}S$ je konjugovaná s permutáciou Q predstavujúcou reflektor, a teda z predošlého tvrdenia majú rovnakú štruktúru cyklov. Každé možné nastavenie Enigmy, čím myslím každé možné natočenie trojice rotorov a prepojenie dvojíc v prepojovacej doske teda jednoznačne definuje istú šifrovaciu permutáciu obsahujúcu 13 transpozíc.

Keďže permutácie A,B,C,D,E,F sú tiež konjugované s reflektorom, tak z tvrdenia 1 dostávame, že obsahujú iba transpozície a preto sú sami sebe inverzné

(napr. $A = A^{-1}$). Prenásobením rovnice 2.5 zľava inverzami dostávame

$$\begin{aligned} A^{-1}p_1 &= AA^{-1}k_1 \Rightarrow Ap_1 = k_1 \\ B^{-1}q_1 &= BB^{-1}l_1 \Rightarrow Bq_1 = l_2 \\ C^{-1}r_1 &= CC^{-1}m_1 \Rightarrow Cr_1 = m_3 \\ D^{-1}p_2 &= DD^{-1}k_1 \Rightarrow Dp_2 = k_1 \\ E^{-1}q_2 &= EE^{-1}l_1 \Rightarrow Eq_2 = l_2 \\ F^{-1}r_2 &= FF^{-1}m_1 \Rightarrow Fr_2 = m_3 \end{aligned} \tag{2.7}$$

Z toho

$$\begin{aligned} Ap_1 &= Dp_2 \\ Bq_1 &= Eq_2 \\ Cr_1 &= Fr_2 \end{aligned} \tag{2.8}$$

čím sa dostávame k

$$\begin{aligned} DAp_1 &= p_2 \\ EBq_1 &= q_2 \\ FCr_1 &= r_2 \end{aligned} \tag{2.9}$$

Poznámka. V prvom protokole šifrovania tiež šifrujeme dvakrát individuálny kľúč, preto v ňom môžeme používať zadefinované permutácie v 2.3 a úvahy za tým.

Podotknime, že permutácie A,B,C,D,E,F závisia na pozícii rotorov z, y, x, a teda závisia na nastavenom *ring-setting* a individuálnom *ground-setting*.

Matematický model nám odhalil slabosť prvého a druhého protokolu. Slabosť spočíva v tom, že nám indikátor dáva isté informácie o zložených permutáciách DA, EB a FC, ktoré hrali rolu pri odhaľovaní denných kľúčov. Následujúce tvrdenie budeme neskôr potrebovať pri dôkaze správnosti jednej metódy odhaľovania.

Tvrdenie 2. *Permutácie DA a*

$$P^{-(x+4)}R^{-1}P^{(x+4)}TP^{-(x+4)}RP^{(x+4)}P^{-(x+1)}R^{-1}P^{(x+1)}TP^{-(x+1)}RP^{(x+1)}$$

majú rovnakú štruktúru cyklov.

Dôkaz. Označme si

$$\rho = P^{-(x+4)}R^{-1}P^{(x+4)}TP^{-(x+4)}RP^{(x+4)}P^{-(x+1)}R^{-1}P^{(x+1)}TP^{-(x+1)}RP^{(x+1)}$$

Ďalej

$$\begin{aligned} DA = S^{-1}(P^{-(x+4)}R^{-1}P^{(x+4)})T(P^{-(x+4)}RP^{(x+4)})S \\ S^{-1}(P^{-(x+1)}R^{-1}P^{(x+1)})T(P^{-(x+1)}RP^{(x+1)})S \end{aligned}$$

a teda

$$\begin{aligned} DA = S^{-1}(P^{-(x+4)}R^{-1}P^{(x+4)})T(P^{-(x+4)}RP^{(x+4)}) \\ (P^{-(x+1)}R^{-1}P^{(x+1)})T(P^{-(x+1)}RP^{(x+1)})S \end{aligned}$$

Vidíme, že $DA = S^{-1}\rho S$, z čoho zisťujeme že permutácie DA a ρ sú konjugované, a teda z tvrdenia 1 majú rovnakú štruktúru cyklov. Inak povedané, permutácia S predstavujúca prepojovaciu dosku nemení štruktúru cyklov permutácie ρ.

□

Tvrdenie som sformulovala pre zloženú permutáciu DA, ale vidíme, že tvrdenie platí aj pre zložené permutácie EB a FC.

Vráťme sa opäť k prvému protokolu šifrovania, v ktorom každý individuálny kľúč v jednom dni bol šifrovaný rovnakým *ground-setting* určeným dňom. Indikátor mal tvar $p_1q_1r_1\ p_2q_2r_2$, čo odpovedalo zašifrovaniu dvakrát trojice písmen individuálneho kľúča, teda $k_1l_1m_1\ k_1l_1m_1$. S predpokladom, že opäť jedine pravý bubon sa otáča, pre $p_1q_1r_1\ p_2q_2r_2$ a $k_1l_1m_1\ k_1l_1m_1$ platia všetky rovnosti 2.5 až 2.9. Nepoznaním individuálnych kľučov a $k_1l_1m_1$ nedokážeme jednoznačne určiť permutácie A,B,C,D,E,F. Na druhú stranu ale v prvom protokole dokážeme vypočítať celé zložené permutácie DA, EB a FC, ak sme odpočuli dostatočné množstvo správ takých, že sa na pozíciách 1 a 4, 2 a 5, 3 a 6 indikátora prestriedali všetky písmená abecedy. Zložené permutácie DA, EB a FC môžeme vypočítať z rovností 2.9.

Počítanie týchto zložených permutácii DA, EB a FC bolo dôležité pre vypočítanie vnútorného prepojenia všetkých typov rotorov, ktorému sa ale venovať nebudem, keďže presahuje zadanie práce. Príklad vypočítania permutácií doporučujem si pozrieť v zdroji (Tůma, 2003, str. 40-43).

Vypočítať zložené permutácie DA, EB a FC nebolo ale možné v druhom protokole šifrovania, keďže v ňom každá šestica $p_1q_1r_1\ p_2q_2r_2$ bola zašifrovaná s iným individuálnym *ground-setting*. Stále bolo možné vypočítať permutácie DA, EB a FC, ale k tomu bolo potrebné odpočuť viac správ s rovnakými prvými troma písmenami $X_1X_2X_3$. Keďže si tieto tri písmená operátori volili sami a náhodne, tak bolo nepravdepodobné odpočuť dostatočné množstvo takých správ.

2.3 Fixné body

V obidvoch protokoloch nám indikátor dáva informáciu o tom či aspoň jedna z permutácií DA, EB a FC obsahujé cyklus dĺžky jedna. Predpokladajme, že sme odpočuli správu, v ktorej indikátor na 1. a 4. pozícii obsahuje rovnaké písmená, napr.

BPS kwd kap

Z 2.9 máme, že $DA\mathtt{k} = \mathtt{k}$, kde DA je permutácia závislá na nejakej pozícii rotorov z, y, x. Táto permutácia teda obsahuje aspoň jeden cyklus dĺžky jedna.

Definícia 3. *Písmeno abecedy α také, že $DA\alpha = \alpha$ nazývame fixným bodom permutácie DA.*

Rovnako definujeme fixné body permutácií EB a FC. Fixné body boli pri metódach odhaľovania kľúčov veľmi dôležité ako neskôr zistíme (Rejewski, 1980, str. 15) .

3. Poľské metódy odhaľovania denných kľúčov

V následujúcej kapitole sa budem venovať dvom poľským metódam (Rejewského bomba a Zygalského plachty), ktoré boli schopné z denných kľúčov odhaliť poradie rotorov, a *ring-setting* v období používania druhého šifrovacieho protokola. Postupom bolo odhaliť množinu kandidátov na denný kľúč a následne ručným overením každého kandidáta nájsť toho správneho. Nevýhodou týchto dvoch metód bolo, že neodhalili *plugboard-setting*, ale v závere kapitoly uvediem postup, ktorý mohol byť na vypočítanie tohoto nastavenia používaný.

Ako som ukázala v poznámke a príklade v sekcií 1.4.2, sme schopní podľa individuálneho *ground-setting* v indikátore určiť či sa ľavý alebo stredný bubon pootočí pri šifrovaní dvakrát individuálneho kľúča. Preto v následujúcich metódach zvolili najprv isté poradie rotorov (vyberali z troch typov rotorov), a následne k nemu vyfiltrovali z odpočutých správ tie, ktoré nespôsobovali pootočenie ľavého alebo stredného bubna. Naďalej teda budeme predpokladať, že pracujeme s takými správami, pri ktorých sa otáča iba pravý bubon o 1/26 pri každom stlačení klávesy.

Na začiatku každej metódy uvediem citované texty z originálnych zdrojov od Rejewského, ktoré predstavujú jediné existujúce originálne informácie o metódach odhaľovania denných kľúčov, a následne svojími úvahami na texty naviažem a matematicky zdôvodním prečo metódy fungovali.

3.1 Rejewského bomba

> With enough cipher material it can happen that on a given day three messages will be found with keys as in the following example:
>
> `RTJ wah wik`
>
> `HPN raw ktw`
>
> `DQY dwj mwr`
>
> where the first and fourth, the second and fifth, or the third and sixth letters in the keys of all three messages are the same. In this case it is the letter `w`, but it could also be any other letter, just so it is the same in all three messages. Let us assume for the time being that permutation S was the identity. If the ring setting was also identical and if we knew the order of the drums on the shaft, it would be sufficient to set the drums at position `RTJ`; then by striking key `w` three times in a row, the same lamp would light. The same would happen in drum positions `HPN` and `DQY`. The setting of the rings makes the positions of the drums at which this would happen unknown to us, but the differences in the positions will be maintained and thus are known.
>
> One need only construct a device that in principle would consist of sets of drums from six Enigmas and that, preserving the known mu-

> tual differences in the positions of the drums, would turn the drums synchronicaly. After passing through all possible $26^3 = 17\ 576$ positions in a specified time (about two hours), the machine would indicate when three pairs of lamp (the same lamp in each pair) lighted. ...
>
> During this period, permutation S consisted of five to eight transpositions; that is, it changed half the letters on the average. One could therefore expect that a letter that is repeated six times in three measages (the letter `w` in this case) would not be changed by permutation S at least every second time (Rejewski, 1981, str. 226).

Držme sa Rejewského predpokladov, že prepojovacia doska neprehadzuje písmená, teda predstavuje identickú permutáciu, a že sme odpočuli správy s indikátormi:

`RTJ wah wik` (3.1)

`DQY dwj mwr` (3.2)

`HPN raw ikw` (3.3)

(Predpoklad, že prepojovacia doska neprehadzuje písmená slúži len k vysvetleniu princípu používania Rejewského bomby. Reálne Enigma, ktorá správy šifrovala mala prepojovaciu dosku nastavenú podľa denného kľúča.)

Poznáme písmená abecedného krúžku, ktoré bolo vidieť cez okienka na začiatku šifrovania individuálneho kľúča, ale nepoznáme poradie a pozíciu rotorov pod abecednými krúžkami. Jedným riešením ako zistiť toto natočenie je vyskúšať všetkých $26^3 = 17\ 576$ možností písmen, ktoré sa môžu nachádzať pod písmenami na abecedných krúžkoch, pre každé poradie rotorov. Tento útok hrubou silou vykonávala Rejewského bomba.

Použitím Rejewského bomby bolo možné zistiť poradie rotorov a ich *ring-setting* pre daný deň, z ktorého boli tri vyššie indikátory odpočuté. Bomba pozostávala zo spojených šiestich Enigiem, pričom každá jedna bola použitá pre kontrolovanie jednej podmienky. Určovanie podmienok z trojice indikátorov 3.1, 3.2, 3.3, tak ako aj princíp a stavbu Rejewského bomby ilustrujem a vysvetlím v následujúcom príklade.

3.1.1 Príklad používania Rejewského bomby

Predpokladajme, že skúmame poradie rotorov `I II III` a predpokladajme, že je to správne poradie, ktoré šifrovalo tri odpočuté správy. Označme si $(\widetilde{z_1}, \widetilde{y_1}, \widetilde{x_1})$ trojicu písmen na rotoroch, ktoré sú zakryté trojicou `RTJ` na abecednom krúžku z indikátora 3.1. Trojica $(\widetilde{z_1}, \widetilde{y_1}, \widetilde{x_1})$ teda tvorí začiatočnú pozíciu rotorov, ktorým prvý indikátor bol šifrovaný. Rovnako tak označme $(\widetilde{z_2}, \widetilde{y_2}, \widetilde{x_2})$ a $(\widetilde{z_3}, \widetilde{y_3}, \widetilde{x_3})$ písmená na rotoroch, ktoré sú zakryté trojicami `DQY` a `HPN` z indikátorov 3.2 a 3.3. Ďalej nech $k_1\ l_1\ m_1$ je nezašifrovaný individuálny kľúč k indikátoru 3.1, $k_2\ l_2\ m_2$ k 3.2 a $k_3\ l_3\ m_3$ k 3.3. Podotknem, že písmená k_1, l_2 a m_3 nemusia byť rovnaké písmená. Trojice $(\widetilde{z_1}, \widetilde{y_1}, \widetilde{x_1})$, $(\widetilde{z_2}, \widetilde{y_2}, \widetilde{x_2})$ a $(\widetilde{z_3}, \widetilde{y_3}, \widetilde{x_3})$, tak ako aj individuálny kľúč, sú pre nás neznáme a chceme ich zistiť.

Z indikátorov vieme, že s nastavenou prepojovacou doskou podľa denného kľúča a správnym natočením rotorov (teda *ring-setting*) Enigma s pozíciou bubnov `RTJ` stlačením písmena k_1 vracia písmeno `w`, a rovnako s pozíciou bubnov

`RT(J+3)`, teda `RTM`, stlačením písmena k_1 vracia písmeno `w` (z indikátora 3.1). Ďalej `DQ(Y+1)`, teda `DQZ`, stlačením písmena l_2 vracia písmeno `w`, keďže `w` sa nachádza až na druhom mieste v šestici zašifrovaného individuálneho kľúča, a `DQ(Y+4)`, teda `DQC`, stlačením písmena l_2 vracia `w` (z indikátora 3.2). Nakoniec `HP(N+2)`, teda `HPP`, stlačením písmena m_3 vracia `w`, a rovnako `HP(N+5)`, teda `HPS`, stlačením písmena m_3 vracia `w` (z indikátora 3.3). Naďalej budeme ale predpokladať, že správy sú šifrované s prepojovacou doskou predstavujúcou identitu, a že aj tak spĺňajú vyššie zmienené šifrovania v tomto odstavci.

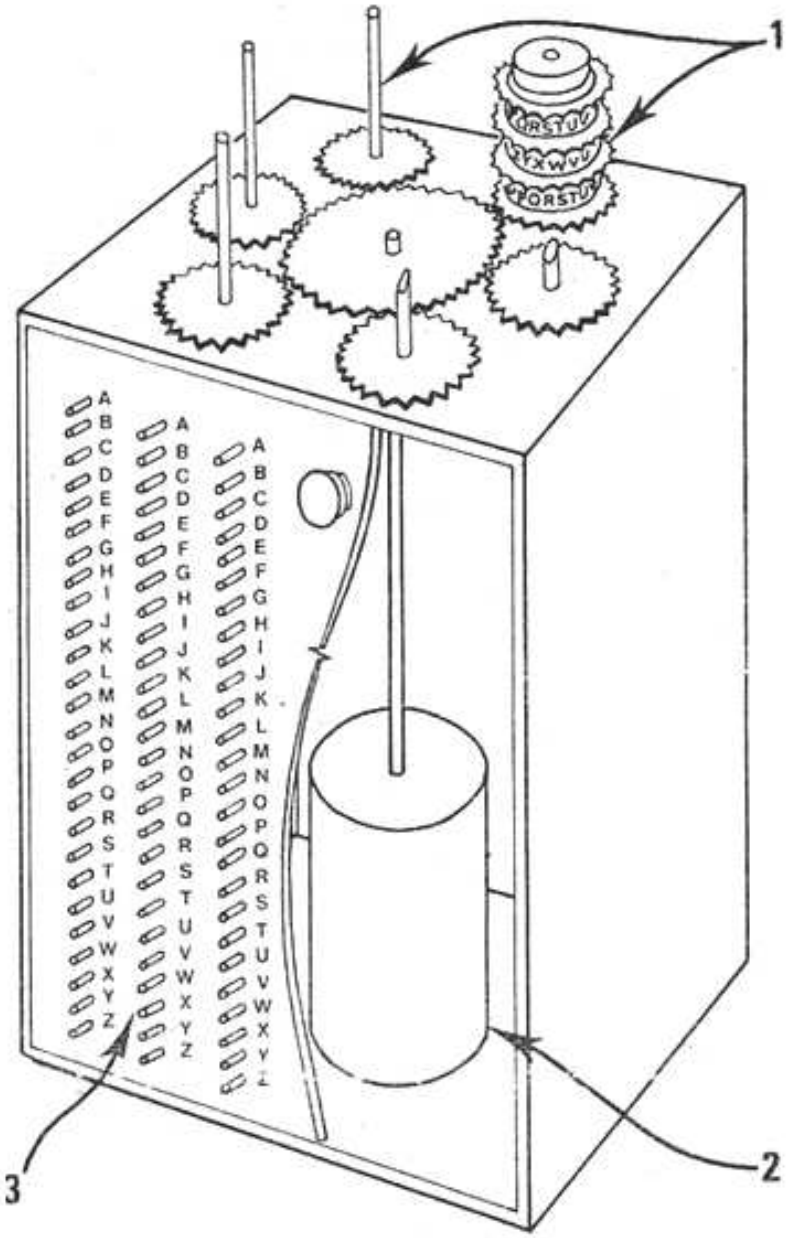
Ako som už vyššie zmienila, Rejewského bomba (obr. 3.1) pozostáva zo šiestich Enigiem. Každá Enigma neobsahuje abecedné krúžky, teda naše vymyslené písmená na rotoroch sú odkryté. Enigmy sú rozdelené do troch dvojíc, pričom rotory každej Enigmy v druhej a tretej dvojici sú posunuté vzhľadom k rotorom prvej dvojice. Bomba nepoužíva prepojovaciu dosku, teda Enigmy v bombe šifrujú s prepojovacou doskou, ktorá nemá prepojené žiadne písmená.

Pred spustením bomby rotory prvej dvojice Enigiem nastavíme do pozície (z_1, y_1, x_1) a $(z_1, y_1, x_1{+}3)$, keďže vieme že pri správnej pozícii rotorov by obidvoje natočenia mali podľa indikátora 3.1 vracať rovnaké písmeno stlačením písmena `w`. Rotory druhej dvojice nastavíme na $(z_2,\ y_2,\ x_2) = (z_1 + 12,\ \ y_1 + 23,\ \ x_1 + 15)$ a $(z_2,\ y_2,\ x_2 + 3) = (z_1 + 12,\ \ y_1 + 23,\ \ x_1 + 18)$. Rotory poslednej dvojice na $(z_3, y_3, x_3) = (z_1{+}16,\ y_1{+}22,\ x_1{+}4)$ a $(z_3, y_3, x_3{+}3) = (z_1{+}16,\ y_1{+}22,\ x_1{+}7)$. Ako som prišla k týmto relatívnym natočeniam vzhľadom k prvej trojici ukážem v dôkaze správnosti algoritmu používania Rejewského bomby v sekcii 3.1.2.

Každá dvojica Enigiem v bombe kontroluje jeden z indikátorov. Bomba bude postupne za $(z_1,\ y_1,\ x_1)$ voliť všetkých 26^3 možných pozícií rotorov, napr. začne na $(z_1,\ y_1,\ x_1) =$ `(Z, Z, Z)`, vyhodnotí rovnosť podmienok, a ďalej skúša `Z Z A`, `Z Z B`, atď. Bomba synchronne posúva rotory na všetkých šiestich Enigmách, a preto zamieňaním $(z_1,\ y_1,\ x_1)$ sa menia aj pozície rotorov v každej dvojici, ale relatívne vzdialenosti všetkých rotorov vzhľadom k prvej dvojici, a teda voľbe $(z_1,\ y_1,\ x_1)$, stále spĺňajú rovnosti z predošlého odstavca. Bomba teda používa krokovací mechanizmus iba v tom zmysle, že po otočení všetkých pravých rotorov 26-krát posunie o jedna všetky stredné rotory, a neskôr po otočení všetkých stredných rotorov 26-krát pootočí všetky ľavé rotory o jedna, atď., aby bomba vyskúšala všetkých 26^3 možných pozícií rotorov.

Pri každej možnej pozícii rotorov $(z_1,\ y_1,\ x_1)$ je do bomby vpustený prúd z písmena `w`, akoby sme pri každej možnej pozícii rotorov stláčali klávesu `w`. Bomba vyhodnotí či sa výstupy dvoch Enigiem v každej dvojici rovnajú. Ak áno, tak sa bomba zastaví, čím nám ukáže kandidáta na správnu trojicu $(\widetilde{z_1},\ \widetilde{y_1},\ \widetilde{x_1})$. Upozorňujem, že rovnaký výstup z jednej dvojice Enigiem sa nemusí rovnať rovnakému výstupu z inej dvojice Enigiem, ale aj v tomto prípade sa bomba zastaví. Následne spustíme bombu, aby pokračovala s ďalšími možnosťami.

Povedzme, že nám bomba vrátila $(z_1,\ y_1,\ x_1) =$ `(A, B, C)`, a predpokladajme, že je to správna pozícia rotorov $(\widetilde{z_1},\ \widetilde{y_1},\ \widetilde{x_1})$. Aby sme zistili *ring-setting*, tak stačí na rotory v pozícii `(A, B, C)` nasunúť abecedný krúžok tak, aby pod písmenami `RTJ` z indikátora 3.1 sa nachádzali písmená `ABC`. Vzdialenosti `A`$-$`R`, `B`$-$`T`, `C`$-$`J` nám jednoznačne určujú rozdiely medzi písmenami na abecednom krúžku a písmenami nachádzajúcimi sa pod nimi na rotoroch. Napríklad v našom prípade `A`$-$`R` $= 9$, teda na ľavom bubne sa každé písmeno na abecednom krúžku nachádza nad písmenom vzdialeným v abecede o 9 písmen. Vďaka vzdialenostiam vieme vypočítať



Obr. 3.1: Nákres Rejewského bomby. Na vrchnej strane stroja môžeme vidieť šesť miest pre vloženie trojíc rotorov, ktoré sú synchronne otáčané motorom nachádzajúcim sa vo vnútri stroja. Zdroj (Reuvers a Simons, a)

ktoré písmeno má byť uchytené pinou, keďže tá ukazuje vždy na začiatočný kolík a kontakt rotoru, teda písmeno `a`. Tým dostávame *ring-setting*. V našom prípade je teda *ring-setting* (`A`+9, `A`+8, `A`+19) = (`J, I, T`) (Copeland, 2004, str. 239-245). Zistili sme, že hľadanie *ring-setting* je ekvivalentné hľadaniu trojice pozície rotorov (z_1, y_1, x_1), ktorá splňuje isté podmienky dané indikátormi.

Vypustime už predpoklad, že Enigma šifrujúca tri indikátory mala identickú prepojovaciu dosku. V predošlom odstavci sme predpokladali, že kandidát vrátený bombou bol správny. Bomba ale pre jedno poradie rotorov vracia množinu kandidátov, s ktorých sa každý musí ručne overiť. Na to, aby sme určili či je kandidát

správny alebo falošný, musíme najprv začať ručne odhaľovať prepojenia v prepojovacej doske z daného dňa, a až potom sme schopní určiť správneho kandidáta ak odhaľovaním prepojení v doske ku danému kandidátovi dostaneme dešifrovaním odpočutej správy zmysluplný text, alebo resp. ak pri odhaľovaní prepojení narazíme na spor. Tejto metóde sa budem venovať v závere tejto kapitoly.

3.1.2 Matematické odôvodnenie

V následujúcej sekcii dokážem správnosť algoritmu používania Rejewského bomby a jej závislosť na prepojovacej doske. Pre prehľadnosť v dôkaze budem v tejto sekcii miesto permutácie $E_{z,y,x}$ písať $E(z, y, x)$.

Tvrdenie 3. *Predpokladajme, že sme odpočuli tri správy s indikátormi 3.1, 3.2 a 3.3, a nech písmeno* `w` *nie je prepojené v prepojovacej doske s iným písmenom. Potom so správnym poradím rotorov bomba vždy nájde aspoň jedného kandidáta na ring-setting, pričom neminie toho správneho.*

Dôkaz. Nech trojica (z_1, y_1, x_1) je hľadaná správna pozícia rotorov, ktorá šifrovala prvý indikátor, a $k_1\ l_1\ m_1$, $k_2\ l_2\ m_2$ a $k_3\ l_3\ m_3$ sú nezašifrované individuálne kľúče z indikátorov 3.1, 3.2 a 3.3. Ďalej nech trojice (z_2, y_2, x_2) a (z_3, y_3, x_3) predstavujú pozície rotorov pri šifrovaní druhého a tretieho indikátora.

Pozrime sa opäť na indikátory 3.1 a 3.2. Písmená v okienkach pravých bubnov na začiatku šifrovania sú `J` a `Z` keď berieme v úvahe pravý bubon patriaci druhému indikátoru už o jedna pootočený, aby stláčaním písmena l_2 vracal písmeno `w` na 1. a 4. pozícii. Vzdialenosť medzi `J` a `Z` je 16, a tým aj vzdialenosť medzi pozíciami pravých rotorov x_1 a $x_2 + 1$ je 16. Rovnako uvážime vzdialenosti aj pre ľavý a stredný rotor. Dostávame

$$\begin{aligned} 16 &= \texttt{Z} - \texttt{J} = (x_2 + 1) - x_1 \\ 23 &= \texttt{Q} - \texttt{T} = y_2 - y_1 \\ 12 &= \texttt{D} - \texttt{R} = z_2 - z_1 \end{aligned} \tag{3.4}$$

Podobne pre dvojicu indikátorov 3.1 a 3.3

$$\begin{aligned} 6 &= \texttt{P} - \texttt{J} = (x_3 + 2) - x_1 \\ 22 &= \texttt{P} - \texttt{T} = y_3 - y_1 \\ 16 &= \texttt{H} - \texttt{R} = z_3 - z_1 \end{aligned} \tag{3.5}$$

Ďalej z všetkých predošlých rovností dostávame

$$\begin{aligned} x_2 &= x_1 + 15 \\ y_2 &= y_1 + 23 \\ z_2 &= z_1 + 12 \\ \\ x_3 &= x_1 + 4 \\ y_3 &= y_1 + 22 \\ z_3 &= z_1 + 16 \end{aligned} \tag{3.6}$$

čo sú vzťahy, ktoré som už v sekcii 3.1.1 bez zdôvodnenia uviedla.

Trojice (z_1, y_1, x_1), (z_2, y_2, x_2) a (z_3, y_3, x_3) boli doteraz pre nás neznáme, ale zistili sme isté závislosti medzi nimi, viď 3.6, a preto z deviatich neznámich dostávame len tri neznáme (z_1, y_1, x_1). Následne postupujeme natočením rotorov bomby podľa týchto závislostí a bombu spúšťame ako som už ukázala v príklade.

Bomba zastaví práve vtedy keď sú následujúce tri rovnosti splňené

$$\begin{aligned} E(z_1, y_1, x_1)\mathtt{w} &= E(z_1, y_1, x_1 + 3)\mathtt{w} \\ E(z_1 + 12, y_1 + 23, x_1 + 15)\mathtt{w} &= E(z_1 + 12, y_1 + 23, x_1 + 15 + 3)\mathtt{w} \\ E(z_1 + 16, y_1 + 22, x_1 + 4)\mathtt{w} &= E(z_1 + 16, y_1 + 22, x_1 + 4 + 3)\mathtt{w} \end{aligned} \tag{3.7}$$

ktoré predstavujú reálne šifrovanie písmena `w` v indikátoroch Enigmou bez prepojovacej dosky (teda tou, ktorou šifrovali poliaci).

Bomba podľa predpokladov skúma správne poradie rotorov. Aby sme dokázali, že medzi kandidátmi pri ktorých bomba zastavila je aj správny kandidát, musíme ešte dokázať, že rovnosti z 3.7 sú ekvivalentné s

$$\begin{aligned} S^{-1}E(z_1, y_1, x_1)S\mathtt{w} &= S^{-1}E(z_1, y_1, x_1 + 3)S\mathtt{w} = k_1 \\ S^{-1}E(z_2, y_2, x_2 + 1)S\mathtt{w} &= S^{-1}E(z_2, y_2, x_2 + 1 + 3)S\mathtt{w} = l_2 \\ S^{-1}E(z_3, y_3, x_3 + 2)S\mathtt{w} &= S^{-1}E(z_3, y_3, x_3 + 2 + 3)S\mathtt{w} = m_3 \end{aligned} \tag{3.8}$$

čo sú rovnosti predstavujúce reálne šifrovanie písmena `w` v indikátoroch Enigmou s prepojovacou doskou nastavenou podľa denného kľúča (teda tou, ktorou šifrovali nemci).

Prenásobením rovností 3.8 zľava permutáciou S dostávame

$$\begin{aligned} E(z_1, y_1, x_1)S\mathtt{w} &= E(z_1, y_1, x_1 + 3)S\mathtt{w} = Sk_1 \\ E(z_2, y_2, x_2 + 1)S\mathtt{w} &= E(z_2, y_2, x_2 + 1 + 3)S\mathtt{w} = Sl_2 \\ E(z_3, y_3, x_3 + 2)S\mathtt{w} &= E(z_3, y_3, x_3 + 2 + 3)S\mathtt{w} = Sm_3 \end{aligned} \tag{3.9}$$

a keďže z predpokladu tvrdenia sa $S\mathtt{w} = \mathtt{w}$, tak 3.9 sa rovnajú

$$\begin{aligned} E(z_1, y_1, x_1)\mathtt{w} &= E(z_1, y_1, x_1 + 3)\mathtt{w} = Sk_1 \\ E(z_2, y_2, x_2 + 1)\mathtt{w} &= E(z_2, y_2, x_2 + 1 + 3)\mathtt{w} = Sl_2 \\ E(z_3, y_3, x_3 + 2)\mathtt{w} &= E(z_3, y_3, x_3 + 2 + 3)\mathtt{w} = Sm_3 \end{aligned} \tag{3.10}$$

čo z 3.6 je 3.7. A teda sú ekvivalentné, čím sme zároveň dokázali, že Rejewského bomba závisí na prepojovacej doske, a že predpoklad, že písmeno ktoré do bomby vpúšťame nie je v doske prepojené s iným je dôležitý. Ak by sa $S\mathtt{w} \neq \mathtt{w}$, potom by 3.7 a 3.8 neboli ekvivalentné a preto by bomba pri správnej hľadanej pozícii rotorov nezastala.

□

3.1.3 Nevýhoda Rejewského bomby

V matematickom odôvodnení správnosti Rejewského bomby som ukázala, že nevýhoda používania Rejewského bomby spočívala v jej závislosti na prepojovacej doske, a že dôležitým predpokladom v našom príklade bola neprepojenosť

písmena `w` v prepojovacej doske. Pokým sa používalo len šesť káblov, a teda spolu 12 písmen sa doskou menilo, tak pravdepodobnosť, že jedno písmeno (v našom prípade písmeno `w`) bolo prepojovacou doskou zmenené bola približne 46% ($12/26 \approx 0.46$).

Neskôr sa ale používalo až 10 a viac káblov, čím pravdepodobnosť, že jedno písmeno bolo doskou zmenené bola aspoň 77% ($20/26 \approx 0.77$). S touto pravdepodobnosťou začínala byť Rejewského bomba už nespoľahlivá, a preto začali používať rýchlejšiu metódu, ktorá dokonca nezávisela na prepojovacej doske.

3.2 Zygalského plachty

> For each of the 26 possible positions of drum L, a square partitioned into 51 x 51 smaller squares is drawn on a large sheet of paper (about 60 x 60 cm). The square is labeled with the consecutive letters of the alphabet: the letters `A` through `Z` followed by `A` through `Y` are written along the sides, on the top, and on the bottom of each square. This was, as it were, a coordinate system in which the abscissa and ordinate denoted consecutive possible positions of drums M and N (*pozn.* Rejewski značil pravý rotor písmenom N), and each small square denoted a permutation with of without one-letter cycles corresponding to that position. Squares with one-letter cycles were perforated. ...
>
> When these sheets of paper were placed on top of each other according to a precisely defined program, in proper order and properly displaced with respect to each other, the number of perforations showing through gradually decreased. If an adequate number of keys with one-letter cycles were at hand, at the end one perforation remained showing through all the sheets of paper, most likely corresponding to a good case.
>
> The order of the drums was derived from the identity of the set to which the sheets of paper belonged. From the position of the perforation and the letter on the paper, we could compute the settings of the rings, and by comparing the letters of the keys with the letters in the machine, we could obtain permutation S - that is, the entire daily key (Rejewski, 1981, str. 227).

Na rovnakom princípe ako Rejewského bomba sú založené Zygalského plachty, ktorých používanie narozdiel od používania bomby nezáviselo na prepojovacej doske.

Metóda Zygalského plachiet využíva informáciu o tom, či permutácia DA (zadefinovaná v kapitole 2) obsahuje fixný bod. Plachty neboli vytvorené pre zložené permutácie EB a FC, pretože ak sa dvojice písmen na 2. a 5., alebo 3. a 6. pozícii rovnajú, potom ich môžeme previesť do 1. a 4. pozície točením pravého bubna (túto metódu sme videli v Rejewského bombe).

Predpokladajme, že sme v jednom dni odpočuli správy s indikátormi takými, že písmená na 1. a 4. pozícii sa rovnajú, a teda permutácie DA patriace k jednotlivým indikátorom obsahujú fixný bod. Pripomeňme, že permutácia DA závisí na úvodnej pozícii rotorov každého indikátora. Uvažujme takéto indikátory nachádzajúce sa v tabuľke 3.1.

(1.) BSU aqy afk	(4.) XLV iej iru	(7.) PTJ xzi xpg
(2.) CEH cms cid	(5.) EON nsf nlg	(8.) VJD ieo ini
(3.) EYD hcg hby	(6.) BUG rcj rvu	(9.) MLQ tbl tsn

Tabuľka 3.1: Odpočuté indikátory s fixnými bodmi.
Vygenerované pomocou (Sale, The Zygalsky sheets)

Rovnako aj pri tejto metóde budeme uvažovať, že abecedné krúžky nie sú na rotoroch nasadené, čím sú pozície rotorov odkryté. Ako už bolo zmienené v citácií, pre každé poradie rotorov existovala jedna sada 26-tich plachiet. Plachty boli označné písmenami od `A` do `Z`, pričom každá plachta predstavovala istú pozíciu ľavého rotora pri danom poradí rotorov. Každá plachta obsahovala mriežku s spolu 51×51 štvorčekami. Po všetkých štyroch bokoch boli napísané písmená `A, B, ..., Z, A, B, ..., Y`. Písmená pri hornom a dolnom boku predstavovali možné pozície stredného rotora a písmená pri pravom a ľavom boku predstavovali možné pozície pravého rotora. Teda napr. políčko v `B`-tom stĺpci a `C`-tom riadku na plachte `A`, prezentovalo pri danom poradí rotorov pozíciu rotorov takú, že na vrchu ľavého rotora sme videli `A`, na vrchu stredného rotora `B` a na pravom rotori `C`. Nákres Zygalskej plachty môžeme vidieť na obrázku 3.2.

Dôvodom prečo abecedy na bokoch boli napísané skoro dvakrát je ten, že sa pri algoritme plachty na seba skladali a vzájomne posúvali. Keby sme mali dve plachty na sebe s mriežkou o rozmere len 26×26, tak už po posunutí vrchnej plachty doprava o x políčok by x stĺpcov bolo mimo spodnú plachtu, čím by sme strácali prehľad o informáciách, ktoré plachty nesú.

S tromi rotormi na výber existovalo $6 \times 26 = 156$ plachiet. Neskôr s piatimi rotormi na výber bolo už potrebných $60 \times 26 = 1560$ plachiet, čo už poliaci nedokázali vyrobiť. Naďalej budeme predpokladať, že sa vyberalo len z troch rotorov.

Políčka niesli informáciu o tom či permutácia *DA* definovaná istou pozíciou rotorov danou políčkom, obsahuje fixný bod alebo nie. Ak áno, tak celé políčko bolo vyrezané. Plachty sa presvecovali zdola svetlom, ktoré prechádzalo iba vyrezanými políčkami. Pri útoku sa plachty na seba skladali a posúvali doprava a dole, čím sa redukoval počet vyrezaných políčok, až kým neexistovalo v najlepšom prípade iba jedno políčko, ktoré prepúšťalo svetlo, čo predstavovalo kandidáta na správnu pozíciu rotorov.

3.2.1 Príklad používania Zygalského plachiet

Na príklade ukážem hľadanie správneho poradia rotorov a *ring-setting*, s ktorým boli šifrované indikátory v tabuľke 3.1. Pri správnom dennom nastavení šifrovanie bubnami natočenými podľa prvých troch písmen v indikátoroch by malo dávať rovnaké zašifrované písmená na 1. a 4 pozícii, teda permutácie *DA* k jednotlivým indikátorom by mali obsahovať fixný bod.

Najprv vyberieme sadu plachiet, ktorá patrí istému poradiu rotorov, napr. `I II III`, a predpokladajme že pri žiadnom indikátore z tabuľky 3.1 sa nepootočil ľavý a stredý rotor. Ďalej si zvolíme konkrétnu správu, napr. (1.) `BSU aqy afk`, a pevné písmeno $z \in \{\texttt{A},\ldots,\texttt{Z}\}$, napr. $z = \texttt{Z}$, ktoré bude predstavovať výber skúmanej plachty, a teda náš tip na správnu pozíciu ľavého rotora. Tým naša

hypotéza je, že na abecednom krúžku písmeno B leží nad písmenom Z. Na plachte vídíme všetkých $26 \times 26 = 676$ možných dvojíc $[y][x]$ predstavujúcich možné pozície stredného a pravého rotora. Z nich nás zaujímajú len tie, ktorých políčka sú vyrezané.

Z relatívnych vzdialeností indikátorov (1.) a (2.) určíme, že na plachtu Z máme položiť plachtu $\mathtt{A} = \mathtt{Z} + (\mathtt{C} - \mathtt{B})$ posunutú do prava o $12 = \mathtt{E} - \mathtt{S}$ a dole o $13 = \mathtt{H} - \mathtt{U}$ políčok. Presvietením plachiet svetlom zdola svetlo prechádza len tými dvomi políčkami nad sebou, ktoré sú obe vyrezané, čo nám zmenšuje množinu vyrezaných políčok na prvej plachte Z na tie políčka $[y][x]$, ktoré s pozíciou rotorov (Z, y, x) a zároveň pozíciou (A, $y + 12$, $x + 13$) dávajú fixné body.

Ďalej z relatívnych vzdialeností indikátorov (1.) a (3.) vieme, že položením plachty $\mathtt{C} = \mathtt{Z} + (\mathtt{E} - \mathtt{B})$, posunutej o $6 = \mathtt{Y} - \mathtt{S}$ políčok doprava a o $9 = \mathtt{D} - \mathtt{U}$ dole na plachty Z a A sa opäť počet políčok prepúšťajúcich svetlo zredukuje iba na tie políčka $[y][x]$, v ktorých pozície rotorov (Z, y, x), (A, $y + 12$, $x + 13$) a (C, $y + 6$, $x + 9$) zároveň dávajú fixné body.

Rovnakým algoritmom na plachty Z, A a C pokladáme ďalšie plachty pomocou ďalších správ, kým nedostávame jediného kandidáta (alebo veľmi malú množinu kandidátov) na pozíciu rotorov. Odoberieme všetky plachty až na najspodnejšiu plachtu Z, a pozrieme sa, ktoré políčko $[y][x]$ definujúce jednoznačne pozíciu rotorov splňuje predošlé úvahy. Povedzme, že týmto políčkom je [A][B], a teda kandidátom je (Z, A, B). Pre zistenie *ring-setting* použijeme rovnaký postup ako pri používaní Rejewského bomby, teda otočíme rotory do pozície (Z, A, B) a nasunieme abecedné krúžky tak, aby písmeno B sa nachádzalo nad Z, písmeno S nad A, a U nad B.

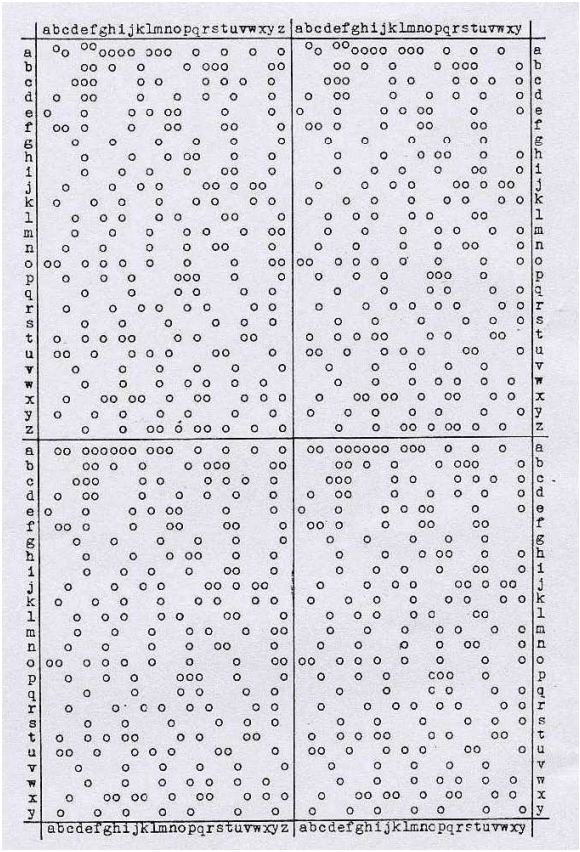
Rovnako ako pri Rejewského bombe, aj v tejto metóde nedostávame žiadnu informáciu o individuálnom kľúči a prepojení v prepojovacej doske, ale iba poradie rotorov a *ring-setting*. A rovnako tiež dostávame množinu kandidátov, z ktorých musíme ručne určiť toho správneho. Aj pri tejto metóde sa správnosť kandidáta určí až pri ručnom odhaľovaní prepojovacej dosky, ktoré popíšem v závere kapitoly.

Na konci algoritmu prekrývania plachtami sa môže stať, že žiadne políčko neprepúšťa svetlo. To môže znamenať: Buď naša hypotéza bola nesprávná a teda pozícia ľavého rotora sa nerovná Z, alebo ak ani po uskutočnení 26-tich hypotéz nedostávame správnú pozíciu rotorov, tak sme testovali zlé poradie rotorov. V prvom prípade zvolíme novú hypotézu na písmeno z, napr. A, a vykonávame celý algoritmus odznova. V druhom prípade zameníme poradie rotorov na napr. I III II, a znovu volíme správy a hypotézy na pozíciu ľavého rotora.

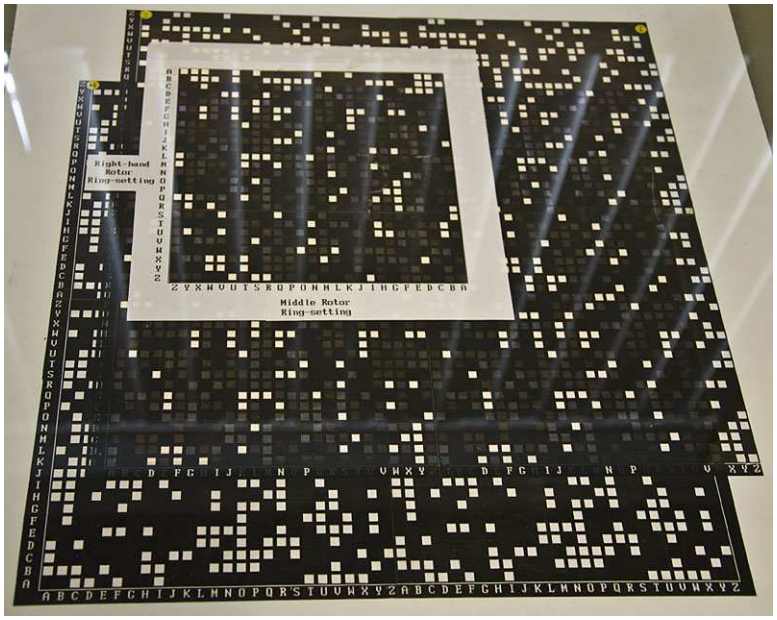
Narozdiel od Rejewského bomby sme nepotrebovali predpokladať, že 1. a 4. písmeno zašifrovaného individuálneho kľúča nie je zmenené prepojovacou doskou. V algoritme používame iba informáciu, či permutácia DA obsahuje fixný bod alebo nie. Aj keby 1. a 4. písmeno bolo zmenené prepojovacou doskou, tak informácia o DA by bola rovnaká.

3.2.2 Matematické odôvodnenie

V následujúcej sekcii dokážem správnosť metódy Zygalských plachiet a ich nezávislosť na prepojovacej doske.



Obr. 3.2: Nákres Zygalského plachty. Koliečka predstavujú vyrezané políčka. Nákres obsahuje chybu v prvom riadku, kde koliečka pri písmenách `b`, `e` a `f` sú zobrazené mimo riadka. Zdroj (Rejewski, 1980)



Obr. 3.3: Fotografia dvoch plachiet. Vidíme, že prekrytím prvej plachty druhou sa počet presvetlených políčok znížil. Zdroj `http://www.garnek.pl/forum/enigma`

Definícia 4. *Nech poradie rotorov je* `I II III`*. Nech pre* z, y, $x \in \{$`A,...,Z`$\}$

je $(z,\ y,\ x)$ *pozícia rotorov. Definujeme zobrazenie*

$$\prod_{z}^{I\ II\ III}(y,\ x):\ \mathbb{Z}_{26}\times\mathbb{Z}_{26}\to\mathbb{Z}_2$$

nadobúdajúce hodnotu 1, ak permutácia DA, kde

$$D=S^{-1}P^{-(x+4)}R^{-1}P^{(x+4)}TP^{-(x+4)}RP^{(x+4)}S$$

$$A=S^{-1}P^{-(x+1)}R^{-1}P^{(x+1)}TP^{-(x+1)}RP^{(x+1)}S$$

a $T=P^{-y}M^{-1}P^{y}P^{-z}L^{-1}P^{z}QP^{-z}LP^{z}P^{-y}MP^{y}$ *obsahuje fixný bod, a 0 ak DA neobsahuje fixný bod.*

Definícia 5 (matematický model Zygalského plachty)**.** *Zygalského plachta patriaca písmenu* $z\in\{\texttt{A},\ldots,\texttt{Z}\}$ *s poradím rotorov* `I II III` *je matica* M_z *rádu* 26 *nad telesom* $\mathbb{Z}_2$*, kde na mieste* $(y,\ x)$ *pre každé* $y,\ x\in\{\texttt{A},\ldots,\texttt{Z}\}$ *sa nachádza hodnota*

$$\prod_{z}^{(I.\ II.\ III)}(y,\ x)$$

Ďalej už informáciu o poradí rotorov do zobrazenia písať nebudeme. Ak zobrazenie $\prod_z(y,\ x)$ nadobúda hodnotu 1, tak na reálnej plachte patriacej písmenu z je políčko v y-tom stĺpci a x-tom riadku vyrezané. A je permutácia predstavujúca šifrovanie rotormi v pozícii $(z,\ y,\ x+1)$, a D šifrovanie rotormi v pozícii $(z,\ y,\ x+4)$.

Tvrdenie 4. *Predpokladajme, že sme odpočuli správy s indikátormi v tabuľke 3.1. Potom so správnym poradím rotorov metódou Zygalského plachiet nájdeme aspoň jedného kandidáta na ring-setting, pričom neminieme toho správneho.*

Dôkaz. To, že prepojovacia doska nemení štruktúru cyklov som už dokázala v Tvrdení 2, a preto nemení ani informáciu, na ktorej sú Zygalského plachty založené, a teda nezávisia na prepojovacej doske.

Nech sme zvolili správnu hypotézu voľby prvej plachty z a nech správna pozícia rotorov, ktorá šifrovala indikátor (1.) v tabuľke 3.1 je $(z,\ y,\ x)$. Pozrime sa na ďalšie indikátory v tabuľke. Vďaka prvým trom písmenám v indikátoroch vieme určiť vzdialenosti medzi písmenami, ktoré určujú pozíciu rotorov pod abecednými krúžkami, aj keď tieto písmená nepoznáme, rovnako ako pri Rejewského bombe. Písmeno, ktoré určuje pozíciu ľavého rotora pri šifrovaní $(i.)$-teho indikátora v tabuľke budeme značiť z_i. Rovnako y_i a x_i pre stredný a pravý rotor. (*pozn.* so značením sa teda $(z,\ y,\ x)=(z_1,\ y_1,\ x_1)$)

Z indikátora (1.) vieme, že zložená permutácia DA, kde

$$D=S^{-1}P^{-(x+4)}R^{-1}P^{(x+4)}TP^{-(x+4)}RP^{(x+4)}S$$

$$A=S^{-1}P^{-(x+1)}R^{-1}P^{(x+1)}TP^{-(x+1)}RP^{(x+1)}S$$

a $T=P^{-y}M^{-1}P^{y}P^{-z}L^{-1}P^{z}QP^{-z}LP^{z}P^{-y}MP^{y}$, obsahuje fixný bod keďže 1. a 4. písmeno indikátora sa rovnajú, a teda podľa definície 4

$$\prod_{z}(y,\ x)=1 \tag{3.11}$$

Uvažujme indikátor (2.). Z relatívnych vzdialeností

$$\begin{aligned} 1 &= \mathtt{C} - \mathtt{B} = z_2 - z \\ 12 &= \mathtt{E} - \mathtt{S} = y_2 - y \\ 13 &= \mathtt{H} - \mathtt{U} = x_2 - x \end{aligned} \tag{3.12}$$

vieme určiť, že keď ľavý rotor natočíme do pozície $z + (\mathtt{C} - \mathtt{B}) = z + 1$, stredný rotor natočíme do pozície $y + (\mathtt{E} - \mathtt{S}) = y + 12$ a pravý rotor do pozície $x + (\mathtt{H} - \mathtt{U}) = x + 13$, tak zložená permutácia DA, kde

$$D = S^{-1}P^{-(x+13+4)}R^{-1}P^{(x+13+4)}TP^{-(x+13+4)}RP^{(x+13+4)}S$$

$$A = S^{-1}P^{-(x+13+1)}R^{-1}P^{(x+13+1)}TP^{-(x+13+1)}RP^{(x+13+1)}S$$

a $T = P^{-(y+12)}M^{-1}P^{(y+12)}P^{-(z+1)}L^{-1}P^{(z+1)}QP^{-(z+1)}LP^{(z+1)}P^{-(y+12)}MP^{(y+12)}$, obsahuje tiež fixný bod, a teda

$$\prod_{z+1}(y + 12,\, x + 13) = 1 \tag{3.13}$$

Rovnako z indikátora (3.) dostávame

$$\begin{aligned} 3 &= \mathtt{E} - \mathtt{B} = z_3 - z \\ 6 &= \mathtt{Y} - \mathtt{S} = y_3 - y \\ 9 &= \mathtt{D} - \mathtt{U} = x_3 - x \end{aligned} \tag{3.14}$$

a pre rotory v pozíciách $z + (\mathtt{E} - \mathtt{B}) = z + 3$, $y + (\mathtt{Y} - \mathtt{S}) = y + 6$ a $x + (\mathtt{D} - \mathtt{U}) = x + 9$ opäť platí, že zložená permutácia DA, kde

$$D = S^{-1}P^{-(x+9+4)}R^{-1}P^{(x+9+4)}TP^{-(x+9+4)}RP^{(x+9+4)}S$$

$$A = S^{-1}P^{-(x+9+1)}R^{-1}P^{(x+9+1)}TP^{-(x+9+1)}RP^{(x+9+1)}S$$

a $T = P^{-(y+6)}M^{-1}P^{(y+6)}P^{-(z+3)}L^{-1}P^{(z+3)}QP^{-(z+3)}LP^{(z+3)}P^{-(y+6)}MP^{(y+6)}$, obsahuje fixný bod, a teda znovu

$$\prod_{z+3}(y + 6,\, x + 9) = 1 \tag{3.15}$$

Pre každý z indikátorov (4.) až (9.) by sme rovnakým algoritmom dostali ďalšie podmienky $\prod_{z+a_j}(y + b_j,\, x + c_j) = 1$, kde $a_j,\, b_j,\, c_j \in \mathbb{Z}_{26}$ pre $j = 4,\, ...,\, 9$.

Spolu dostávame

$$\prod_{z}(y,\, x) = \prod_{z+1}(y + 12,\, x + 13) = \prod_{z+3}(y + 6,\, x + 9) = ... = 1 \tag{3.16}$$

a teda hľadanie kandidáta na *ring-setting* je ekvivalentné hľadaniu takej trojice pozície rotorov $(z,\, y,\, x)$, ktorá splňuje 3.16, keďže po jej nájdení už vieme odvodiť *ring-setting* rovnakým spôsobom ako pri Rejewského bombe. Keďže hľadaná správna pozícia rotorov určite splňuje tieto rovnosti, algoritmus správneho kandidáta neminie.

□

Podobnosť používania Zygalského plachiet a používania Rejewského bomby môžeme vidieť v tom, že aj v tejto metóde si najprv určíme niekoľko obmedzujúcich podmienok (viď 3.16 a 3.7) na kandidátov (z, y, x), a potom hrubou silou skúšame všetky možné trojice písmen, pričom kontrolujeme, či tieto podmienky sú splnené. Zygalského plachty sú ale rýchlejšie, keďže nemusíme prechádzať všetkými možnými 676-timi pozíciami stredného a pravého rotora, ale už ich rovno všetky vidíme na jednej plachte. Svetlo sa v plachtách chová ako elektrický prúd v bombe a hneď vyraďuje pozície, ktoré nepredstavujú fixný bod.

3.3 Zisťovanie prepojovacej dosky

Pomocou používania Rejewského bomby alebo Zygalského plachiet boli poliaci schopní zistiť poradie rotorov a *ring-setting* pre daný deň. Z denných kľúčov druhého protokola šifrovania nám zostáva neznáme ešte prepojenie písmen v prepojovacej doske v danom dni (*plugboard-setting*) a individuálny kľúč každej odpočutej správy. Vieme ale, že individuálny kľúč dostaneme dešifrovaním indikátora Enigmou nastavenou podľa denného kľúča, a teda zistením prepojení písmen v prepojovacej doske zistíme automaticky aj individuálne kľúče. Naším cieľom bude teda zistiť permutáciu S.

Opäť aj táto metóda odhaľovania prepojovacej dosky nebola v originálnych zdrojoch dostatočne popísaná. Budeme vychádzať iba z následujúcej vety z Rejewského článku nadvezujúcej na výsledok metódy používania Zygalského plachiet:

> From the position of the perforation and the letter on the paper, we could compute the settings of the rings, and by comparing the letters of the keys (pozn. indikátorov) with the letters in the machine, we could obtain permutation S - that is, the entire daily key (Rejewski, 1981, str. 227).

Podľa informácie v uvedenej vete sme došli k metóde, ktorá mohla byť využívaná pri hľadaní prepojení v prepojovacej doske. Metódu opäť vysvetlím na príklade. Predpokladajme, že sme použitím Rejewského bomby alebo Zygalského plachiet zistili poradie rotorov a *ring-setting*. Vyfiltrujme z odpočutých správ tie, ktorých šifrovanie individuálneho kľúča pri danom poradí rotorov nepootočilo ľavý a stredný rotor. Ďalej predpokladajme, že medzi vyfiltrovanými správami boli aspoň dve správy s indikátormi obsahujúcimi rovnaké písmená na 1. a 4. pozícii, napr.

$$\begin{aligned} &(1.)\ \texttt{HSP}\ \underline{\texttt{a}}\texttt{qi}\ \underline{\texttt{a}}\texttt{zl} \\ &(2.)\ \texttt{KVO}\ \underline{\texttt{a}}\texttt{sr}\ \underline{\texttt{a}}\texttt{mb} \end{aligned} \tag{3.17}$$

Pripomeňme, že permutácie A a D (ktoré definujú permutáciu šifrovania písmen na 1. a 4. pozícii indikátora) závisia na zvolenom individuálnom *ground-setting*, teda na `HSP` alebo `KVO`. Teda aj zložená permutácia DA závisí na zvolenom individuálnom *ground-setting* správy.

Podľa kapitoly 2 definujme

$$(DA)_{(1.)} = S^{-1}E(z_1, y_1, x_1 + 3)E(z_1, y_1, x_1)S \tag{3.18}$$

ako permutáciu DA patriacu indikátoru (1.) a

$$(DA)_{(2.)} = S^{-1}E(z_2,\, y_2,\, x_2+3)E(z_2,\, y_2,\, x_2)S \tag{3.19}$$

ako permutáciu DA patriacu indikátoru (2.). Permutácie $(DA)_{(1.)}$ a $(DA)_{(2.)}$ ale nepoznáme, keďže sú zložené z permutácií predstavujúcich šifrovanie Enigmou nastavenou podľa denného kľúča, teda obsahujú permutáciu S, ktorú nepoznáme.

Z kapitoly 2 a z oboch indikátorov vieme, že

$$\begin{aligned}(DA)_{(1.)}\mathtt{a} &= \mathtt{a}\\ (DA)_{(2.)}\mathtt{a} &= \mathtt{a}\end{aligned} \tag{3.20}$$

teda vieme, že `a` je fixný bod permutácií $(DA)_{(1.)}$ a $(DA)_{(2.)}$.

Keďže poznáme *ring-setting* a individuálne *ground-setting* obidvoch indikátorov, vieme zistiť aj $(z_1,\, y_1,\, x_1)$ a $(z_2,\, y_2,\, x_2)$, a teda vieme vypočítať celé permutácie

$$(\widetilde{D}\widetilde{A})_{(1.)} = E(z_1,\, y_1,\, x_1+3)E(z_1,\, y_1,\, x_1) \tag{3.21}$$

a

$$(\widetilde{D}\widetilde{A})_{(2.)} = E(z_2,\, y_2,\, x_2+3)E(z_2,\, y_2,\, x_2) \tag{3.22}$$

ktoré predstavujú zloženie permutácií predstavujúcich šifrovanie Enigmou nastavenou podľa denného kľúča bez prepojovacej dosky, a to následovne: Pre zistenie permutácie $(\widetilde{D}\widetilde{A})_{(1.)}$ pre každé písmeno abecedy nastavíme Enigmu do pozície $(z_1,\, y_1,\, x_1)$, zašifrujeme dané písmeno, pootočíme pravý rotor o tri pozície a znovu zašifrujeme dané písmeno abecedy. Teda v podstate šifrujeme rovnaké písmeno akokeby na 1. a 4. pozícii indikátora. Teda ak sa napr. písmeno `a` na 1. a 4. pozícii zašifrovalo pozíciou rotorov na $(z_1,\, y_1,\, x_1)$

`s·· u··`

a písmeno `b` na

`u·· n··`

a písmeno `f` na

`n·· s··`

potom vieme, že

$$\begin{aligned}(\widetilde{D}\widetilde{A})_{(1.)}\mathtt{s} &= \mathtt{u}\\ (\widetilde{D}\widetilde{A})_{(1.)}\mathtt{u} &= \mathtt{n}\\ (\widetilde{D}\widetilde{A})_{(1.)}\mathtt{n} &= \mathtt{s}\end{aligned}$$

a teda permutácia $(\widetilde{D}\widetilde{A})_{(1.)}$ obsahuje trojcyklus

$$(\mathtt{s},\, \mathtt{u},\, \mathtt{n})$$

Takýmto šifrovaním všetkých písmen abecedy sme schopní vypočítať celú permutáciu $(\widetilde{D}\widetilde{A})_{(1.)}$ a rovnako aj permutáciu $(\widetilde{D}\widetilde{A})_{(2.)}$ šifrovaním s pozíciou rotorov (z_2, y_2, x_2).

V tvrdení 2 sme dokázali, že permutácie $\widetilde{D}\widetilde{A}$ a DA majú rovnakú štruktúru cyklov, keďže sú konjugované permutáciou S. Z následujúceho tvrdenia z (Rejewski, 1980, str. 8) vieme, že permutácie $\widetilde{D}\widetilde{A}$ a DA obsahujú párny počet cyklov rovnakej dĺžky, keďže permutácie D a A obsahujú 13 transpozícií.

Tvrdenie 5. *Ak dve permutácie nad rovnakou množinou pozostávajú z rovnakého počtu transpozíc, potom ich zloženie obsahuje párny počet cyklov rovnakej dĺžky.*

Dôkaz. viď (Rejewski, 1980, str. 8)

□

Ďalšie tvrdenie bude dôležité dokázať pre zistenie celej permutácie S.

Tvrdenie 6. *Písmeno* $\mathtt{a}$ *je fixným bodom permutácie* DA *práve vtedy keď písmeno* $S\mathtt{a}$ *je fixným bodom permutácie* $\widetilde{D}\widetilde{A}$.

Dôkaz. Písmeno $\mathtt{a}$ je fixným bodom DA, a teda

$$DA\mathtt{a} = \mathtt{a} \tag{3.23}$$

Vynásobením rovnosti 3.23 zľava permutáciou a malou úpravou dostávame

$$\underbrace{SDAS^{-1}}_{\widetilde{D}\widetilde{A}} S\mathtt{a} = \widetilde{D}\widetilde{A}S\mathtt{a} = S\mathtt{a} \tag{3.24}$$

a teda písmeno $S\mathtt{a}$ je fixným bodom permutácie $\widetilde{D}\widetilde{A}$.

Platí aj opačná implikácia. Stačí rovnosť $\widetilde{D}\widetilde{A}S\mathtt{a} = S\mathtt{a}$ vynásobiť zľava permutáciou S^{-1} a podobnou úpravou dostaneme $DA\mathtt{a} = \mathtt{a}$.

□

Tvrdenie 6 nám už ukázalo cestu ako zistiť neznáme písmeno $S\mathtt{a}$. Tým, že poznáme celé permutácie $(\widetilde{D}\widetilde{A})_{(1.)}$ a $(\widetilde{D}\widetilde{A}_{(2.)})$, vlastníme aj všetky ich fixné body. Fixnými bodami sú 1-cykly v týchto permutáciách. Z tvrdenia 5 vieme, že ich je párny počet. Z tvrdenia 6 vieme, že

$$\begin{aligned} (DA)_{(1.)}\mathtt{a} = \mathtt{a} \;&\Leftrightarrow\; (\widetilde{D}\widetilde{A})_{(1.)}S\mathtt{a} = S\mathtt{a} \\ (DA)_{(2.)}\mathtt{a} = \mathtt{a} \;&\Leftrightarrow\; (\widetilde{D}\widetilde{A})_{(2.)}S\mathtt{a} = S\mathtt{a} \end{aligned} \tag{3.25}$$

a teda zistili sme, že písmeno $S\mathtt{a}$ sa nachádza v 1-cykloch oboch permutácií $(\widetilde{D}\widetilde{A})_{(1.)}$ a $(\widetilde{D}\widetilde{A})_{(2.)}$. Jediné čo nám už teraz zostáva je pozrieť sa na fixné body oboch permutácií a nájsť to jedno písmeno, ktoré obe obsahujú.

Ak napr. fixné body permutácie $(\widetilde{D}\widetilde{A})_{(1.)}$ sú (k) (w) (x) (t) a fixné body $(\widetilde{D}\widetilde{A})_{(2.)}$ sú (h) (x), potom sme zistili, že $S\mathtt{a} = \mathtt{x}$.

Následne budeme hľadať ďalšie dvojice správ s rovnakými písmenami na 1. a 4. pozícii, aby sme mohli získať prepojenia ďalších písmen.

Doteraz som odhaľovanie ilustrovala na dvojiciach indikátorov s rovnakými písmenami na 1. a 4. pozíciách, ale rovnaký postup funguje aj pre zložené permutácie EB a FC, teda rovnaké písmená na 2. a 5. pozíciách, a 3. a 6. pozíciách.

Dokonca v týchto dvoch prípadoch nám stačí len pootočiť pravý rotor o jednu alebo dve pozície a následne aplikovať postup odhaľovania permutácie S ako vyššie s permutáciou DA.

Nemusí sa nám ale vždy podariť nájsť pre každé písmeno abecedy dva odpočuté indikátory s rovnakými písmenami na daných pozíciách. Majme napríklad indikátor

$$(3.)\ \texttt{OSA}\ \underline{\texttt{q}}\texttt{jv}\ \underline{\texttt{q}}\texttt{pd} \tag{3.26}$$

ku ktorému sme nenašli ďalší taký indikátor s rovnakým písmenom q na 1. a 4. pozícii (alebo podľa predošlého odstavca na 2. a 5. alebo 3. a 6.). Vieme ale, že

$$(DA)_{(3.)}\texttt{q} = \texttt{q} \tag{3.27}$$

a vieme opäť vypočítať podľa vyššie zmieneného algoritmu permutáciu $(\widetilde{DA})_{(3.)}$, čím poznáme aj všetky fixné body permutácie $(\widetilde{DA})_{(3.)}$.

Ako zistiť neznáme písmeno $S\texttt{q}$ nám znovu ukáže tvrdenie 6, ktoré hovorí, že

$$(DA)_{(3.)}\texttt{q} = \texttt{q} \ \Leftrightarrow\ (\widetilde{DA})_{(3.)}S\texttt{q} = S\texttt{q} \tag{3.28}$$

a to znamená, že nám stačí sa pozrieť na fixné body permutácie $(\widetilde{DA})_{(3.)}$ a tie budú kandidátmi na písmeno $S\texttt{q}$, teda kandidátmi na prepojenie písmena q v prepojovacej doske. Aby sme ale vedeli jednoznačne určiť $S\texttt{q}$, musíme pred tým poznať už nejaké prepojené dvojice z predošlých dvojíc indikátorov, ktorých písmená na daných pozíciách sa zhodovali, aby sme mohli vylúčiť sporné prípady. Napr. povedzme, že fixné body permutácie $(\widetilde{DA})_{(3.)}$ sú (d), (x). Z dvojice indikátorov (1.) a (2.) sme ale zistili, že $S\texttt{a} = \texttt{x}$, a preto musí platiť $S\texttt{q} = \texttt{d}$, aby prepojenie písmen nebolo sporné. Ak by fixné body permutácie $(\widetilde{DA})_{(3.)}$ boli (d), (x), (y), (v), potom by sme jednoznačne mohli určiť $S\texttt{q}$ až neskôr s výsledkami z iných indikátorov, keďže v tomto prípade máme na $S\texttt{q}$ tri možnosti.

Existuje ešte jedna možnosť ako odvodiť ďalšie prepojenia písmen v prepojovacej doske aj bez toho, aby sme mali indikátor s fixným bodom. Je ale potrebné už o nejakých dvojiciach v prepojovacej doske vedieť. Vieme, že $S\texttt{q} = \texttt{d}$ a predpokladajme, že sme odpočuli indikátor

$$(4.)\ \texttt{XYZ qbu fhi} \tag{3.29}$$

Povedzme, že vypočítaním permutácie $(\widetilde{DA})_{(4.)}$ podľa vyššie zmieneného algoritmu zistíme, že

$$(\widetilde{DA})_{(4.)}\texttt{d} = \texttt{r} \tag{3.30}$$

Všimnime si, že tvrdenie 6 platí obecne, a nie len pre fixný bod, a teda platí

$$(DA)_{(4.)}\texttt{q} = \texttt{f} \ \Leftrightarrow\ (\widetilde{DA})_{(4.)}S\texttt{q} = S\texttt{f} \tag{3.31}$$

Z $S\texttt{q} = \texttt{d}$ sa 3.30 rovná $(\widetilde{DA})_{(4.)}S\texttt{q} = \texttt{r}$, a teda z 3.31 sme zistili, že $S\texttt{f} = \texttt{r}$. Tým máme ďalší spôsob odhaľovania dvojíc v prepojovacej doske.

Kombináciou predošlých postupov sme schopní zrekonštruovať celé *plugboard-setting*, a teda budeme schopní prečítať akúkoľvek odpočutú správu v daný deň.

Vráťme sa ešte ku výsledkom používania Rejewského bomby alebo Zygalského plachiet. Pri vysvetľovaní postupu odhaľovania permutácie S som predpokladala, že máme správneho kandidáta na poradie rotorov a *ring-setting*. Metódy nám ale vrátia istú množinu kandidátov. Jediným spôsobom ako zistíme toho správneho, je aplikovať na každého jedného kandidáta postup odhaľovania prepojení v prepojovacej doske z tejto sekcie. Pri falošnom kandidátovi by tento postup mal končiť vždy sporom alebo nezmyselným textom získaným dešifrovaním. Správny kandidát vždy algoritmom prejde bez sporu a dešifrovaním odpočutej správy získame zmysluplný text, čím sme zistili celý denný kľúč a dokončili kapitolu o poľských metódach.

4. Anglické metódy odhaľovania denných kľúčov

V poslednej kapitole ukážem ako sa na problém odhaľovania denných kľúčov pozerali angličania na čele s Alanom Turingom. Pred samotným vysvetlením Turingovej bomby a jej fungovania spravím jeden príklad pre pochopenie princípu, na ktorom bomba bola založená. V závere kapitoly sa budem venovať procesom, ktoré hľadanie správnych kandidátov zrýchlili, a komponente vymyslenej Gordonom Welchmanom, ktorá zredukovala počet falošných zastavení bomby.

Rozdiel medzi poľskými a anglickými metódami bol ten, že zatiaľ čo poliaci skúmali len prvých deväť písmen každej správy predstavujúcich individuálny *ground-setting* a šifrovaný individuálny kľúč, angličania k odhaleniu denných kľúčov využívali hlavnú šifrovanú správu. Dôvodom boli obavy z toho, že by nemci prestali šifrovať svoje individuálne kľúče dvakrát, čo sa aj stalo v máji 1940, keď zmenili protokol šifrovania, viď 1.4.3, a teda poľské metódy začali byť nepoužiteľné. Cieľom angličanov bolo vytvoriť metódu, ktorá by fungovala nezávisle na dvakrát šifrovanom individuálnom kľúči, a ktorá by naraz našla všetky časti denného kľúča, teda aj *plugboard-setting*.

4.1 Princíp Turingovej bomby

Predstavme si, že sme odpočuli zašifrovanú správu ku ktorej poznáme poradie rotorov a časť jej nezašifrovaného znenia. Nevieme ale v ktorej časti správy sa táto nezašifrovaná časť nachádza. Známu nezašifrovanú časť správy budeme nazývať *crib*. Ďalej nech poznáme pozíciu všetkých troch rotorov na začiatku šifrovania cribu. Tým poznáme aj celú šifrovaciu transpozíciu pre každý stav, v ktorom sa Enigma nachádzala počas šifrovania cribu až na premenovanie písmen prepojovacou doskou. Pokúsime sa na základe týchto poznatkov nájsť prepojenie dvojíc v prepojovacej doske Enigmy, ktorá správu šifrovala. Rovnako ako v predošlej kapitole budem predpokladať, že počas šifrovania cribu nedošlo k pootočeniu ľavého a stredného rotora.

Najprv musíme zistiť pozíciu časti zašifrovanej správy, ktorá je šifrovaným cribom. Vďaka faktu, že Enigma nikdy nešifruje písmeno na rovnaké písmeno, vieme vylúčiť všetky nemožné pozície cribu v texte jednoduchým porovnávaním. Ak crib umiestnime pod istú časť zašifrovanej správy a aspoň na jednom mieste sa písmeno správy a cribu rovná, tak časť správy nie je zašifrovaný crib a v tom prípade posunieme crib o jedno písmeno ďalej a opakujeme postup. Predpokladajme, že sme vyššie zmienenou metódou našli pozíciu cribu v správe. Samozrejme takých pozícii môže byť viac, ale pre jednoduchosť príkladu predpokladajme, že sme našli práve jednu. V tabuľke 4.1 uvádzam príklad časti takej správy prevzanej z (Turing, 1940, str. 97). Zbytok správy aj so zašifrovaným individuálnym kľúčom nás teraz nebude zaujímať.

Pred tým ako Enigma začala šifrovať časť správy v tabuľke bola v nejakej pozícii rotorov, ktorú budem nazývať *nultá pozícia*. Prvé písmeno cribu `k` sa zašifrovalo na písmeno `d` s pravým rotorom o jedna pootočeným od jeho nultej pozície. Nastavenie Enigmy s touto pozíciou rotorov vhľadom k nultej pozícii ro-

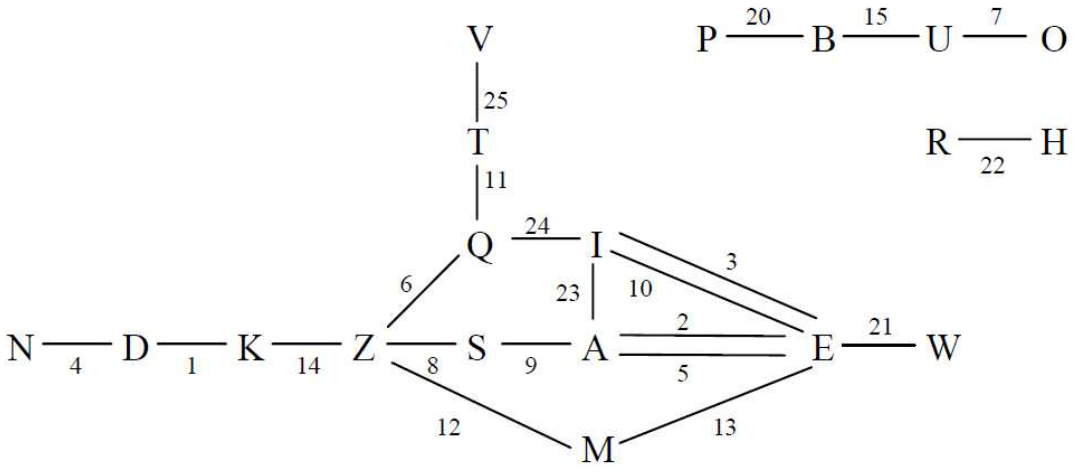
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
d	a	e	d	a	q	o	z	s	i	q	m	m
k	e	i	n	e	z	u	s	a	e	t	z	e
14	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	
z	b	i	l	g	m	p	w	h	a	l	v	
z	u	m	v	o	r	b	e	r	i	q	t	

Tabuľka 4.1: Časť odpočutej správy obsahujúcej crib.
Zdroj (Turing, 1940)

torov a cribu budem nazývať Enigmou v *prvej pozícii*. Rovnako druhé písmeno cribu `e` sa s pravým rotorom o dva pootočeným od nultej pozície rotorov zašifrovalo na `a` a Enigmu s týmto pootočením budem nazývať Enigmou v *druhej pozícii*. Pravý rotor Enigmy v i-tej pozícii je teda vždy pootočený o jedna od pravého rotora Enigmy v pozícii $i - 1$.

Pripomeňme, že Enigma je recipročná a teda ak `k` sa šifruje v prvej pozícii na `d`, tak zároveň `d` sa v prvej pozícii šifruje na `k`.

Všimnime si, že Enigma v druhej pozícii šifruje písmeno `a` na písmeno `e`, zároveň písmeno `e` Enigma v tretej pozícii šifruje na `i`, a zároveň `i` na 23-tej pozícii znovu na `a`. Takúto postupnosť písmen `a`, `e`, `i` budeme nazývať *cyklus*. Rovnako by sme mohli nájsť aj iné cykly v správe. Graf cribu vytvorený z príkladu so znázornenými cyklami môžeme vidieť na obrázku 4.1, kde očíslované hrany medzi písmenami určujú v ktorej pozícii Enigma šifruje dve písmená spojené hranou vzájomne na seba (Turing, 1940, str. 99). Podotknime, že graf je neorientovaný kvôli reciprocite Enigmy.



Obr. 4.1: Graf cribu.
Zdroj (Turing, 1940)

V grafe cribu vidíme, že písmeno `a` sa nachádza vo viacerých cykloch. Takéto písmeno budeme nazývať *centrálny bod*.

Zamerajme sa na cyklus s písmenami `a, e, i`, ktoré sú prepojené Enigmami v pozíciách 2, 3 a 23. Následujúci príklad som si vymyslela tak, aby som na ňom ukázala základný princíp Turingovej bomby popísaný v (Turing, 1940, str. 97-101). K príkladu budeme potrebovať permutácie E_2, E_3, E_{23} v tabuľkách 4.2,

4.3 a 4.4, ktoré som si sama vygenerovala. Permutácia E_l predstavuje šifrovanie Enigmou v l-tej pozícii s identickou prepojovacou doskou.

a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
h	z	r	t	q	s	j	a	v	g	w	y	n
n	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
m	x	u	e	c	f	d	p	i	k	o	l	b

Tabuľka 4.2: Permutácia E_2

a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
y	c	b	l	t	v	w	z	q	m	o	d	j
n	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
u	k	s	i	x	p	e	n	f	g	r	a	h

Tabuľka 4.3: Permutácia E_3

a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
z	e	l	m	b	p	v	t	o	q	n	c	d
n	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
k	i	f	j	u	x	h	r	g	y	s	w	a

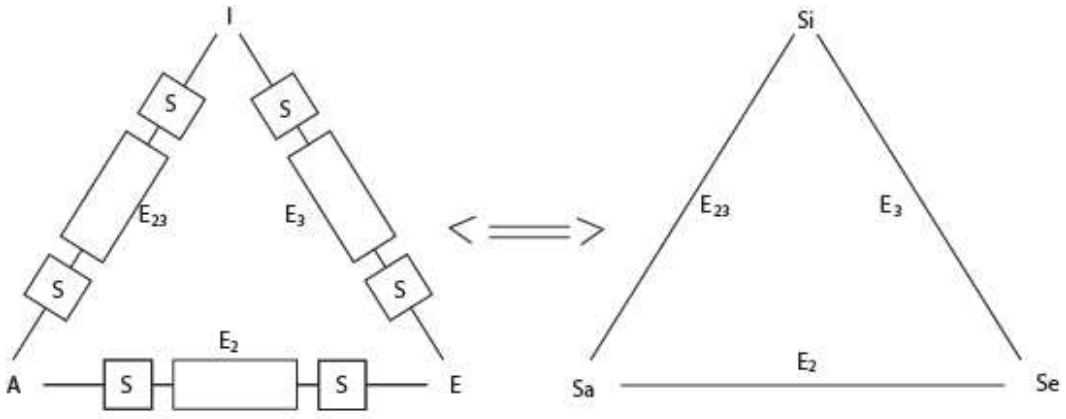
Tabuľka 4.4: Permutácia E_{23}

Predstavme si, že vlastníme tri Enigmy, ktoré drôtmi prepojíme do trojcyklu tak, že výstup z jednej Enigmy bude vstupom do druhej Enigmy. Môj príklad budeme robiť ale mechanicky, preto netreba aby Enigmy boli prepojené. Ako som na začiatku sekcie predpokladala, poznáme správnu začiatočnú pozíciu rotorov, ktorá šifrovala crib, a teda rotory v každej Enigme v trojcykle natočíme na túto pozíciu. S terminológiou ktorú som nedávno zaviedla je v tomto momente každá Enigma v nultej pozícii. Ďalej pootočíme pravé rotory každej Enigmy následovne: prvá Enigma šifrujúca písmeno `a` bude v druhej pozícii, druhá Enigma šifrujúca písmeno `e` bude v tretej pozícii a tretia Enigma šifrujúca `i` v 23-tej pozícii. Ďalej z každej Enigmy odstránime *stepping mechanizmus*, takže pri stlačení akejkoľvek klávesy sa rotory Enigiem nebudú pohybovať. Prepojovaciu dosku v každej Enigme necháme bez prepojení. Naším cieľom je zistiť prepojenie aspoň jedného písmena v cykle, a to písmena `a` keďže je centrálnym bodom. Vyskúšame všetkých 26 možností. Jednou možnosťou je, že písmeno je prepojené samo so sebou. Našu hypotézu overíme alebo vyvrátime následujúcim algoritmom (detailnejšie viď postup na grafe cyklu na obrázku 4.2):

- Písmeno `a` v prepojovacej doske prepojíme s písmenom podľa hypotézy v každej Enigme v cykle. Keďže naša hypotéza bola, že `a` nie je s ničím prepojené, tak tento krok vynecháme.
- V prvej Enigme stlačíme klávesu `a`. Písmeno `a` prejde prepojovacou doskou kde sa nezmení a následne prejde permutáciou E_2, ktorá zmení písmeno `a` $= S$`a` na písmeno `h` podľa tabuľky 4.2. Vieme ale, že vstup druhej Enigmy (čo je písmeno `e`) je zároveň výstupom z prvej Enigmy. Z permutácie E_2

nám ale vyšiel výstup `h` a preto vieme odvodiť, že prepojovacia doska musí meniť písmeno `h` na písmeno `e` aby písmená v cykle sedeli.

- V prepojovacej doske každej Enigmy prepojíme písmená `e` a `h`.
- V druhej Enigme stlačíme klávesu `e`. Písmeno `e` sa prechodom cez dosku zmení na $\mathtt{h} = S\mathtt{e}$ a prechodom cez E_3 na `z` podľa tabuľky 4.3. Opäť dedukujeme, že písmeno `z` je v doske prepojené s písmenom `i` ako v druhom bode.
- V prepojovacej doske každej Enigmy prepojíme písmená `i` a z.
- V poslednej tretej Enigme v cykle stlačíme klávesu písmena `i`, ktoré sa v prepojovacej doske zmení na `z` a to prechodom cez E_{23} na `a` podľa tabuľky 4.4. Keďže $\mathtt{a} = S\mathtt{a}$, tak sme overili, že $S\mathtt{a} = \mathtt{a}$ je naozaj kandidát.
- Volíme novú hypotézu, napr. $S\mathtt{a} = \mathtt{b}$, a opakujeme postup.



Obr. 4.2: Detailné zobrazenie cyklu `{a, e, i}` so šifrovacími komponentami

Ak by v predposledom bode vyšlo, že $E_{23}S\mathtt{i} = E_{23}\mathtt{z} \neq S\mathtt{a} = \mathtt{a}$, potom by naša hypotéza bola nesprávna keďže vedie k sporu, že jedno písmeno je v doske prepojené s dvomi písmenami. Po vyskúšaní všetkých 26 možností množina všetkých písmen ktoré prešli algoritmom môže byť veľká, preto rovnaký postup aplikujeme na iné cykly v grafe obsahujúce rovnaký centrálny bod, v našom prípade písmeno `a`. Množina kandidátov, ktoré prejdú algoritmom pre všetky cykly v grafe by sa mala znižovať, najlepšie na jedno písmeno. Behom tohoto algoritmu dostávame prepojenia všetkých písmen v cykle. Prečo tento algoritmus funguje podrobnejšie popíšem v sekcii 4.3.

Poznámka. Dva diagramy na obrázku 4.2 sú si ekvivalentné. Z pravého diagramu si všimnime, že v cykloch sa nepracuje s písmenami zo správy, teda `a, e, i`, ale len s ich prepojenými dvojicami v prepojovacej doske, teda $S\mathtt{a}$, $S\mathtt{e}$, $S\mathtt{i}$.

Ak už poznáme správne prepojenie viacerých písmen z cyklov včetne centrálneho bodu, možeme algoritmus aplikovať aj na necykly a tým získať prepojenie všetkých písmen, a teda celé *plugboard-setting*.

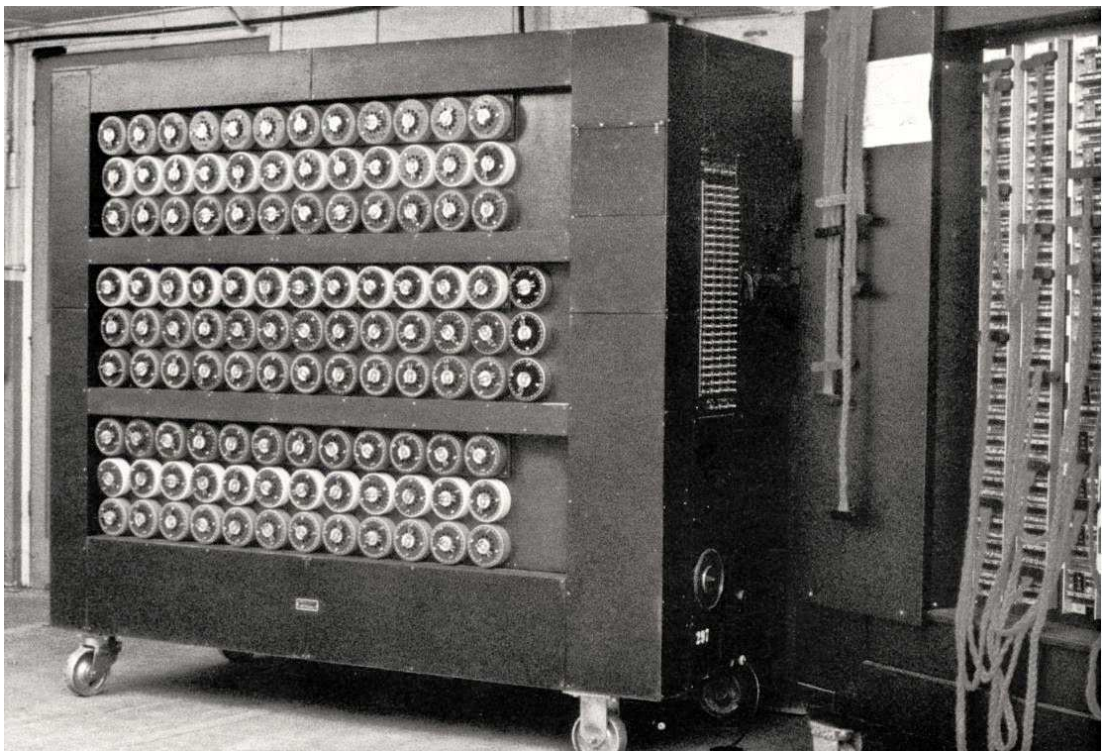
Na tomto princípe bola založená Turingova bomba. Vytváraním grafov a cyklov ako vyššie sa definovali podmienky, ktoré by správne denné nastavenie Enigmy malo splňovať, a podľa ktorých bomba zastavovala alebo nie.

4.2 Turingova bomba

V príklade som ukázala základnú myšlienku Turingovej bomby. Reálne sme ale v situácii kedy máme len odpočutú správu o ktorej nevieme nič viac ako dátum a čas jej odoslania. Nepoznáme ani jednu časť z denného nastavenia, ani crib.

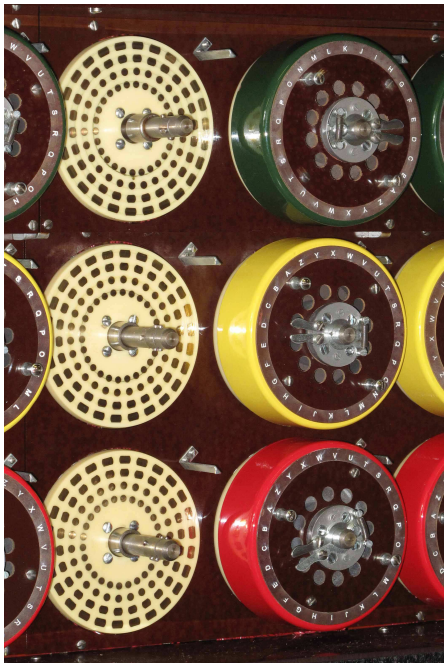
Turingova bomba (obr. 4.3) bola zložitý stroj preto sa jej architektúre budem venovať len prehľadovo. Bomba obsahovala 36 trojíc valcov, pričom každá trojica simulovala jednu trojicu rotorov v jednej Enigme. Valce boli farebne odlíšené podľa typu rotora, ktorý napodobňovali.

Aj keď trojice valcov napodobňovali trojice rotorov v Enigmách, ich konštrukcia bola rozdielna. Zatiaľ čo rotor v Enigme mal jednu sadu 26-tich kolíkov a jednu sadu 26-tich elektrických plochých kontaktov, valec v bombe ich obsahoval po dve sady, jednu pre priechod prúdu smerom ku reflektoru, a druhú pre priechod prúdu smerom od reflektora, viď obrázok 4.5. A teda aj reflektor v bombe bol obojstranný narozdiel od reflektora v Enigme, ktorý mal kolíky len na jednej strane. Tým boli vytvorené oddelené prepojenia pre vstup a výstup, vďaka čomu mohli byť trojice valcov v zadnej časti bomby prepojené do sérií podľa grafu cribu. To zabezpečilo, že vpustením prúdu výstup z jednej trojice bol vstupom do druhej trojice, ktorá bola s prvou prepojená v zadnej doske. Vo vnútri valca bolo prepojenie kolíkov a elektrických kontaktov rovnaké ako v rotore, ktorý valec napodobňoval (Sale, Letter pairs).

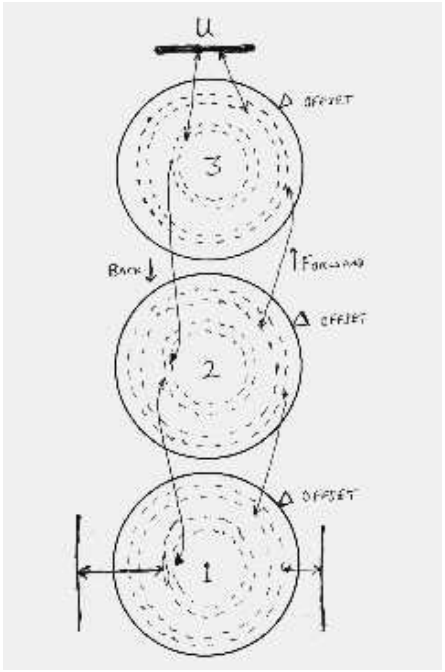


Obr. 4.3: Turingova bomba. Po vojne boli všetky materiály ohľadom prelomovania Enigmy včetne samotných bomb zničené. Bomba na fotografii bola skutočná bomba nachádzajúca sa v Bletchley Park. Zdroj (Copeland, 2004)

Posledná trojica valcov v strednom rade napravo slúžila na vyčítanie *ring-setting* keď bomba zastavila. Táto trojica bola špeciálne upravená a pootočená



Obr. 4.4: Detailný záber trojíc valcov na Turingovej bombe. Zdroj (Coles, 2011)



Obr. 4.5: Nákres priechodu prúdu valcami. Zdroj (Sale, Alan Turing, the Enigma and the Bombe)

tak, aby ukazovala rovno *ring-setting*, čím sa nemusel počítať ručne (Carter, The three indicator drums).

Angličania vedeli kedy nemci posielali správy s istým obsahom, napr. správy o počasí, a poznali stereotyp operátorov, ktorý na tieto špecialne správy používali rovnaké nemecké frázy. Aj s týmito informáciami bolo ale určenie či správa obsahovala crib náročné a vyžadovalo veľa pokusov a omylov (Copeland, 2004, str. 248).

Hneď ako sa našla správa, ktorá s veľkou pravdepodobnosťou obsahovala crib, zvolilo sa poradie rotorov a nasadilo sa toľko valcov, koľko bolo potrebné na vyrobenie reprezentácie grafu cribu. Každý valec sa natočil tak, aby boli všetky v rovnakej pozícii, teda aby pri ukazatele každého valca bolo rovnaké písmeno, napr. písmeno `z`. V každej trojici sa valec predstavujúci pravý rotor otočil tak, aby natočenie jednotlivých trojíc predstavovalo Enigmy v istých pozíciách určených grafom. Nakoniec sa trojice poprepájali v zadnej časti bomby tak, aby vytvárali graf ako na obrázku 4.1.

Ďalej sa nastavila hypotéza na prepojenie centrálneho bodu v prepojovacej doske a bomba sa zapla. Rovnakým spôsobom ako pri Rejewského bombe, sa skúšalo všetkých 26^3 možností na nultú pozíciu, teda tak, že sa synchronne otáčali všetky trojice. Bomba teda pre každú zvolenú hypotézu prešla všetkými možnými pozíciami rotorov a zastavila v tom prípade, ak konkrétna testovaná pozícia rotorov spĺňala hypotézu a podmienky určené grafom. V tom prípade si kryptológ odpísal pozíciu rotorov a všetky bombou vypočítané prepojenia v prepojovacej doske, a so skutočnou Enigmou nastavenou vypočítaným kľúčom skúsil dešifrovať časť správy. Ak dostal crib, tak mal správny denný kľúč. Ak mu vyšiel nezmyselný text, potom bomba zastavila pri falošnom kandidátovi na pozíciu rotorov, alebo

ak už bomba prešla všetkých 26^3 pozícií, tak sa volila nová hypotéza na prepojenie písmena `a`.

Bomba obsahovala až 36 trojíc valcov, čo znamená, že sa mohol použiť crib až 36 písmen dlhý. Vieme ale, že pri takom dlhom cribe by sa určite pootočil stredný rotor, a preto sa volili kratšie criby u ktorých šanca otočenia bola menšia.

Vďaka 36-tim trojiciam valcov bolo možné skúmať napríklad jeden crib dlhý 12 písmen zároveň pre tri rôzne poradia rotorov, alebo tri rôzne criby dlhé maximálne 12 písmen.

4.3 Matematické odôvodnenie

Niektoré pojmy, ktoré som v predošlých sekciách používala teraz formálnejšie zadefinujem.

Definícia 6. *Nech S je permutácia prepojovacej dosky nastavenej podľa denného kľúča. Enigmu v nultej pozícii rotorov s pootočenými rotormi o z, y, x od počiatočnej pozície definujeme ako zloženie*

$$S^{-1}E_{z,y,x}S$$

kde $E_{z,y,x} = P^{-x}R^{-1}P^xP^{-y}M^{-1}P^yP^{-z}L^{-1}P^zQP^{-z}LP^zP^{-y}MP^yP^{-x}RP^x$. *Ďalej budeme značiť* $E_0 := E_{z,y,x}$. *Enigmu v l-tej pozícii vzhľadom k nultej pozícii E_0 definujeme ako*

$$S^{-1}E_lS$$

kde

$$E_l = P^{-(x+l)}R^{-1}P^{(x+l)}P^{-y}M^{-1}P^yP^{-z}L^{-1}P^zQP^{-z}LP^zP^{-y}MP^yP^{-(x+l)}RP^{(x+l)}$$

Definícia 7. *Cyklom definujeme množinu písmen $\{a_1,...,a_n\}$, pre ktoré existujú $\{i_1,...,i_n\}$, kde $i_j \in \mathbb{N}$ také, že*

$$\begin{aligned} E_{i_1}Sa_1 &= Sa_2 \\ E_{i_2}Sa_2 &= Sa_3 \\ &... \\ E_{i_n}Sa_n &= Sa_1 \end{aligned} \tag{4.1}$$

Predpokladajme, že sme odpočuli správu, ktorej časť je zašifrovaný crib ako v tabuľke 4.1. Naším cieľom bude zistiť poradie rotorov, *ring-setting* a *plugboard-setting*, ktorými bola správa šifrovaná.

Zamerajme sa na cykly z grafu 4.1: `{a, e, i}`, `{a, i, q, z, s}` a `{a, e, m, z, s}`. Vidíme, že písmeno `a` sa nachádza v každom cykle, a teda je centrálnym bodom, ku ktorému chceme nájsť písmeno s ktorým je v prepojovacej doske prepojené. Vytvoríme hypotézu, že $S\mathtt{a} = \mathtt{a}$. Chceme túto hypotézu potvrdiť alebo vyvrátiť a zároveň chceme k nej zistiť aká bola pozícia rotorov pred šifrovaním cribu, a teda aká bola nultá pozícia Enigmy.

Vieme, že pre permutácie E_2, E_3, E_{23}, E_9, ..., ktoré sú vzhľadom k neznámej nultej pozícii, platí

$$\begin{aligned} E_2S\mathtt{a} &= S\mathtt{e} \\ E_3S\mathtt{e} &= S\mathtt{i} \\ E_{23}S\mathtt{i} &= S\mathtt{a} \end{aligned} \tag{4.2}$$

alebo inak napísané

$$E_{23}E_3E_2S\mathtt{a} = S\mathtt{a} \tag{4.3}$$

Rovnako z ďalších dvoch cyklov dostávame

$$E_9E_8E_6E_{24}E_{23}S\mathtt{a} = S\mathtt{a} \tag{4.4}$$

a

$$E_9E_8E_{12}E_{13}E_5S\mathtt{a} = S\mathtt{a} \tag{4.5}$$

Z predošlých rovností sme zistili, že $S\mathtt{a}$ je fixný bod permutácií $E_{23}E_3E_2$, $E_9E_8E_6E_{24}E_{23}$ a $E_9E_8E_{12}E_{13}E_5$.

Bomba bude k zvolenej hypotéze prepojenia centrálneho bodu v prepojovacej doske hľadať nultú pozíciu rotorov (z, y, x) takú, že platia rovnosti 4.3, 4.4 a 4.5, teda bude testovať či písmeno $S\mathtt{a}$ je fixným bodom všetkých troch zložených permutácií. Keďže trojice valcov v bombe simulujú Enigmy a sú relatívne pootočené tak, aby predstavovali šifrovanie písmen z grafu cribu v konkrétnych pozíciách, tak bomba pozná aj všetky permutácie E_l, a teda je schopná zároveň nájsť aj prepojenia ostatných písmen v cykloch v prepojovacej doske, a to následovným spôsobom.

Bomba si bude vytvárať retiazky písmen cyklov, z ktorých odvodí ich prepojenia v prepojovacej doske a zároveň vyhodnotí správnosť voľby testovanej pozície rotorov, algoritmom ktorý som už popísala na konci sekcie 4.1.

Z prvého cyklu `{a, e, i}` vytvorí retiazok:

$$\begin{aligned}
&\mathtt{a} \xrightarrow{S} \mathtt{a} \xrightarrow{E_2} \mathtt{h} \xrightarrow{S} \mathtt{e} \implies S\mathtt{e} = \mathtt{h} \\
&\mathtt{e} \xrightarrow{S} \mathtt{h} \xrightarrow{E_3} \mathtt{z} \xrightarrow{S} \mathtt{i} \implies S\mathtt{i} = \mathtt{z} \\
&\mathtt{i} \xrightarrow{S} \mathtt{z} \xrightarrow{E_{23}} \mathtt{a} \xrightarrow{S} \mathtt{a}
\end{aligned} \tag{4.6}$$

Rovnako si vytvorí retiazky z ďalších dvoch cyklov a skontroluje či v každom poslednom riadku z retiazku je predposledné písmeno pred prechodom cez permutáciu S písmeno `a`. (Pre následujúci retiazok som si písmená, ktoré sú výstupom Enigiem v pozíciách 24, 6, ... pre príklad vymyslela.) Vidíme, že pre prvý cyklus `{a, e, i}` hypotéza platila, ale pre retiazok vytvorený z druhého cyklu `{a, i, q, z, s}`

$$\begin{aligned}
&\mathtt{a} \xrightarrow{S} \mathtt{a} \xrightarrow{E_{23}} \mathtt{z} \xrightarrow{S} \mathtt{i} \implies S\mathtt{i} = \mathtt{z} \\
&\mathtt{i} \xrightarrow{S} \mathtt{z} \xrightarrow{E_{24}} \mathtt{l} \xrightarrow{S} \mathtt{q} \implies S\mathtt{q} = \mathtt{l} \\
&\mathtt{q} \xrightarrow{S} \mathtt{l} \xrightarrow{E_6} \mathtt{b} \xrightarrow{S} \mathtt{z} \implies S\mathtt{z} = \mathtt{b} \\
&\mathtt{z} \xrightarrow{S} \mathtt{b} \xrightarrow{E_8} \mathtt{t} \xrightarrow{S} \mathtt{s} \implies S\mathtt{s} = \mathtt{t} \\
&\mathtt{s} \xrightarrow{S} \mathtt{t} \xrightarrow{E_9} \mathtt{d} \xrightarrow{S} \mathtt{a}
\end{aligned} \tag{4.7}$$

vychádza $S\mathtt{a} = \mathtt{d}$ čo je spor, keďže v prepojovacej doske nemôže byť jedno písmeno prepojené s dvomi písmenami zároveň. V tomto prípade bomba vyhodnotí testovanú pozíciu rotorov za nesprávnu a bez zastavenia skúša novú pozíciu.

4.4 Turing-Welchmanova bomba

V predošlých sekciách som uviedla, že pre každú z 26-tich hypotéz na prepojenie centrálneho bodu bomba vyskúša všetkých 26^3 možných pozícii rotorov, čo je spolu $26 \times 17\ 576 = 456\ 976$ možností pre jedeno poradie rotorov. Tento postup zabral veľa času, a preto cieľom angličanov bolo pre každú možnú pozíciu rotorov skúmať všetkých 26 hypotéz na prepojenie centrálneho bodu naraz.

Ďalej som uviedla algoritmus vytvárania retiazkov z cyklov, ktorý vyhodnocoval správnosť hypotézy prepojenia centrálneho bodu v istej pozícii rotorov a odvodzoval prepojenia ostatných písmen v cykle. Neuviedla som, že ale aj retiazok ktorý vyhodnotí hypotézu ako správnu môže obsahovať prepojenia písmen v cykle vedúce k sporu. Takýto retiazok bombu zastaví, ale bude sa jednať o falošného kandidáta, o ktorom nesprávnosť sa ukáže až pri ručnom overovaní. Táto chyba opäť viedla ku zbytočnému predlžovaniu času. Dokonca v mojom príklade v retiazku 4.7 sa táto chyba vyskytuje, k čomu sa vrátim neskôr.

V následujúcej sekcii zakončím kapitolu o Turingovej bombe ukázaním ako algoritmus hľadania denných kľúčov bol zrýchlený a upravený tak, aby zredukoval falošné zastavenia. Ďalej predstavým novú komponentu bomby vymyslenú Welchmanom zvanú *diagonálna doska*, bez ktorej by skonštruovanie bomby, ktorá by zároveň vedela odvodiť prepojenia písmen v prepojovacej doske z cyklu a zároveň zastavovala len pri nesporných kandidátoch, bolo náročné. Turingova bomba obsahujúca diagonálnu dosku sa dnes označuje ako *Turing-Welchmanova bomba*.

4.4.1 Súčasné skúmanie hypotéz

Predpokladajme, že skúmame správne poradie a správnu pozíciu rotorov. Zamerajme sa opäť na cyklus `{a, i, q, z, s}` a z neho vytvorený retiazok 4.7. Chceme aby bomba v tejto skúmanej pozícii rotorov súčasne vyskúšala všetkých 26 hypotéz na prepojenie centrálneho písmena `a`. Stále ale musíme my zvoliť prvotnú hypotézu, napr. $S\mathtt{a} = \mathtt{a}$. Vidíme, že retiazok 4.7 došiel k sporu. V poznámke za obrázkom 4.2 som poznamenala, že v cykloch vôbec nezáleží na písmenách zo správy, teda na `a, i, q, z, s`, ale len na ich pároch v prepojovacej doske, teda $S\mathtt{a}$, $S\mathtt{i}$, $S\mathtt{q}$, $S\mathtt{z}$ a $S\mathtt{s}$, keďže tieto v cykloch kolujú. Upravme teda retiazok podľa tejto poznámky na

$$S\mathtt{a} \xrightarrow{E_{23}} S\mathtt{i} \xrightarrow{E_{24}} S\mathtt{q} \xrightarrow{E_{6}} S\mathtt{z} \xrightarrow{E_{8}} S\mathtt{s} \xrightarrow{E_{9}} S\mathtt{a} \tag{4.8}$$

Na konci retiazku sme dostali, že $S\mathtt{a} = \mathtt{d}$, čo viedlo k sporu. Prepojme teraz ale výstup z retiazku 4.8 s jeho vstupom káblom. Teda písmeno `d`, ktoré z retiazku vyšlo zase pustíme do retiazku ako novú hodnotu $S\mathtt{a}$. Výstup z tohoto retiazku sa do neho pustí znovu a proces sa opakuje pokým nie sú všetky možné písmená vyčerpané, alebo pokým sa nenájde správna hodnota $S\mathtt{a}$. Ak sa správna hodnota nájde, tak retiazok už bude vždy končiť aj začínať touto hodnotou, a preto proces nebude ďalej generovať nové písmená. Tento proces ale nemusí nagenerovať všety písmená abecedy, preto bolo potrebné mať crib, ktorý viedol ku grafu s viacerými cyklami (Carter, Voltage feedback, Finding the correct hypothesis).

Pustením písmena `d` do cyklu dostaneme rovnaký výstup ako keby sme na písmeno $S\mathtt{a}$ aplikovali zloženú permutáciu $(E_9E_8E_6E_{24}E_{23})^2$, a teda proces v predošlom odstavci odpovedá mocneniu permutácie $(E_9E_8E_6E_{24}E_{23})$.

Aby sme vedeli všetky písmená, ktoré boli v tomto procese zahrnuté, pripojíme ku káblu spojujúcemu vstup a výstup retiazkov 26 žiaroviek, každej označenej písmenom abecedy. Zo 26-tich žiaroviek sa rozsvietia všetky tie, na ktoré sa zašifruje písmeno $S\mathtt{a}$ permutáciami $(E_{23}E_3E_2)$, $(E_{23}E_3E_2)^2$, $(E_{23}E_3E_2)^3$, ..., $(E_9E_8E_6E_{24}E_{23})$, $(E_9E_8E_6E_{24}E_{23})^2$, $(E_9E_8E_6E_{24}E_{23})^3$, ..., $(E_9E_8E_{12}E_{13}E_5)$, $(E_9E_8E_{12}E_{13}E_5)^2$, $(E_9E_8E_{12}E_{13}E_5)^3$, ... Ak teda zvolená hypotéza napr. $S\mathtt{a} = \mathtt{b}$ je správna (teda hypotéza je splnená vo všetkých retiazkoch), potom aplikovaním ktorejkoľvek mocniny všetkých troch zložených permutácií na $S\mathtt{a}$ sa vždy z retiazku vráti písmeno `b`, a teda bude svietiť len jedna žiarovka s písmenom `b`.

V našom prípade keďže hypotéza $S\mathtt{a} = \mathtt{a}$ je nesprávna, tak sa rozsvieti viac žiaroviek, keďže v procese mocnenia bolo zahrnutých viac písmen ako len `a`. Tie žiarovky, ktoré sa nerozsvietia budú predstavovať možných kandidátov na hodnotu $S\mathtt{a}$, ktoré sa ešte neoverili. Dokonca sa môžu rozsvietiť všetky žiarovky až na jednu, ktorej písmeno bude v tomto prípade jedinou nevylúčenou hypotézou na správnu hodnotu $S\mathtt{a}$, ktorú sa ešte oplatí overiť. Keby sa počas procesu mocnenia nagenerovala správna hodnota $S\mathtt{a}$, potom by sa iné písmená už nenagenerovali, a teda by svietila len jedna žiarovka. Keďže ale jedine jedna žiarovka nebola rozsvietená, znamená to, že v procese písmeno patriace žiarovke nagenerované nebolo, a teda je ešte možným kandidátom na správne prepojenie písmena `a`. Ak by sa rozsvietili všetky písmená, znamenalo by to, že pre dané poradie a pozíciu rotorov ani jedna hypotéza na hodnotu $S\mathtt{a}$ nesplňuje požiadavky, a teda že túto pozíciu rotorov môžeme úplne vylúčiť z kandidátov (Carter, Finding the correct hypothesis, Summary).

Týmto procesom bomba v každej skúmanej pozícii rotorov súčasne vyhodnotila všetkých 26 hypotéz na prepojenie centrálneho bodu v prepojovacej doske.

4.4.2 Falošné zastavenia a diagonálna doska

Predpokladajme opäť, že bomba skúma správne poradie a správnu pozíciu rotorov, a zamerajme sa opäť na cyklus `{a, i, q, z, s}`. Pozrime sa na retiazok 4.7 a predpokladajme, že v poslednom riadku Enigma v deviatej pozícii šifruje písmeno `t` na písmeno `a`, a teda bomba zastaví lebo hypotézu $S\mathtt{a} = \mathtt{a}$ vyhodnotila ako správnu. Retiazok teda vyzerá následovne

$$\begin{aligned}
\mathtt{a} \xrightarrow{S} \mathtt{a} \xrightarrow{E_{23}} \mathtt{z} \xrightarrow{S} \mathtt{i} &\implies S\mathtt{i} = \mathtt{z} \\
\mathtt{i} \xrightarrow{S} \mathtt{z} \xrightarrow{E_{24}} \mathtt{l} \xrightarrow{S} \mathtt{q} &\implies S\mathtt{q} = \mathtt{l} \\
\mathtt{q} \xrightarrow{S} \mathtt{l} \xrightarrow{E_6} \mathtt{b} \xrightarrow{S} \mathtt{z} &\implies S\mathtt{z} = \mathtt{b} \\
\mathtt{z} \xrightarrow{S} \mathtt{b} \xrightarrow{E_8} \mathtt{t} \xrightarrow{S} \mathtt{s} &\implies S\mathtt{s} = \mathtt{t} \\
\mathtt{s} \xrightarrow{S} \mathtt{t} \xrightarrow{E_9} \mathtt{a} \xrightarrow{S} \mathtt{a}
\end{aligned} \tag{4.9}$$

Pozrime sa ale na prvý a tretí riadok retiazku. Bomba vydedukovala, že $S\mathtt{i} = \mathtt{z}$ a zároveň $S\mathtt{z} = \mathtt{b}$, čo je samozrejme spor keďže nemôže platiť, že $S\mathtt{z} = \mathtt{b}$ a zároveň $S\mathtt{z} = \mathtt{i}$. Bomba sa ale pozerala len na to či na začiatku a na konci retiazku vychádza rovnaké písmeno, preto vyhodnotila hypotézu ako možného kandidáta, keďže spĺňa požiadavky, a zastala. Jedná sa ale o falošné zastavenie.

Tieto falošné zastavenia, kedy sa hypotéza javila ako správna, ale prepojenia písmen v cykloch boli sporné, vyriešila implementácia tzv. *diagonálnej dosky*, ktorej myšlienka bola založená na reciprocite Enigmy.

Diagonálna doska bola veľká štvorcová doska obsahujúca 26×26 zásuviek usporiadaných do 26 riadkov a 26 stĺpcov. Riadky a stĺpce boli v abecednom poradí označené písmenami. Prvý riadok odpovedal všetkým možným 26-tim prepojeniam písmena `a` v prepojovacej doske, druhý riadok odpovedal všetkým možným prepojeniam písmena `b`, atď. Riadky boli prepojené následovne: Prvá zásuvka v riadku `b` bola prepojená s druhou zásuvkou v riadku `a`, čím bola zároveň prepojená druhá zásuvka v riadku `a` s prvou zásuvkou v riadku `b`. To odpovedalo prepojeniu v prepojovacej doske dvojice `ab` a teda zároveň `ba`. Tretia zásuvka v riadku `b` bola prepojená s druhou zásuvkou v riadku `c`, atď. pre všetky možné dvojice. Všetky zásuvky na doske boli v podstate prepojené symetricky podľa diagonály, z čoho vznikol názov diagonálnej dosky (Carter, Diagonal Board).

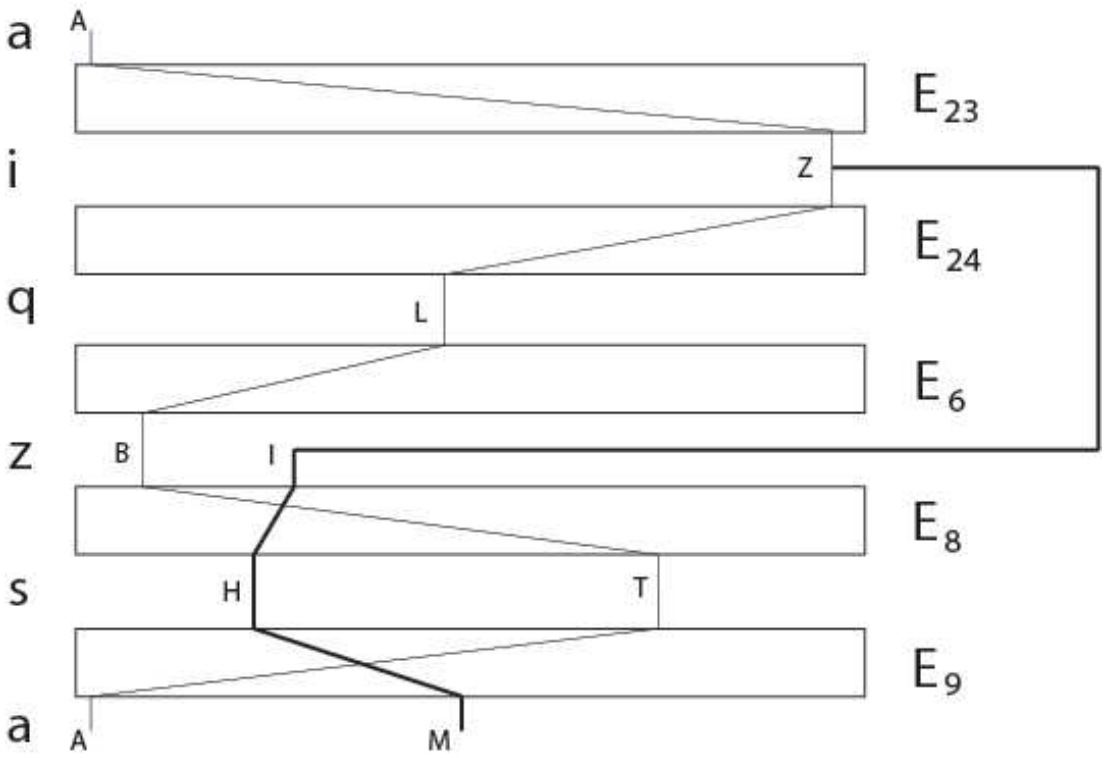
Enigmy v bombe sú na diagonálnu dosku napojené podľa grafu tak, že Enigma v pozícii 23 je prepojená s riadkom `i` na diagonálnej doske a zároveň napojená na ďalšiu Enigmu v sérii v pozícii 24. Pri prejdení prúdu touto Enigmou v pozícii 23 prúd smeruje do zásuvky $S\texttt{i}$ v riadku `i`, odkiaľ je poslaný do zásuvky `i` v riadku $S\texttt{i}$. Ak je riadok $S\texttt{i}$ prepojený s ďalšou Enigmou v nejakej pozícii v sérii, tak prúd pokračuje do tejto Enigmy. V opačnom prípade ak riadok už nie je prepojený s ďalšou Enigmou, tak sa prúd v tejto vetve zastaví, ale prúd prechádzajúci sériou Enigiem zostáva. Rovnako sú prepojené ďalšie Enigmy v sérii s diagonálnou doskou (Sale, The diagonal board).

Prečo diagonálna doska fungovala ukážem na mojom príklade. Z retiazku a grafu vieme, že

$$\begin{aligned} E_{23}S\texttt{a} = S\texttt{i} = z \\ E_{24}S\texttt{i} = S\texttt{q} = l \\ E_{6}S\texttt{q} = S\texttt{z} = b \\ E_{8}S\texttt{z} = S\texttt{s} = t \\ E_{9}S\texttt{s} = S\texttt{a} = a \end{aligned} \tag{4.10}$$

Pozrime sa na obrázok 4.6, ktorý predstavuje priechod prúdu v bombe skúmaným cyklom so spornou hypotézou, ktorá sa javí ako správna. Písmená napísané veľkým písmom predstavujú $S\texttt{a}$, $S\texttt{i}$, $S\texttt{q}$, $S\texttt{z}$ a $S\texttt{s}$ k písmenám z cyklu napísanými malým písmom. Tenká čiara predstavuje šifrovanie sériou Enigiem v pozíciách 23, 24, 6, 8 a 9, teda 4.10. Hrubá čiara predstavuje spojenie dvoch písmen v diagonálnej doske a následný priechod prúdu od tejto vetvy.

V bombe s implementovanou diagonálnou doskou dostávame po poslednom šifrovaní Enigmou v pozícii 9 dva výstupy, jeden $S\texttt{a} = \texttt{s}$ a druhý $S\texttt{a} = \texttt{m}$. Dva výstupy, ktoré spôsobia spor a nezastavenie bomby pri tejto hypotéze, dostávame vďaka diagonálnej doske, keďže po šifrovaní Enigmou v pozícii 23 prúd smeruje do ďalšej Enigmy v pozícii 24 a zároveň do riadku `i` na diagonálnej doske do zásuvky $S\texttt{i}$, teda `z`. Táto zásuvka je zo symetrie spojená na diagonálnej doske so zásuvkou `i` v riadku $S\texttt{i}$, teda `z`. Keďže ale na tento riadok je napojená Enigma v pozícii 6, tak prúd začne rozdvojene prechádzať cyklom a preto dostávame dva výstupy, teda dve hodnoty prepojenia písmena `a`, čo je spor. Vďaka diagonálnej doske si bomba akokeby po každom vydedukovaní dvojice v prepojovacej doske tieto písmena sama prepojí, aby sa brali v úvahe aj pri ďalších krokoch dedukovania, a preto bomba nezastaví nikdy pri hypotéze, ktorá by viedla k prípadu kedy by jedno písmeno bolo v prepojovacej doske prepojené s dvomi písmenami.



Obr. 4.6: Príklad sporného vydedukovania *plugboard-setting* bombou, ktoré je odchytené diagonálnou doskou

Spomeňme si na algoritmus dedukovania prepojení písmen v prepojovacej doske, ktorý som po bodoch napísala na konci sekcie 4.1. V tomto algoritme som po zistení nejakej prepojenej dvojice túto dvojicu hneď prepojila v prepojovacej doske, a tým skúmanie ďalších písmen v cykle už počítalo s touto dvojicou. Toto bol presne zmysel diagonálnej dosky.

Záver

V tejto práci sme matematicky popísali metódy, ktoré boli použité na prelomenie nemeckého šifrovacého stroja Enigmy, a dokázali ich správnosť. Najprv sme vytvorili matematický model Enigmy (problému), do ktorého sme preložili informácie o metódach z originálnych zdrojov, a z toho sme zrekonštruovali postupy, ktoré v zdrojoch neboli uvedené, resp. neboli dostatočne matematicky popísané.

Zistili sme, že každá metóda fungovala na princípe prehľadávania hrubou silou a vyžadovala definovanie istých podmienok, založených na množine skúmaných správ, podľa ktorých metódy vedeli rozlíšiť, ktoré nastavenie mohlo byť kandidátom na správny denný kľúč, a ktoré nemohlo.

Zistené princípy a postupy metód sme ilustrovali na zjednodušených príkladoch, ktorých vstupy (teda odpočuté indikátory alebo časti správ) sme buď prebrali z originálnych zdrojov, alebo vymysleli tak, aby ukazovali schopnoti metód, resp. ich nedostatky. Zjednodušenie príkladov spočívalo v tom, že sme predpokladi odpočutie správ, ktoré splňovali naše predpoklady pre úspešnosť metód, ako napríklad predpoklad o neotočení ľavých a stredných rotorov počas šifrovania indikátorov alebo častí správ, resp. predpoklad o nezmenení konkrétnych písmen prepojovacou doskou.

Štúdium Enigmy a jej prelomenia je rozsiahle a zaujímavé. Vo svojej práci sme sa venovali len odhaľovaniu denných nastavení stroja s predpokladom, že Enigmu vlastníme, a poznáme konštrukciu a prepojenie všetkých jej komponent. Konštrukcia a prepojenie jednotlivých komponent bola na začiatku pre poliakov taktiež neznáma, ale dokázali ich vypočítať pomocou teórie permutácií. Postupu výpočtu prepojení som sa vo svojej práci nevenovala, keďže presahuje zadanie práce, ale dočítate sa o ňom v originálnych Rejewského článkoch, napr. v (Rejewski, 1980). Práve o týchto postupoch bolo dostatok originálnych zdrojov, zatiaľ čo o postupoch pri odhaľovaní denných kľúčov ich bolo málo, resp. im chýbal matematický základ.

Celkovo práca, ktorú museli poliaci a angličania denne vykonávať, aby našli správne denné nastavenie, bola nepredstaviteľná. Vo svojej práci som vždy predpokladala, že máme niekoľko odpočutých správ, ktoré nám správne denné nastavenia naozaj odkryjú, ale oni museli denne prejsť veľkým množstom správ, a ešte väčším množstvom pokusov a omylov, aby sa vôbec k odhaleniu denných kľúčov priblížili.

Zoznam použitej literatúry

Carter, F. The turing bombe. URL http://www.rutherfordjournal.org/article030108.html. Bletchley Park reports.

Coles, T. (2011). Bombe drums and mounting plate. URL https://en.wikipedia.org/wiki/File:Bombe_Drums_and_Mounting_Plate.jpg.

Copeland, J. (2004). *The essential Turing: seminal writings in computing, logic, philosophy, artificial intelligence, and artificial life, plus the secrets of Enigma*. New York: Oxford University Press. ISBN 0-19-825079-7. URL http://www.cse.chalmers.se/~aikmitr/papers/Turing.pdf.

Rejewski, M. (1980). An application of the theory of permutations in breaking the enigma cipher. *Applicationes Mathematicae*, **16**(4).

Rejewski, M. (1981). How polish mathematicians broke the enigma cipher. *IEEE Annals of the History of Computing*, **3**, 213–234. ISSN 1058-6180.

Reuvers, P. a Simons, M. Enigma i. URL http://www.cryptomuseum.com/crypto/enigma/i/index.htm.

Reuvers, P. a Simons, M. History of the enigma. URL http://www.cryptomuseum.com/crypto/enigma/hist.htm.

Rijmenants, D. Technical details of the enigma machine. URL http://users.telenet.be/d.rijmenants/en/enigmatech.htm.

Sale, A. E. Codes and ciphers in the second world war: The history, science and engineering of cryptanalysis in world war ii. URL www.codesandciphers.org.uk/.

Tůma, J. (2003). Permutation groups and the solution of german enigma cipher. pages 33–43. URL http://www.karlin.mff.cuni.cz/~tuma/nciphers/oulu.pdf.

Turing, A. (1940). *Turing's Treatise on the Enigma: (the Prof's Book)*.

Woland, M. (2007). Enigma wiring kleur. URL https://commons.wikimedia.org/wiki/File:Enigma_wiring_kleur.svg.