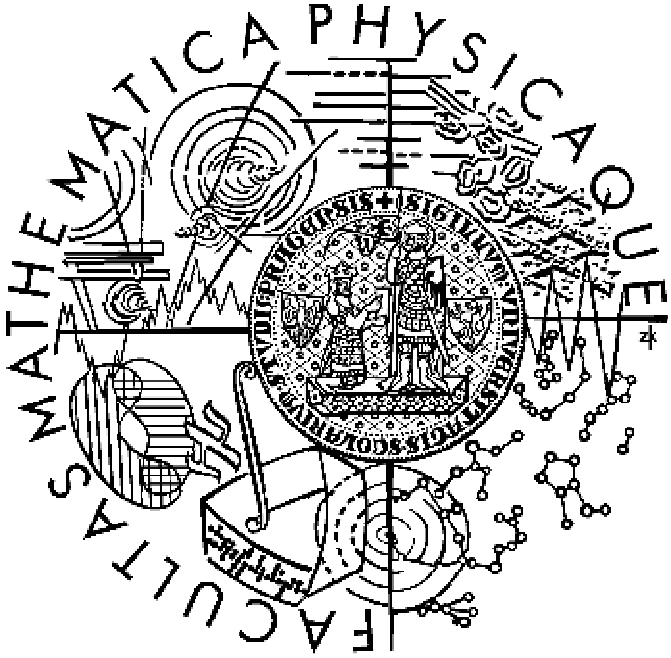
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

# BAKALÁŘSKÁ PRÁCE




Barbora Galaczová

# REJEWSKÉHO A TURINGOVA BOMBA

Katedra algebry

Vedoucí bakalářské práce: Doc. RNDr. Jiří Tůma, DrSc.

Studijní program: Matematika, Obecná matematika

2007

Na tomto místě bych chtěla poděkovat především svému vedoucímu bakalářské práce Doc. RNDr. Jiřímu Tůmovi, DrSc.za cenné připomínky a rady a také kolegovi Mgr. Jiřímu Vábkovi za jeho inspirativní poznámky aktivní pomoc při vypracování bakalářské práce. Také bych ráda poděkovala své rodině a přátelům, že mě po celou dobu studia podporovali.

Prohlašuji, že jsem svou bakalářskou práci napsala samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne 30. května 2007 Barbora Galaczová

# Obsah

**Název práce:** *Rejewského a Turingova bomba*
**Autor:** *Barbora Galaczová*
**Katedra:** *Katedra algebry*
**Vedoucí bakalářské práce:** *Doc. RNDr. Jiří Tůma, DrSc.*
**e-mail vedoucího:** *tuma@karlin.mff.cuni.cz*

**Abstrakt:** *V této práci se snažíme podat ucelený přehled metod zjišťování denního klíče u německé vojenské šifry Enigma. Zaměřujeme se především na práci polských kryptoanalytiků Mariana Rejewského a jeho kolegů z Biura Szyfrow. Němci začali používat šifrovací přístroj Enigma ještě před vypuknutím druhé světové války. V letech 1932-1939 polští kryptoanalytici zjistili vnitřní propojení přístroje (v prosinci 1932) a vynalezli velké množství metod zjišťování denního klíče. Během války Němci několikrát změnili způsob šifrování zpráv, což vedlo ke vzniku Rejewského bomby a později také Turingovy bomby, jež zjednodušily způsob zjišťování denního klíče. Pomocí těchto zařízení byly až do konce druhé světové války luštěny zachycené německé depeše.*

**Klíčová slova:** *Enigma, Rejewski, permutace.*

**Title:** *Rejewski`s and Turing`s bomb*
**Author:** *Barbora Galaczová*
**Department:** *Department of Algebra*
**Supervisor:** *Doc. RNDr. Jiří Tůma, DrSc.*
**Supervisor`s e-mail address:** *tuma@karlin.mff.cuni.cz*

**Abstract:** *In the present work we describe the methods of reconstruction of daily keys used with the German military cipher Enigma. We concentrate especially on Marian Rejewski`s work in the Polish Biuro Szyfrow. The German army used the cipher machine Enigma already before the start of the Second World War. During the years 1932-1939 the Polish cryptologists reconstructed the internal structure of Enigma (in December 1932) and then invented a lot of methods how to reconstruct the daily keys. The German army modified the operating rules of the Enigma machine a few times prior and during the Second World War. These changes led to the invention of Rejewski`s bomb and later of Turing`s bomb that simplified the reconstruction of daily keys. Because of these machines the Allies could read most of the messages encrypted by Enigma throughout the WWII.*

**Keywords:** *Enigma, Rejewski, permutation.*

# 1. Úvod

Kryptologie již odpradávna ovlivňovala historii národů, pomáhala na bitevním poli, skrývala tajné milence a milenky, zabezpečovala různá obchodní tajemství a také chránila soukromí obyčejných lidí. Neustálý boj mezi kryptografy na jedné straně a kryptoanalytiky na druhé je nedílnou součástí historie lidstva. Zdá se, že tato bitva nemá vítěze. Chvíli vítězí kryptografové se svými rádoby neprolomitelnými šiframi a chvíli zase kryptoanalytici se svými novými myšlenkami a postupy jak šifry rozbít. Kdo nakonec zvítězí? Tato otázka zůstává stále nezodpovězena a nalézt správnou odpověď je velice nesnadný úkol.

Zaměříme se pouze na určitý krátký historický úsek. Především na vzestup a pád známého šifrovacího stroje Enigma, jež je důkazem toho jak kryptografové a kryptoanalytici ovlivňují chod dějin.

Enigma je elektromechanické zařízení připomínající psací stroj. Její vynálezce německý inženýr Arthur Scherbius se narodil 20. října 1878 ve Frankfurtu nad Mohanem. Vystudoval Technickou Univerzitu v Mnichově a později v Hannoveru. Roku 1918 založil se svým přítelem Richardem Ritterem firmu Scherbius & Ritter, která se zabývala různými technickými inovacemi. Scherbius byl vynalézavý a zručný, nejvíce se však zajímal o zdokonalení vojenských šifrovacích systémů. Svůj šifrovací stroj Enigma si nechal patentovat dne 23. 2. 1918. Nutno podotknout, že Scherbius nebyl jediný, kdo podobný stroj vynalezl. Zmiňme například Alexandra Kocha z Nizozemska, Arvida Damma ze Švédska nebo Edwarda Heberna z Ameriky. Všichni vynalezli šifrovací přístroj, všichni si jej nechali patentovat a všichni věřili, že jim přinese slávu a peníze. Jediný kdo uspěl byl právě Arthur Scherbius.

Enigma měla být neprolomitelnou šifrou, ale zpočátku nebyla přijímána ani obchodníky ani německou vojenskou správou. Obchodníci se zdráhali investovat velké peníze do koupi přístroje a vojenská správa si nebyla vědoma odhalení svého šifrovacího systému během první světové války, a tedy neměla žádné ambice zvyšovat bezpečnost utajení vojenské komunikace. Teprve roku 1923, kdy byly publikovány dokumenty, které dokazovaly selhání německé tajné služby, si velení německé armády uvědomilo jak důležitou roli ve válce hraje dobrá neprolomitelná šifra. Roku 1925 mohl Scherbius zahájit velkovýrobu svého šifrovacího stroje a o rok později jím vybavil německou armádu a státní organizace. Do konce války německá armáda disponovala přinejmenším sta tisíci přístroji Enigma

# 2. Enigma a její použití

Enigma je elektromechanický rotorový šifrovací stroj, podobající se starému psacímu stroji. Celý mechanismus tvoří tři základní jednotky navzájem propojené elektrickými vodiči. První částí je klávesnice pro zadávání otevřeného textu, druhou částí je šifrovací zařízení, které převádělo vždy každé písmeno otevřeného textu na příslušné písmeno šifrového textu a třetí částí je signální deska se žárovičkami pro zobrazení znaků šifrového textu.

Klávesnice byla tvořena 26 klávesami, kde každá klávesa reprezentovala jedno písmeno standardní latinské abecedy. Rozložení kláves bylo téměř shodné s dnešními klávesnicemi, ale chyběly klávesy jako mezera, velká písmena, interpunkce nebo číslice.

Signální deska byla tvořena 26 žárovičkami. Při stisknutí klávesy se rozsvítila některá žárovička a tím indikovala odpovídající šifrové písmeno na signální desce. Písmena na signální desce byla rozložena stejně jako na klávesnici.

Šifrovací zařízení se skládalo z několika důležitých komponent, především propojovací desky, tří rotorů zapojených postupně za sebou a reflektoru.

Propojovací deska umožňovala vzájemně prohodit několik dvojic písmen pomocí několika kabelů. Původně bylo používáno jen 6 kabelů, později se počet kabelů zvýšil až na 10. Tedy při propojení dvojice písmen, řekněme `q` a `r`, proud, který reprezentoval písmeno `q` se přístrojem šířil jako by bylo stisknuto `r` a naopak. Protože kabelů bylo jen 10, mohlo být přehozeno jen 10 párů písmen a zbylých šest písmen zůstalo nepropojeno. Tato součást měla rozhodující podíl na počtu možných kombinací nastavení stroje, avšak sama o sobě by nebyla nic platná, neboť představuje jen jednoduchou substituci. Počet možných propojení na propojovací desce při použití 6 kabelů:

$$\binom{26}{2}\cdot\binom{24}{2}\cdot\binom{22}{2}\cdot\binom{20}{2}\cdot\binom{18}{2}\cdot\binom{16}{2}\cdot\frac{1}{6!}\approx 1{,}0039\cdot 10^{11}$$

Důležitou součástí, na které je celý šifrovací mechanismus založen, představují tři otočné rotory. Rotory byly vyjímatelné, a bylo tedy možno navzájem měnit jejich pozici. Později byly přidány další dva rotory, takže obsluha stroje vždy vybrala tři z pěti možných rotorů a ty pak umístila na dané pozice na hřídel v přístroji. Každý rotor vypadal jako tlustý kotouč opatřený z obou plochých stran šestadvaceti kontakty uspořádanými do kruhu. Kontakty z jedné strany byly propojeny s kontakty z druhé strany pomocí drátků ukrytých uprostřed kotouče. Toto propojení bylo nepravidelné a pro každý rotor specifické. Kotouče byly po obvodu opatřeny zuby, kterými byl zajištěn otočný pohyb příslušného rotoru. Navíc byl každý rotor obepnut prstencem se šestadvaceti písmeny (v některých verzích čísly). Tento prstenec bylo možno uchytit na rotor v jedné z 26 pozic. Celé zařízení bylo chráněno krytem s okénky, jež umožňovaly určit polohu rotorů pomocí písmen na prstencích. Před vlastním šifrováním bylo nutno všechny rotory nastavit do smluvené výchozí pozice, jež byla součástí denního klíče (tímto se zabývá podrobně Jiří Vábek ve své diplomové práci [8]).

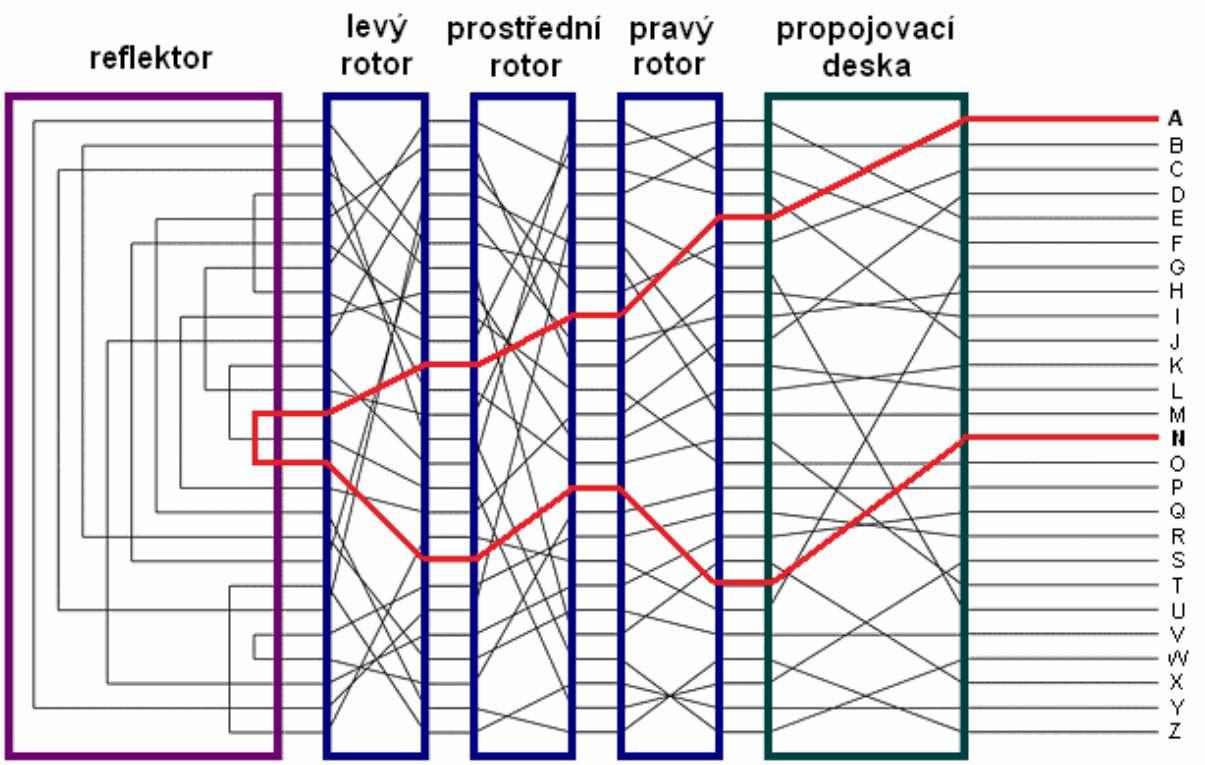
Propojovací deska byla s pravým rotorem spojena prostřednictvím vstupního rotoru. Vstupní rotor byl nepohyblivý a jeho vnitřní propojení přestavovalo identickou permutaci. Tento fakt nebyl zřejmý na první pohled, byl to však jeden ze správných předpokladů, které učinili polští kryptoalanytici při zjišťování vnitřního propojení Enigmy.

Zbývá popsat poslední část šifrovacího zařízení, a tou je reflektor. Reflektor měl podobnou konstrukci jako rotory, tlustý kotouč s vnitřním zapojením vodičů. Na rozdíl od rotorů se však

neotáčel a vodiče do něj vstupující vystupovaly opět na stejné straně. Reflektor měl tedy také 26 kontaktů, ale pouze na jedné straně kotouče. Tato součástka zajišťovala symetričnost mezi šifrováním a dešifrováním.

Jak vlastně celá Enigma fungovala? Na obrázku je znázorněno schéma vnitřního zapojení všech částí šifrovacího zařízení Enigmy. Pokud chceme zašifrovat například písmeno `a`, stiskneme příslušnou klávesu. Proud se dostane do propojovací desky, kde v našem případě je `a` spojeno s písmenem `e`. Dále proud pokračuje jako by reprezentoval písmeno `e`, projde postupně všemi třemi rotory do reflektoru, který jej pošle přes tyto tři rotory zase zpět, ale odlišnou cestou. Proud opět dorazí do propojovací desky, tentokrát reprezentující písmeno `t`. To je propojeno s písmenem `n`, což znamená, že na signální desce se rozsvítí žárovička indikující písmeno `n`. Výsledkem zašifrování písmena a je tedy písmeno `n`. Takto můžeme postupovat dále, až zašifrujeme celou zprávu.

Obr. 1: Schéma průběhu proudu Enigmou




Geniální myšlenka, kterou Scherbius převedl do funkční podoby spočívala v otočném pohybu jednotlivých rotorů. Jakým způsobem se vlastně rotory otáčely? Rotor na první pozici se pootočil vždy o 1/26 otáčky po stisknutí každé klávesy s písmenem. Rotor na druhé pozici se pootočil pouze na popud prvního rotoru a poslední rotor se pootočil pouze na popud prostředního. Způsob otáčení rotorů byl stejný jako otáčení koleček v počítadle kilometrů. Když kolečko udávající kilometry dotočí celou otáčku, pak se pohne kolečko udávající desítky kilometrů a obdobně se pohne kolečko udávající stovky kilometrů. Takovýto způsob otáčení byl zajištěn speciální součástí tvaru T, umístěnou mezi pravým a prostředním rotorem a mezi prostředním a levým rotorem. Při stisknutí klávesy se tato součást automaticky přiklopila na obvod rotorů. Pokud jedno rameno této součásti zapadlo do zářezu na prstenci v určitém rotoru, druhé rameno zapadlo do ozubení následujícího rotoru a pootočil tímto rotorem o 1/26 otáčky.

Důležitou součástí byly otočné rotory. Po každém stisknutí klávesy se vždy pro šifrování použije jiná šifrová abeceda. Ve skutečnosti se tyto abecedy začnou opakovat, ale až po 26x25x26 = 16 900 stisků kláves. Prostřední rotor poskytuje pouze 25 možností, což je dáno konstrukcí přístroje. Enigma tedy obsahuje 16 900možných šifrových abeced. Společně s počtem možných zapojení kabelů v propojovací desce a možných uspořádání rotorů na hřídeli přístroje dosahuje počet všech možných počátečních nastavení Enigmy neuvěřitelných $10^{16}$. Nepřítel, který nezná počáteční nastavení přístroje, je nucen vyzkoušet všechny možnosti. Vytrvalý kryptoanalytik, který by vyzkoušel jedno zapojení za minutu, by potřeboval k prověření všech možností dobu delší než je známý věk vesmíru.

## 2.1. Klíče

Než mohla obsluha Enigmy začít se šifrováním zprávy, musela přístroj nastavit podle příslušného denního klíče. Co to vlastně byl denní klíč? Každý operátor Enigmy obdržel jednou měsíčně kódovou knihu, která obsahovala klíče na každý den pro celý následující měsíc. Denní klíč se skládal z následujících částí:

- *Pořadí rotorů:* Původně byly rotory pouze tři, udávalo se tedy pořadí těchto tří rotorů. Později přibyly další dva rotory a tento údaj byl rozšířen o informaci, které tři z pěti rotorů vybrat (rotory byly číslovány římskými číslicemi).
- *Pozice prstenců:* Tento údaj udával pozice, ve které měly být přichyceny prstence k jednotlivým rotorům. Byla to sekvence tří písmen (v některých verzích čísel).
- *Nastavení propojovací desky:* Zde byly vypsány dvojice písmen, která se měla přehodit pomocí kabelů na propojovací desce.
- *Základní nastavení:* Toto nastavení udávalo orientaci rotorů, konkrétně určovalo tři písmena která měla být vidět v okénkách v krytu rotorů.

Uveďme si příklad, jak mohl vypadat konkrétní denní klíč:

- *Pořadí rotorů:* **II.-III.-I.**
- *Pozice prstenců:* **21-02-17**
- *Nastavení propojovací desky:* **A/L – P/R – Q/W – I/D – K/F – O/Y - J/Z - U/S - C/X - T/B**
- *Základní nastavení:* **A-C-L**

## 2.2. Nastavení Enigmy

Kdyby byla každá zpráva odesílaná v rámci jednoho dne zašifrována pomocí příslušného denního klíče, značně by to ulehčilo práci kryptoanalytikům, neboť počet odesílaných zpráv denně byl v řádu několika set. Němci proto vymysleli dodatečné pravidlo, že denním klíčem se bude šifrovat pouze tzv. klíč zprávy. Operátor Enigmy tedy nastavil přístroj podle daného denního klíče, poté náhodně zvolil trojici písmen, řekněme **Q**, **W**, **B** (klíč zprávy). Zvolená písmena zašifroval dvakrát po sobě, aby předešel případné chybě při následném přenosu zprávy. Sekvenci písmen **QWBQWB** tedy zašifroval například jako **HJNRGC**. Odesílatel následně změnil *základní nastavení* (tj. orientaci rotorů) na **Q-W-B** a mohl začít šifrovat vlastní text zprávy. Na druhé straně, příjemce zprávy nastavil Enigmu také podle daného denního klíče, zapsal prvních šest písmen, čímž získal klíč pro danou zprávu. Pak přístroj přenastavil podle tohoto klíče a již lehce dešifroval zbytek zprávy. Tímto opatřením se Němci vyhnuli posílání značného množství textu šifrovaného jediným klíčem. Výrazně tím byla ztížena práce kryptoanalytiků, ne však znemožněna.

# 3. Polské Biuro Szyfrow

Po první světové válce pokračovali spojenci v odchytávání a luštění německých depeší. Roku 1926 začali však zachycovat šifrové zprávy, se kterými si vůbec nevěděli rady. To právě vstoupila do hry Enigma. Spojenečtí kryptoanalytici se snažili s novou šifrou bojovat, ale jejich snaha nepřinášela valné výsledky a tak se brzy vzdali naděje na úspěch. Jediný stát, který si nemohl dovolit odpočívat bylo Polsko. Během první světové války bylo polské území násilně připojeno k Německu. Po německé prohře obnovilo Polsko svou nezávislost, ale obávalo se opětovného německého útoku.

V Polsku bylo založeno nové oddělení Biuro Szyfrow, které zodpovídalo za luštění nepřátelských depeší. Vedení tohoto oddělení došlo k názoru, že při luštění mechanického šifrovacího stroje by mohly mít úspěch vědecké a hlavně matematické mozky. Do té doby tajné služby vyhledávaly spíše odborníky na strukturu jazyka. Biuro uspořádalo kurs kryptografie a vybralo několik úspěšných absolventů s talentem luštit šifry. Jedním z nejnadanějších matematiků byl Marian Rejewski. Rejewského úkol byl zřejmý, rozluštit německé šifrové zprávy a tím zlomit Enigmu.

Protože se na trhu objevil šifrovací přístroj Enigma určený pro obchodní účely, mohli se kryptoanalytici právem domnívat, že německé vojsko používá k šifrování podobný přístroj. Biuro Szyfrow zakoupilo Enigmu obchodního typu a poskytlo ji Marianu Rejewskému k podrobnému prostudování. Jak se později ukázalo, tento přístroj se značně lišil od vojenské Enigmy, především vnitřním propojením vodičů v jednotlivých částech přístroje. Přes všechnu snahu se polským kryptoanalytikům nedařilo výrazně pokročit při luštění německých zpráv.

Důležitou roli v dalším postupu sehrála francouzská tajná služba, která prostřednictvím svého agenta Hans-Thilo Schmidta získala dva tajné dokumenty německé armády: *Gebrauchsanweisung für die Chiffriermaschine Enigma* (Návod k použití šifrovacího přístroje Enigma) a *Schlüsselanleitung für die Chiffriermaschine Enigma* (Instrukce ke klíči pro šifrovací přístroj Enigma). Protože však ani francouzská ani anglická tajná služba nedokázala tyto informace využít, předala získané dokumenty polskému Biuro Szyfrow na základě dohody o spolupráci.

K vítězství nad Enigmou bylo nutné splnit dva úkoly. Jednak zjistit vnitřní propojení vojenské Enigmy a přístroj zkonstruovat a jednak umět určit denní klíč pouze ze zachycených šifrových zpráv.

## *3.1. Odhalování vnitřního propojení*

Prvním obtížným krokem k úspěšnému luštění německých depeší bylo zjistit vnitřní propojení všech součástí Enigmy. Tohoto úkolu se Marian Rejewski a jeho dva polští kolegové Henryk Zygalski a Jerzy Różycki zhostili úspěšně. Nebudeme se zde zabývat podrobným popisem metod odhalování vnitřního propojení, ten lze nalézt například v diplomové práci Jiřího Vábka [8].

Němci začli používat Enigmu k šifrování svých zpráv již v období před druhou světovou válkou. Pomocí zachycených šifrových zpráv sestavil Rejewski metodu pro zjišťování

vnitřního propojení pravého rotoru. Protože se pozice rotorů na hřídeli měnila, podařilo se Rejewskému postupně stejným způsobem odhalit vnitřní propojení i zbývajících dvou rotorů.

Vnitřní propojení vstupního rotoru z propojovací desky do pravého rotoru Rejewski správně odhadl jako identickou permutaci. Nakonec se mu podařilo i správně určit vnitřní propojení v reflektoru.

Během zjišťování vnitřního propojení všech součástí přístroje Rejewski také nalezl metodu jak určit pozici zářezu pro pootočení následujícího levého (pomalejšího) rotoru na každém ze tří rotorů. Naopak také k nalezené pozici zářezu dokázal přiřadit správný rotor, čehož také využíval Różycki pro určování správného rotoru na pozici vpravo. Pro přehlednost uveďme polohy zářezů pro jednotlivé rotory.

| Rotor | Pozice zářezu |
|---|---|
| I | R |
| II | F |
| III | W |
| IV | K |
| V | A |

Ještě před vypuknutím druhé světové války znali tedy polští kryptoanalytici správné propojení vodičů ve všech součástech vojenské Enigmy. Mohli tak sestrojit repliku tohoto vojenského přístroje a pustit se směle do odhalování denního klíče.

Uveďme nakonec pro úplnost vnitřní propojení rotorů a reflektoru pro příklad řešený v kapitole 3.2.1. Odhalování klíčů zpráv a zmiňovaný v kapitole 3.2.2. Cyklometr a také v kapitole 3.2.3. Rošt.

$$rotor1 = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ e & k & m & f & l & g & d & q & v & z & n & t & o & w & y & h & x & u & s & p & a & i & b & r & c & j \end{pmatrix}$$

$$rotor2 = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ a & j & d & k & s & i & r & u & x & b & l & h & w & t & m & c & q & g & z & n & p & y & f & v & o & e \end{pmatrix}$$

$$rotor3 = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ b & d & f & h & j & l & c & p & r & t & x & v & z & n & y & e & i & w & g & a & k & m & u & s & q & o \end{pmatrix}$$

$$reflektor = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ i & m & e & t & c & g & f & r & a & y & s & q & b & z & x & w & l & h & k & d & v & u & p & o & j & n \end{pmatrix}$$

## 3.2. Metody odhalování denního klíče

Marian Rejewski a jeho kolegové z Biura Szyfrow vytvořili několik různých metod jak zjistit nastavení Enigmy pro daný den. Uvedeme pouze některé vybrané metody. Popis dalších metod lze najít v Rejewského práci [3].

Zaměřme se především na druhou část Rejewského práce, tedy jak ze získaných šifrových zpráv zjistit denní klíč Enigmy.

### 3.2.1. Odhalování klíčů zpráv

Z postupu při šifrování zpráv (viz kapitola 2.2. Nastavení Enigmy) plyne, že prvních šest písmen zprávy představuje dvakrát zašifrovaný klíč pro danou zprávu. Marian Rejewski využil tohoto dvojího šifrování k rozluštění třípísmenného klíče zprávy. Další zjednodušení práce mu připravila neuvědomělá obsluha Enigmy svými fatálními chybami při výběru klíčů zprávy. Různých třípísmenných klíčů zprávy je možné utvořit 26x26x26 = 17 576. Při tolika možnostech a v případě náhodného výběru je velice malá pravděpodobnost, že se v odchycených šifrových zprávách během jednoho dne objeví dva a více stejných klíčů. Ve skutečnosti se stejných klíčů vyskytlo mnohem více, z čehož lze vyvozovat, že šifranti nevybírali klíče zpráv náhodně, ale preferovali určité klíče jako AAA, BBB, ABC, XYZ nebo PWA, QWE apod. Tyto chyby v postupu šifrování umožňovaly určit klíče zpráv i bez hlubší znalosti konstrukce celého přístroje.

Celý postup odhalování klíčů zpráv si popišme na následujícím příkladě. Předpokládejme, že v daném dni byly zachyceny šifrové zprávy s následujícími šesti písmennými indikátory:

```
ahe rvl
ajq rro
afz ref
bhe mvl
bgg mhk
bpk myq
bpk myq
cjl hrs
cgy hhi
cgy hhi
dgq iho
dgq iho
dgq iho
ewb pfv
ein pob
ein pob
ein pob
eny pui
eny pui
fwa tfu
gct ypw
hvh bkm
hzi bmc
hgo bhy
hmt blw
irc oba
igd ohr
jgd ahr
jlf azj
jmh alm
jij aoz
kel cns
lxb xtv
lwc xfa
lnr xue
lsu xjx
ldz xqf
mqb sxv
mnh sum
mjo sry
mnr sue
nke ugl
nbq uio
nbq uio
nbq uio
oab qwv
otc qda
oar qwe
oar qwe
pnb nuv
pqk nxq
pqk nxq
qon jsb
qtt jdw
qev jnd
srb vbv
sdc vqa
sdc vqa
scm vpn
sfq veo
tgp wht
tiu wox
ule kzl
uqk kxq
uam kwn
uur kae
uur kae
uqu kxx
vrp gbt
vdx gqg
vdx gqg
wsc lja
wyu lcx
wuz laf
xnf duj
xel dns
yri ebc
yby eii
ynz euf
zln fzb
```

Každý indikátor jsme rozdělili na dvě části po třech písmenech. První část představuje klíč zprávy po prvním zašifrování a druhá část představuje stejný klíč po druhém zašifrování.

Všechny následující úvahy jsou správné, pokud předpokládáme, že při šifrování prvních šesti písmen se pootočil vždy pouze první rotor. Pohyb druhého eventuálně třetího rotoru způsobuje prstenec umístěný na obvodu prvního rotoru, jak je popsáno v kapitole 2. Počet možných nastavení prstence prvního rotoru je 26, z nichž 21 pozic vyhovují naší úvaze. Tedy následující postup bude fungovat zhruba pro tři čtvrtiny dní.

Uvažujme nejprve pouze písmena na druhé a páté pozici v indikátoru. Podívejme se například na indikátor `oab qwv`. Druhé písmeno je `a`, páté `w`. Zapišme tato dvě písmena v uvedeném pořadí:

`aw`

Nyní hledejme indikátor jehož druhé písmeno je `w`. Je jím `ewb pfv`. Páté písmeno je `f`, připišme jej tedy ke dvojici `dv`:

`awf`

Dále hledejme indikátor jehož druhé písmeno je `f`. Je jím `afz ref`. Páté písmeno je `e`, připišme je tedy na konec dosud nalezené posloupnosti:

`awfe`

Takto postupujeme dále, až obdržíme posloupnost písmen:

`awfenu`

Dalším písmenem by bylo `a`, ale to se již vyskytuje na začátku posloupnosti. Tímto postupem jsme tedy obdrželi uzavřený cykl, který zapisujeme:

`(awfenu)`

Takto získaný cykl je jednoznačně určený až na zápis (viz Dodatek: Kapitola o permutacích).

Zvolme nyní písmeno, které se v nalezeném cyklu nevyskytuje, například `b`. Celý proces opakujme nyní znovu s použitím písmena `b` na začátku. Obdržíme další cykl:

`(biosjr)`

Protože jsme tímto způsobem pořád ještě nevyčerpali všechna písmena abecedy, zvolíme další písmeno, které se nevyskytuje v žádném z předchozích cyklů, a proces opakujeme znovu. Obdržíme tak ještě další cykly:

`(dqxt) (ghvk) (cpy) (lzm)`

Všechny takto získané cykly zapíšeme bezprostředně za sebe:

$A_2A_5$ = `(awfenu)(biosjr)(dqxt)(ghvk)(cpy)(lzm)`

Označení $A_2A_5$ vyjadřuje, že cykly vznikly z druhých a pátých písmen indikátorů. Toto označení zároveň vyjadřuje, že permutace $A_2A_5$ je součínem dvou permutací $A_2$ a $A_5$. Stejným způsobem vytvoříme posloupnosti cyklů:

$A_1A_4$ = `(arzftwlxdioqj)(bmsvgyepnukch)`

$A_3A_6$ = `(auxgkqoyic)(bvdrelshmn)(fjz)(ptw)`

Kde $A_1A_4$ vzniklo z prvních a čtvrtých písmen a $A_3A_6$ vzniklo z třetích a šestých písmen indikátorů. Při vytváření cyklů permutace $A_1A_4$ narazíme hned zpočátku na problém. V našem

seznamu indikátorů se totiž nevyskytuje indikátor začínající písmenem r. Tento nedostatek snadno odstraníme pokud si všimneme, že mezi čtvrtými písmeny indikátorů se vyskytují všechny až na písmeno z. Zřejmě tedy první písmeno r odpovídá čtvrtému písmenu z.

Než budeme pokračovat v dalších úvahách, všimněme si dvou důležitých konstrukčních vlastností Enigmy.

Vnitřní propojení reflektoru (viz Obr. 1) je příčinou skutečnosti, že žádné písmeno nemůže být zašifrováno samo sebou. Konkrétně při zmáčknutí klávesy a při různých počátečních nastaveních přístroje se rozsvítí různé žárovky, ale nikdy ta, která indikuje písmeno a. Tuto vlastnost můžeme nazvat *Pravidlo výlučnosti*. Ze stejného důvodu jsou šifrování a dešifrování symetrické procesy. Přesněji, pokud při určitém nastavení Enigmy zmáčknutí klávesy a způsobilo rozžhnutí žárovičky indikující písmeno b, pak při stejném počátečním nastavení zmáčknutí klávesy b způsobí rozžhnutí žárovičky indikující písmeno a. Tuto vlastnost můžeme nazvat *Pravidlo vzájemnosti*.

Vrátíme-li se nyní k nalezeným permutacím, vidíme, že cykly stejné délky se vyskytují v každé z permutací $A_1A_4$, $A_2A_5$ a $A_3A_6$ v sudém počtu. Formální důkaz tohoto poznatku uvedeme v Dodatku: Kapitola o prermutacích, zde se pokusme na příkladu vysvětlit, proč tomu tak musí být.

V permutaci $A_3A_6$ se vyskytuje třípísmenný cykl (fjz). Podívejme se, ze kterých indikátorů uvažovaný cykl vznikl:

jlf azj

jij aoz

ajz ref

Zajímají nás pouze třetí a šestá písmena těchto indikátorů. Zmáčknutí určitého písmena, označme jej 1, rozsvítí žárovičku s písmenem f na třetí pozici a na šesté pozici rozsvítí žárovičku s písmenem j. Z *Pravidla výlučnosti* je písmeno 1 různé od f i od j. Zmáčknutí jiného písmena, odznačme jej 2, rozsvítí žárovičku s písmenem j na třetí pozici a na šesté pozici rozsvítí žárovičku s písmenem z. Opět z *Pravidla výlučnosti* je písmeno 2 různé od j i od z. Nakonec označme 3 písmeno, které rozsvítí žárovičku s písmenem z na třetí pozici a s písmenem f na šesté pozici. Písmeno 3 je samozřejmě také různé od z i od f. Nyní z *Pravidla vzájemnosti* plyne, že zmáčknutí klávesy f na třetí pozici rozsvítí žárovičku indikující písmeno 1 a na šesté pozici rozsvítí žárovičku indikující písmeno 3. Podobně stisknutí klávesy j na třetí pozici rozsvítí žárovičku indikující písmeno 2 a na šesté pozici rozsvítí žárovičku indikující písmeno 1. Nakonec také stisknutí klávesy z na třetí pozici rozsvítí žárovičku indikující 3 a na šesté pozici 2. Vidíme tedy, že v permutaci $A_3A_6$ se musí kromě cyklu (fjz) vyskytovat další tří písmenný cykl (132). Skutečně, náš hledaný cykl je (ptw). Tedy vidíme, že cykly stejné délky se vyskytují v sudém počtu.

Podobným o něco složitějším způsobem, můžeme vyjasnit párový výskyt vícepísmenných cyklů v každém rozkladu permutací. Přičemž platí, že stisknutí klávesy označené písmenem nacházejícím se v jednom cyklu způsobí rozžhnutí žárovičky indikující písmeno nacházející se v druhém cyklu stejné délky.

Popišme si ještě jednu vlastnost, kterou zaznamenal také Rejewski. Jestliže při určitém nastavení Enigmy stisknutí klávesy a rozsvítí žárovičku indikující písmeno b, pak stisknutí klávesy nacházející se v cyklu vpravo (popř. vlevo) od a rozsvítí žárovičku indikující

písmeno nacházející se v cyklu vlevo (popř. vpravo) od b. Ukažme si na příkladě, co to vlastně znamená.

V rozkladu permutace $A_2A_5$ se vyskytují třípísmenné cykly (lzm) a (cpy). V seznamu indikátorů zachycených šifrových zpráv nalezneme ty indikátory, ze kterých vznikly uvedené cykly:

| (lzm) | (cpy) |
|---|---|
| jlf azj | gct ypw |
| hzi bmc | bpk myq |
| hmt blw | wyu lcx |

Předpokládejme nyní, že stisknutí klávesy l rozsvítilo žárovičku indikující písmeno p. Chceme tedy ukázat, že při zmáčknutí klávesy z (což je napravo od l) rozsvítí žárovičku indikující písmeno c (což je nalevo od p). Podobně pak pro m a y.

Při zmáčknutí klávesy l na druhé pozici se rozsvítí písmeno p (to předpokládáme). Pak při zmáčknutí klávesy l na páté pozici se musí rozsvítit písmeno y. To plyne z indikátoru bpk myq. Naopak musí platit, že při stisknutí klávesy p na druhé pozici se rozsvítí písmeno l, a při stisknutí klávesy p na páté pozici se nutně rozsvítí písmeno z (z indikátoru jlf azj). Pak z *Pravidla vzájemnosti* plyne, že se při zmáčknutí písmena z na páté pozici rozsvítí písmeno p. Opět z indikátoru gct ypw vidíme, že při zmáčknutí písmena z na druhé pozici se rozsvítí písmeno c. Nakonec pro písmeno m nám zbývá jen písmeno y.

Podobně se popsaná vlastnost ukáže i pro cykly jiných délek.

Pokračujme dále v odkrývání klíčů zpráv. Podívejme se na permutaci $A_3A_6$. Obsahuje dva třípísmenné cykly (fjz) a (ptw). Z předchozí úvahy víme, že písmena těchto dvou cyklů si vzájemně odpovídají jako písmena šifrová a otevřená. Máme celkem tři možnosti přiřazení šifrovým písmenům f, j a z otevřená písmena p, t a w:

| f | j | z |
|---|---|---|
| p | w | t |
| w | t | p |
| t | p | w |

Vyzkoušíme-li postupně všechny tři možnosti zjistíme, že pouze jedna vede ke správnému výsledku. V našem případě je správnou volbou zobrazení písmene f na p, písmene j na w a písmene z na t.

Jak jsme již zmiňovali, šifranti preferovali určité klíče zpráv. Předpokládejme, že jeden ze zvolených klíčů je ppp. Zkusme tedy potvrdit tuto hypotézu.

Pokud byl klíč zprávy ppp použit, bude odpovídat některému indikátoru, který má na třetím místě písmeno f. Indikátor xnf duj můžeme vyloučit, protože písmena n a p se v rozkladu $A_2A_5$ vyskytují ve dvou cyklech různé délky. Zbývá tedy indikátor jlf azj. Můžeme se tedy domnívat, že tento odpovídá klíči zprávy ppp.

Zapišme nyní odpovídající si cykly pod sebou tak, aby se v cyklech z rozkladu $A_1A_4$ pod písmenem j nacházelo písmeno p, v cyklech z rozkladu $A_2A_5$ pod písmenem l písmeno p a v cyklech z rozkladu $A_3A_6$ pod písmenem f písmeno p. Přičemž v dolních řadách je posloupnost písmen v cyklu obrácená vzhledem k vlastnosti popsané výše.

```
arzftwlxdioqj
eygvsmbhckunp

     lzm
     pcy

     fjz
     pwt
```

Pokud nahradíme šifrová písmena indikátorů za tato známá otevřená písmena získáme částečně odhalené klíče zpráv. Podíváme-li se například na indikátor `bpk myq`, dostaneme neúplný klíč zprávy `ll?`. Můžeme opět předpokládat, že tento klíč zprávy bude `lll`. Přiřadíme tedy šifrovému písmenu `k` na třetím místě otevřené písmeno `l`. Zapíšeme další odpovídající si cykly z rozkladu $A_3A_6$, tak aby se pod písmenem `k` nacházelo písmeno `l`.

```
auxgkqoyic
nmhslerdvb
```

Nahradíme další šifrová písmena. indikátorů za příslušná otevřená písmena. Zkoušením dalších možností klíčů zpráv a trochou kombinování lze takto uspořádat i zbývající cykly jednotlivých rozkladů.

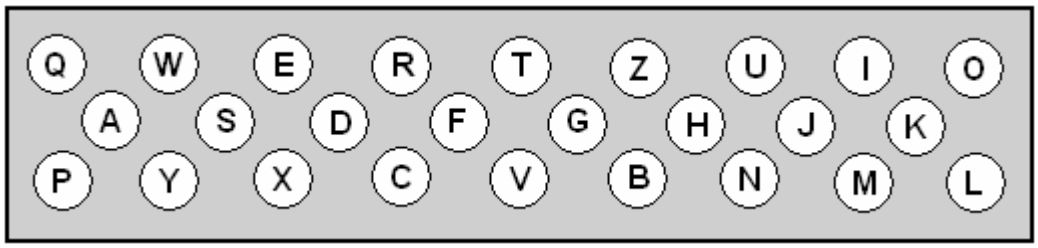
```
arzftwlxdioqj
eygvsmbhckunp

awfenu  dqxt  lzm
ibrjso  gkvh  pcy

 auxgkqoyic  fjz
 nmhslerdvb  pwt
```

Prostřednictvím takto uspořádaných cyklů již jednoduše přiřadíme každému indikátoru odpovídající klíč zprávy. Pro úplnost uveďme získané klíče zpráv.

```
ahe rvl :  ETQ        jmh alm :  PYX        srb vbv :  TFC
ajq rro :  EEE        jij aoz :  PAW        sdc vqa :  TGB
afz ref :  ERT        kel cns :  IJK        scm vpn :  TZU
bhe mvl :  LTQ        lxb xtv :  BVC        sfq veo :  TRE
bgg mhk :  LDS        lwc xfa :  BBB        tgp wht :  SDF
bpk myq :  LLL        lnr xue :  BSO        tiu wox :  SAM
cjl hrs :  DEK        lsu xjx :  BNM        ule kzl :  OPQ
cgy hhi :  DDD        ldz xqf :  BGT        uqk kxq :  OKL
dgq iho :  CDE        mqb sxv :  WKC        uam kwn :  OIU
ewb pfv :  ABC        mnh sum :  WSX        uur kae :  OOO
ein pob :  AAA        mjo sry :  WER        uqu kxx :  OKM
eny pui :  ASD        mnr sue :  WSQ        vrp gbt :  FFF
fwa tfu :  VBN        nke ugl :  QQE        vdx gqg :  FGH
gct ypw :  ZZZ        nbq uio :  QWE        wsc lja :  MNB
hvh bkm :  XXX        oab qwv :  UIC        wyu lcx :  MMM
hzi bmc :  XCV        otc qda :  UHB        wuz laf :  MOT
hgo bhy :  XDR        oar qwe :  UIO        xnf duj :  HSP
hmt blw :  XYZ        pnb nuv :  JSC        xel dns :  HJK
irc oba :  KFB        pqk nxq :  JKL        yri ebc :  RFV
igd ohr :  KDY        qon jsb :  NUA        yby eii :  RWD
jgd ahr :  PDY        qtt jdw :  NHZ        ynz euf :  RST
jlf azj :  PPP        qev jnd :  NJI        zln fzb :  GPA
```

Podíváme-li se na zjištěné otevřené indikátory vidíme, jakých chyb se šifranti při výběru klíčů dopouštěli. Značná část klíčů tvoří buď tři stejná písmena nebo tři písmena jdoucí po sobě v abecedě. Objevují se také klíče jako `PYX`, `QWE`, `RFV`. Porovnáme-li tento výběr klíčů s klávesnicí přístroje zjistíme, že jsou to trojice sousedních kláves.

Obr. 2: Schéma klávesnice Enigmy




Ve skutečnosti práce na rekonstrukci klíčů zpráv nebyla tak jednoduchá, jak ukazuje popsaný příklad. Bylo potřeba velké množství zachycených indikátorů a ne vždy pokryly celou abecedu. Což způsobovalo problémy již při sestavování rozkladů na cykly. Navíc cykly mohly být dlouhé v rozmezí jednoho až třinácti písmen. V rozkladu se mohlo také například vyskytovat šest čtyřpísmenných cyklů. Určení vazeb mezi cykly mohlo být tedy také složitější.

Postupem času se však Němcům podařilo odstranit většinu šifrátorských chyb. Z tohoto důvodu se polští kryptoanalytici pokoušeli vymyslet nové efektivnější metody odhalování denních klíčů. Zmiňme jen některé z dalších používaných metod.

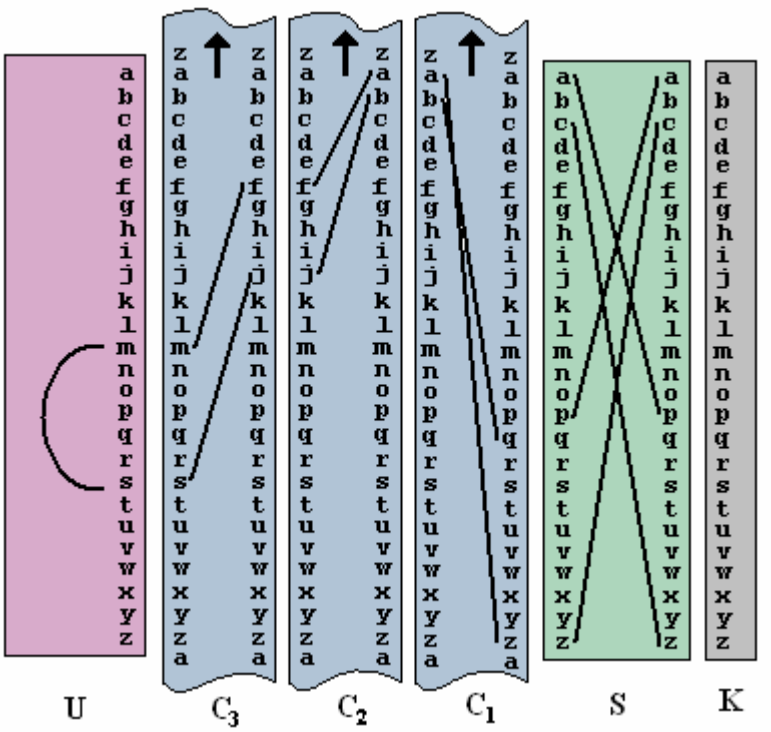
- Metoda statistická spočívala ve zjištění, že písmena se v klíčích zpráv nevyskytují se stejnou frekvencí. Například na prvním místě byla častější A a Q než jiná písmena, na druhém místě se vyskytovaly nejvíce všechny samohlásky a na třetím místě byla nejčastější L a O.
- Metoda různých písmen se zakládala na zákazu vybírání stejných tří písmen pro klíče zpráv. Němečtí šifranti se tímto rozkazem řídili tak pilně, že se vyhýbali jakémukoliv opakování. Přestali používat dokonce i klíče jako AAB nebo FVF, kde se opakují dvě písmena. Takový postup usnadnil hledání vazeb mezi jednotlivými cykly rozkladu.

### 3.2.2. Cyklometr

Další nesnadnou částí úkolu bylo zjistit vazby na propojovací desce. Rejewski chtěl sestrojit katalog určitých charakteristických vlastností pro každé počáteční nastavení Enigmy. K tomuto účelu zkonstruoval přístroj, který nazýval cyklometr.

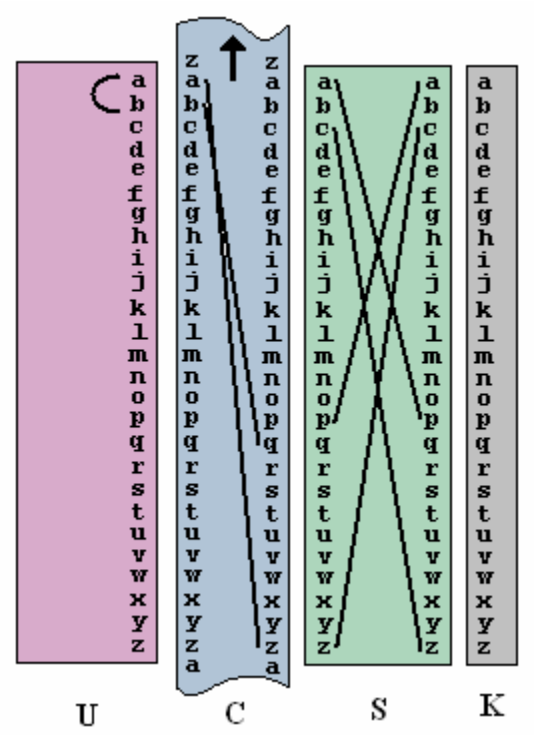
Pro lepší pochopení procesů probíhajících uvnitř mechanizmu, utvořme z třírozměrného přístroje dvourozměrný model. Místo otočných rotorů si můžeme představit posuvnou pásku dostatečně dlouhou na obě strany. Obrázek představuje takovýto dvourozměrný model Enigmy. Sloupec písmen *K* zcela vpravo představuje klávesnici popř. žárovičky. Nalevo od něj se nachází neposuvná páska *S*, označující propojovací desku. Další tři posuvné pásky $C_1$, $C_2$, $C_3$ představují tři otočné rotory a úplně vlevo se nachází sloupec písmen *U* reprezentující reflektor.

Obr. 3: Dvourozměrný model Enigmy




Na obrázku je znázorněno jen několik propojení uvnitř přístroje. Můžeme sledovat, jak proud putuje přístrojem po zmáčknutí klávesy `a`. Pak se páska $C_1$ (pravý rotor) posune ve směru šipky o jedno písmeno a přístroj je připraven k dalšímu použití. Protože nevíme, v kterém okamžiku se pootočí prostřední rotor $C_2$, předpokládejme, že při šifrování prvních šesti písmen se nepootočí vůbec. Levý rotor $C_3$ se tedy také nepootočí. Díky tomuto předpokladu, se pásky *U*, $C_2$ a $C_3$ vůči sobě neposunou. Proto můžeme tyto tři pásky reprezentovat jedinou abstraktní páskou, kterou označíme *U*. Náš dvourozměrný model se tak zjednodušil pouze na tři pásky *S*, *C* a *U*.

Obr. 4: Zjednodušený dvourozměrný model Enigmy




Pokusme se vyjádřit počáteční stav přístroje $A_0$ pomocí permutací. Postupujme podle Obr. 4. Proud vstupuje do propojovací desky s permutací $S$. Pak pokračuje páskou s permutací $C$ a nakonec vejde do abstraktní pásky s permutací $U$. Dále proud postupuje zpátky opačným směrem, tedy přes permutace $C^{-1}$ a $S^{-1}$. Můžeme tedy zapsat rovnost:

$$A_0 = SCUC^{-1}S^{-1}.$$

Poznamenejme, že permutace $S$ a $S^{-1}$ jsou stejné, jak je vidět z vlastnosti permutace $S$ a ze způsobu zapojení na propojovací desce.

Nyní se pokusíme popsat pohyb rotorů. Definujme permutaci $P$, která zobrazuje každé písmeno na svého následovníka v abecedě:

$$P = (\mathtt{abcdefghijklmnopqrstuvwxyz})$$

Při prvním stisknutí klávesy se pootočí pravý rotor, což odpovídá posunutí pásky $C$ ve směru šipky o jedno písmeno. Tento pohyb je adekvátní použití permutace $P$ při vstupu proudu do rotoru a permutace $P^{-1}$ při opouštění rotoru. První stisknutí klávesnice lze tedy popsat permutacemi:

$$A_1 = SPCP^{-1}UPC^{-1}P^{-1}S^{-1}$$

Snadno můžeme odvodit vzorec pro druhé stisknutí klávesy, kdy se páska posune o další písmeno ve směru šipky:

$$A_2 = SP^2CP^{-2}UP^2C^{-1}P^{-2}S^{-1}$$

A podobně další rovnosti:

$$A_3 = SP^3CP^{-3}UP^3C^{-1}P^{-3}S^{-1}$$

$$A_4 = SP^4CP^{-4}UP^4C^{-1}P^{-4}S^{-1}$$

Zaměřme se nyní na permutace $A_1$ a $A_4$, odpovídající prvnímu a čtvrtému stisknutí klávesy. Utvořme součin $A_1A_4$:

$$A_1A_4 = SPCP^{-1}UPC^{-1}P^3CP^{-4}UP^4C^{-1}P^{-4}S^{-1}$$

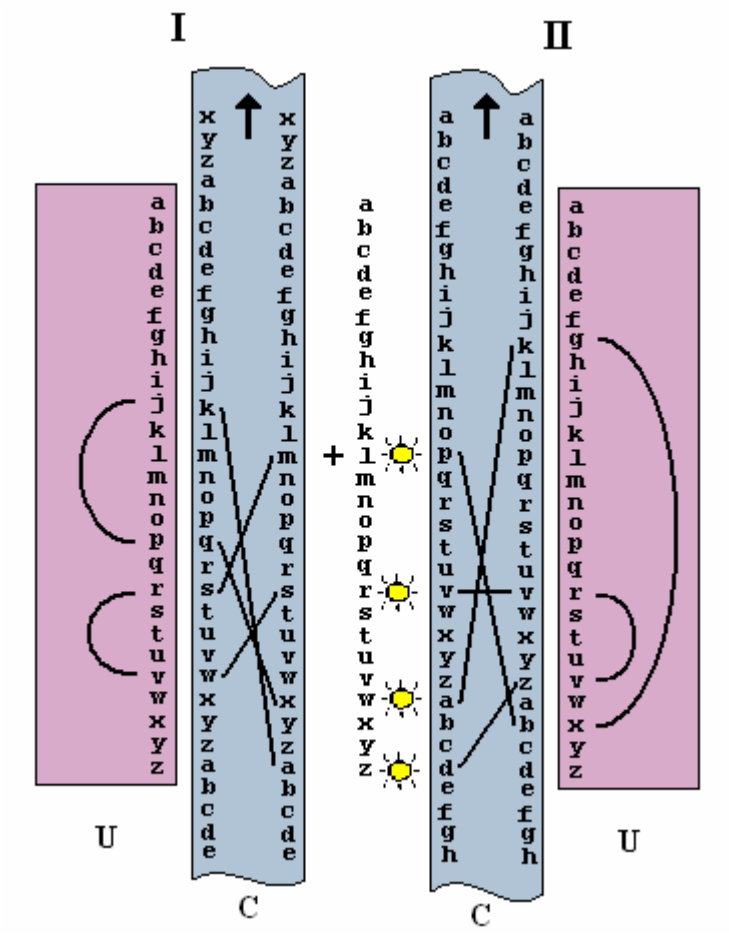
Tento součin permutací je konjugovaný (viz Dodatek: Kapitola o permutacích) se součinem $B_1B_4$. Kde

$$B_1B_4 = PCP^{-1}UPC^{-1}P^3CP^{-4}UP^4C^{-1}P^{-4}.$$

V součinu $B_1B_4$ neznáme pouze permutace $C$ a $U$, které jsou definovány vzájemnou pozicí rotorů. Těchto pozic je 26x26x26 = 17 576, což není tak mnoho. K vytvoření kartotéky obsahující všechny možnosti právě sloužil cyklometr.

Cyklometr se skládal ze dvou spřažených přístrojů Enigma, bez propojovací desky, bez přenastavitelných prstenců, bez klávesnice, ale navíc s elektrickým přepínačem u každé žárovky. Funkci cyklometru ukazuje následující obrázek.

Obr. 5: Schéma zapojení cyklometru




V části II na tomto obrázku je pořadí rotorů opačné než v části I, přičemž páska $U$ reprezentuje dva otočné rotory a reflektor jako ve zjednodušeném dvourozměrném modelu Enigmy. Mezi oběma částmi cyklometru se nachází systém žárovek s elektrickými přepínači. Páska $C$ v části II je předsunuta o tři písmena oproti pásce $C$ v části I. Označíme-li tedy pozici rotorů v části I jako $A_1$, pak pozice rotorů v části II odpovídá $A_4$.

Nyní můžeme k libovolné žárovce zapojit zdroj proudu pomocí příslušného elektrického přepínače. Zapojme například žárovku `l`, jako na obrázku. Proud bude postupně procházet oběma částmi cyklometru, až se po určitém počtu průběhu vrátí opět do zapojené žárovky `l`, čímž se uzavře elektrický obvod. Zároveň se rozsvítí žárovky, kterými proud postupně

procházel. Počet těchto žárovek je samozřejmě sudý a odpovídá dvojnásobnému počtu písmen v některém z cyklů permutace $A_1A_4$. Náš příklad zobrazuje dva dvoupísmenné cykly. Písmena se však částečně liší od skutečných písmen v cyklech permutace $A_1A_4$, protože v cyklometru není zapojena propojovací deska. Po zapojení zdroje proudu k dalšímu přepínači se rozsvítí jiné žárovky, z jejichž počtu získáme informaci o délce dalšího cyklu.

Pomocí cyklometru můžeme takto popsat délky cyklů permutací $B_xB_{x+3}$ Otáčíme postupně rotory v cyklometru a počítáme rozsvícené žárovky. Sestavíme tak katalog délek cyklů permutací pro všech 17 576 vzájemných pozic rotorů.

Pro přehlednost katalogu je nutné očíslovat všechny permutace, které mohou vzniknout.

Tab. 1: Očíslování permutací

| Permutace | Pořadové číslo |
|---|---|
| (13) (13) | 1 |
| (12) (12) (1) (1) | 2 |
| (11) (11) (2) (2) | 3 |
| (11) (11) (1) (1) (1) (1) | 4 |
| … | … |
| (1) (1) (1) (1) … (1) (1) | 101 |

Do katalogu pak pro každou pozici rotorů zapisujeme příslušné pořadové číslo permutace a další dvě pořadová čísla odpovídající permutacím pro následující dvě pozice rotorů. Tato tři čísla se nazývají *charakteristika*.

Tab. 2: Příklad získaných charakteristik

| Pozice rotorů | Charakteristika |
|---|---|
| a a a | 7, 6, 9 |
| a a b | 6, 9, 1 |
| a a c | 9, 1, 3 |
| a a d | 1, 3, 12 |
| … | … |
| z z z | 10, 1, 1 |

Takovýchto katalogů polští kryptoanalytici vytvořili 6, pro šest různých umístění původních tří rotorů na hřídeli v přístroji. V rámci jedné kartotéky se mohlo vyskytnout více stejných charakteristik.

Vytvoříme-li nyní permutace $A_1A_4$, $A_2A_5$ a $A_3A_6$ ze získaných indikátorů během dne a vytvoříme příslušnou *charakteristiku*, pak ji můžeme vyhledat v katalogu a získáme odpovídající umístění rotorů na hřídeli i jejich nastavení (tj. skutečnou polohu rotorů) pro daný den. Pokud pro danou charakteristiku nalezneme více různých nastavení, lze přímo na přístroji Enigma jednoduše ověřit, které nastavení je správné.

Potřebujeme ještě zjistit zapojení na propojovací desce pro daný den. Nastavíme tedy rotory Enigmy podle pozice získané v katalogu a utvoříme součiny permutací $B_1B_4$, $B_2B_5$ a $B_3B_6$. Porovnáním s permutacemi získanými z příslušných indikátorů dostaneme permutaci $S$,

charakterizující zapojení na propojovací desce. Ukážeme si celý postup na našem příkladě z kapitoly 3.1.1. Odhalování klíčů zpráv.

Ze zachycených indikátorů utvoříme příslušné součiny permutací:

$$A_1A_4 = \texttt{(arzftwlxdioqj)(bmsvgyepnukch)}$$

$$A_2A_5 = \texttt{(awfenu)(biosjr)(dqxt)(ghvk)(cpy)(lzm)}$$

$$A_3A_6 = \texttt{(auxgkqoyic)(bvdrelshmn)(fjz)(ptw)}$$

Vidíme, že odpovídající *charakteristika* je 1, 37, 5. Tuto charakteristiku vyhledáme v některém z katalogů. Předpokládejme, že odpovídá nastavení rotorů `g a r`. V Enigmě bez zapojení na propojovací desce nastavíme příslušné rotory do těchto pozic a postupně vyťukáme celou abecedu na klávesnici. Získáme tak permutaci $B_1$.

$$B_1 = \texttt{(ae)(bt)(cz)(dm)(fu)(gw)(ho)(ik)(jy)(ln)(pq)(rv)(sx)}$$

Stejným způsobem vyťukáme celou abecedu při pozici rotorů `g a v`, tedy o tři pozice dál. Získáme tak permutaci $B_4$.

$$B_4 = \texttt{(ab)(ct)(di)(el)(fp)(gr)(hz)(ju)(ko)(ms)(nq)(vx)(wy)}$$

Vynásobíme obě permutace a obdržíme:

$$B_1B_4 = \texttt{(rxmioztalqfjw)(bchkdsvgyupne)}$$

Víme, že permutace $B_1B_4$ je konjugována s permutací $A_1A_4$, protože platí $A_1A_4 = SB_1B_4S^{-1}$. Permutace $S$ má speciální tvar. Skládá se pouze z transpozic a z cyklů délky 1. Víme, že pouze vzájemně zaměňuje některá písmena, ale nezmění cyklickou strukturu permutace $B_1B_4$. Stačí tedy porovnat permutaci $A_1A_4$ se získanou permutací $B_1B_4$ abychom zjistili permutaci $S$. Permutace musíme postupně porovnávat pro všechny možné způsoby zápisu. Pro správné určení permutace $S$ musí platit, že pokud se `a` zobrazí na `b`, pak také `b` se musí zobrazit na `a`.

$$A_1A_4 = \texttt{(arzftwlxdioqj)(bmsvgyepnukch)}$$

$$B_1B_4 = \texttt{(rxmioztalqfjw)(bchkdsvgyupne)}$$

$$B_1B_4 = \texttt{(xmioztalqfjwr)(chkdsvgyupneb)}$$

$$\cdots$$

$$B_1B_4 = \texttt{(alqfjwrxmiozt)(kdsvgyupnebch)}$$

Pokud nevypisujeme jednopísmenné cykly, pak získaná permutace $S$ je:

$$S = \texttt{(bk) (dm) (eu) (jt) (lr) (qz)}$$

Ne vždy byl tento postup tak přímočarý. V katalogu se vyskytovalo více stejných charakteristik pro různé pozice rotorů, pak bylo velice pracné zjistit správné nastavení rotorů pro daný den. Navíc katalog byl sestavován za předpokladu, že se během šifrování prvních šesti písmen pootočil vždy jen pravý rotor. Pokud se tedy během šifrování klíče zprávy pootočil prostřední popřípadě i levý rotor, pak samozřejmě nemohla být nalezena správná pozice rotorů.

Katalog sice mohl být rozšířen o charakteristiky pro pohyb prostředního a levého rotoru, ale tím by přibylo více stejných charakteristik a celý katalog by začal postrádat smysl. Místo toho se polští kryptoanalytici snažili vymyslet jiné účinější metody pro určování nastavení Enigmy.

### 3.2.3. Rošt

Popišme si nyní metodu, kterou Rejewski nazval rošt. Metoda roštu sloužila ke zjišťování zapojení kabelů na propojovací desce. Ukažme si celý postup na názorném příkladě použitém v Rejewského práci [5].

V předchozí kapitole jsme vyjádřili permutace $A_1$, $A_2$, $A_3$,…, $A_6$ pomocí permutací $P$, $S$, $C$ a $U$. Uveďme si je zde pro přehlednost znovu:

$$A_1 = SPCP^{-1}UPC^{-1}P^{-1}S^{-1}$$
$$A_2 = SP^2CP^{-2}UP^2C^{-1}P^{-2}S^{-1}$$
$$A_3 = SP^3CP^{-3}UP^3C^{-1}P^{-3}S^{-1}$$
$$\dots$$
$$A_6 = SP^6CP^{-6}UP^6C^{-1}P^{-6}S^{-1}$$

Z těchto rovnic lze vyjádřit permutaci $U$:

$$U = PC^{-1}P^{-1}S^{-1}A_1SPCP^{-1}$$
$$U = P^2C^{-1}P^{-2}S^{-1}A_2SP^2CP^{-2}$$
$$U = P^3C^{-1}P^{-3}S^{-1}A_3SP^3CP^{-3}$$
$$\dots$$
$$U = P^6C^{-1}P^{-6}S^{-1}A_6SP^6CP^{-6}$$

Permutaci $U$ sice neznáme, víme však, že pokud při šifrování indikátoru, tj. prvních šesti písmen počátku zprávy, se pootočil vždy pouze první rotor, pak permutace $U$ je stejná pro všech šest rovností. Jestliže se během šifrování indikátoru pootočil i prostřední rotor, pak permutace $U$ nabývá dvou různých hodnot. Jedna hodnota charakterizuje stav před a druhá stav po pootočení prostředního rotoru. V každém případě první tři nebo poslední tři hodnoty permutace $U$ se shodují. Předpokládejme například, že první tři hodnoty permutace $U$ jsou stejné.

Permutace $A_1$, $A_2$ a $A_3$ získáme při metodě zjišťování klíčů zpráv popsané v kapitole 3.1.1. Odhalování klíčů zpráv. Každá z těchto permutací se skládá z 13 transpozic.

$A_1$ = (as)(br)(cw)(di)(ev)(fh)(gn)(jo)(kl)(my)(pt)(qx)(uz)

$A_2$ = (ay)(bj)(ct)(dk)(ei)(fn)(gx)(hl)(mp)(ow)(qr)(su)(zv)

$A_3$ = (ax)(bl)(cm)(dg)(ei)(fo)(hv)(ju)(kr)(np)(qs)(tz)(wy)

Permutace $S$ nezaměňuje všechna písmena, proto lze očekávat, že v každé z permutací $A_1$, $A_2$ a $A_3$ zůstane několik transpozic nezměněno při konjugování permutací $S$. Toto tvzení je skutečně pravdivé, přičemž vždy aspoň jedna transpozice zůstane nezměněna. Vysvětleme si, proč tomu tak je.

Permutace $S$ mění pouze 12 písmen a permutace $S^{-1}$ je shodná s permutací $S$. Protože každá z permutací $A_1$, $A_2$ a $A_3$ je tvořena třinácti transpozicemi, nemůže se stát, že by permutace $S$ změnila všech 13 transpozic, vždy aspoň jedna zůstane nezměněna. Případ, kdy zůstane nezměněna právě jedna transpozice odpovídá situaci, kdy každé z dvanácti písmen permutace $S$ se nachází v různých transpozicích permutací $A_1$ resp. $A_2$ nebo $A_3$.

Pokračujme nyní dále v popisování Rejewského metody roštu. Vynecháním permutace $S$ ve všech rovnicích pro permutaci $U$, získáme vyjádření:

$$PC^{-1}P^{-1}A_1PCP^{-1}$$
$$P^2C^{-1}P^{-2}A_2P^2CP^{-2}$$
$$P^3C^{-1}P^{-3}A_3P^3CP^{-3}$$

Tato vyjádření již nebudou rovny permutaci $U$, ani nebudou rovny mezi sebou. Je však značná pravděpodobnost, že se některé transpozice budou ve všech třech rovnicích opakovat. Budeme tedy hledat nějaké opakující se transpozice, přesněji jak píše Rejewski v práci [3] „pewne podobieństwa“.

Ačkoliv známe vnitřní zapojení rotoru $C$, neznáme jeho počáteční nastavení. Různých pozic rotoru $C$ je však pouze 26. Všechny permutace odpovídající všem pozicím rotoru $C$ získáme postupným konjugováním (viz Dodatek: Kapitola o permutacích) permutacemi $P$, $P^2$, …, $P^{25}$. Permutace $P^{26}CP^{-26}$ je již stejná jako permutace $C$. Získáme tedy následující vzorce:

$$C = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ k & j & p & z & y & d & t & i & o & h & x & c & s & g & u & b & r & n & w & f & m & v & e & q & l & a \end{pmatrix}$$

$$PCP^{-1} = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ i & o & y & x & c & s & h & n & g & w & b & r & f & t & a & q & m & v & e & l & u & d & p & k & z & j \end{pmatrix}$$

$$P^2CP^{-2} = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ n & x & w & b & r & g & m & f & v & a & q & e & s & z & p & l & u & d & k & t & c & o & j & y & i & h \end{pmatrix}$$

…

$$P^{25}CP^{-25} = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ b & l & k & q & a & z & e & u & j & p & i & y & d & t & h & v & c & s & o & x & g & n & w & f & r & m \end{pmatrix}$$

Pomocí permutací $A_1$, $A_2$ a $A_3$ vytváříme postupně součiny:

| | | |
|---|---|---|
| $C^{-1}A_1C$ | $PC^{-1}P^{-1}A_1PCP^{-1}$ | $P^2C^{-1}P^{-2}A_1P^2CP^{-2}$ |
| $PC^{-1}P^{-1}A_2PCP^{-1}$ | $P^2C^{-1}P^{-2}A_2P^2CP^{-2}$ | $P^3C^{-1}P^{-3}A_2P^3CP^{-3}$ |
| $P^2C^{-1}P^{-2}A_3P^2CP^{-2}$ | $P^3C^{-1}P^{-3}A_3P^3CP^{-3}$ | $P^4C^{-1}P^{-4}A_3P^4CP^{-4}$ |

…

V určitý okamžik narazíme na takovou trojici permutací, že se některé transpozice začnou opakovat. V našem příkladě to nastane hned při druhém pokusu.

$PC^{-1}P^{-1}A_1PCP^{-1}$ = (aw)(br)(cd)(ei)(fz)(ql)(uj)(xg)(sn)(ht)(ov)(mk)(yp)

$P^2C^{-1}P^{-2}A_2P^2CP^{-2}$ = (ni)(ax)(wt)(bq)(rv)(gz)(my)(fe)(sl)(pj)(ud)(ck)(oh)

$P^3C^{-1}P^{-3}A_3P^3CP^{-3}$ = (wh)(vr)(ay)(qe)(fz)(lk)(ui)(pn)(dj)(ot)(cs)(bm)(xg)

Vidíme, že opakující se transpozice jsou (fz), (xg) a (rv).

Při vyhledávání opakujících se transpozic Rejewski využíval pomůcku připomínající *rošt*. Z permutací $C$, $PCP^{-1}$, $P^2CP^{-2}$, …, $P^{25}CP^{-25}$ vybral pouze druhé řádky a napsal je na tvrdou lepenku s otvory, tak jak to ukazuje následující obrázek.

Obr. 6: Schéma roštu


Pod takto vytvořenou síťku pokládal čtvrtku papíru s vypsanými permutacemi $A_1$, $A_2$ a $A_3$ v základním tvaru (viz Dodatek: Kapitola o permutacích). Mezi horním a dolním řádkem každé permutace vynechal dostatek místa.

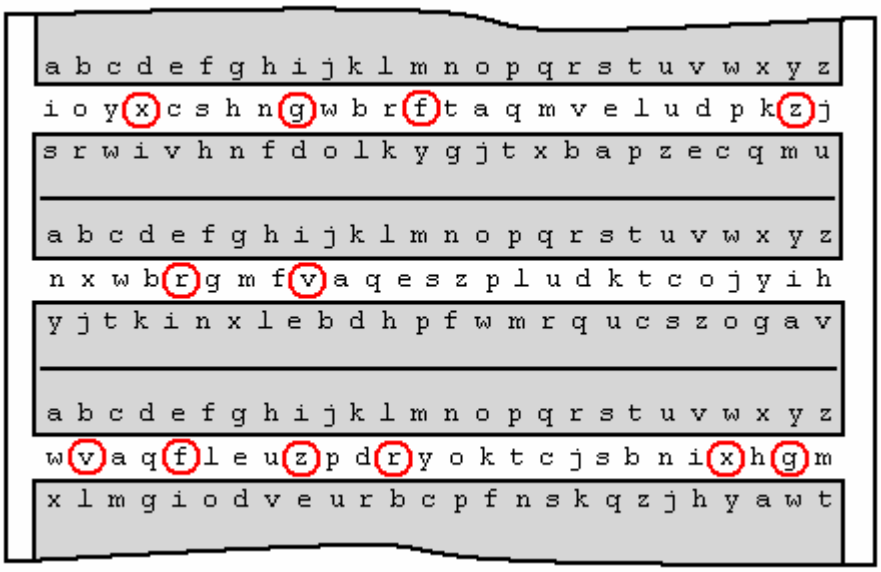
Obr. 7: Permutace $A_1$, $A_2$ a $A_3$

| | |
|---|---|
| | a b c d e f g h i j k l m n o p q r s t u v w x y z |
| $A_1$ | |
| | s r w i v h n f d o l k y g j t x b a p z e c q m u |
| | a b c d e f g h i j k l m n o p q r s t u v w x y z |
| $A_2$ | |
| | y j t k i n x l e b d h p f w m r q u c s z o g a v |
| | a b c d e f g h i j k l m n o p q r s t u v w x y z |
| $A_3$ | |
| | x l m g i o d v e u r b c p f n s k q z j h y a w t |

Pak postupně posouval síťku nad touto čtvrtkou a zároveň kontroloval, jaké transpozice vznikají mezi horními a dolními řádky permutací $A_1$, $A_2$ a $A_3$. Pokud narazil na transpozice, které se opakují, posun zastavil.

V našem případě nalezneme opakující se transpozice `(fz)`, `(xg)` a `(rv)`.

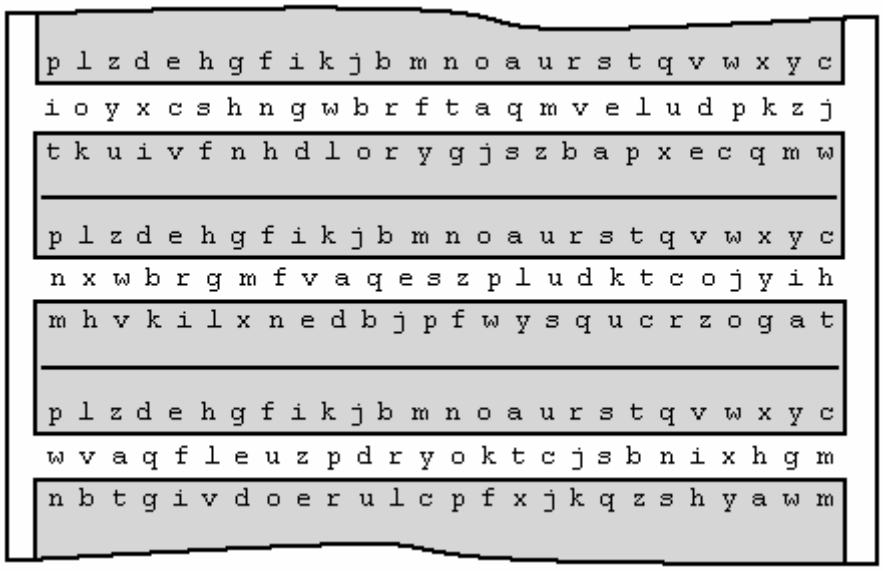
Obr. 8: Opakující se transpozice




Transpozice, které se opakují jsou ty, na které permutace $S$ nepůsobí. Takové transpozice jsou také součástí permutace $U$.

Zbývá vhodně popřehazovat současně horní i dolní písmena v každé z permutací $A_1$, $A_2$ a $A_3$, aby všechny transpozice, které vzniknou mezi horními a dolními řádky permutací $A_1$, $A_2$ a $A_3$ byly stejné.

Obr. 9: Výsledné uspořádání písmen




Transpozice, které vznikly mezi horními a dolními řádky permutací $A_1$, $A_2$ a $A_3$, jsou nyní ve všech třech případech stejné:

(ab)(cd)(eq)(fz)(gx)(ht)(il)(jp)(ku)(my)(ns)(ow)(rv)

Písmena, která byla v permutacích $A_1$, $A_2$ a $A_3$ přehozena tvoří právě permutaci $S$:

$S$ = (ap) (bl) (cz) (fh) (jk) (qu)

Tyto dvojice písmen zároveň udávají propojení v propojovací desce. Zbývající písmena propojena nejsou.

Použitím metody roštu jsme nalezli propojení v propojovací desce a zároveň správné počáteční nastavení pravého rotoru. Pro určení počátečních nastavení zbývajících dvou rotorů musíme vyzkoušet všech 26x26 = 676 možných nastavení levého a prostředního rotoru. Pro každé nastavení rotorů vyťukáme na přístroji Enigma některý z indikátorů zachycených šifrových zpráv, dokud nenarazíme na dvě stejné trojice písmen. Tyto trojice písmen známe, díky metodě pro zjišťování klíčů zpráv (viz kapitola 3.2.1. Odhalování klíčů zpráv).

Popsaná metoda je velice technicky a časově náročná. Zjišťování propojení na propojovací desce (neboli permutace *S*) touto metodou je značně pracné a vyžaduje notnou dávku trpělivosti a soustředěnosti. Pokoušela jsem se pomocí *roštu* zjistit permutaci *S* také v příkladě řešeném v kapitole 3.2.1. Odhalování klíčů zpráv a zmiňovaném v kapitole 3.2.2. Cyklometr. Musím však přiznat, že správné řešení jsem nenalezla, ačkoliv jsem tomu věnovala spoustu času. Pro zvídavé čtenáře přikládam model roštu pro tento příklad (viz Příloha: Model roštu). Všechny další potřebné informace k řešení tohoto příkladu lze pak nalézt v kapitolách 3.1. Odhalování vnitřního propojení (vnitřní propojení rotorů a reflektoru) a 3.2.1. Odhalování klíčů zpráv (permutace $A_1$, $A_2$ a $A_3$).

### 3.2.4. Rózyckého metoda hodin

Rózyckého metoda hodin sloužící k určení rotoru umístěného na pozici vpravo na hřídeli přístroje je založena na znalosti tzv. *indexu koincidence*.

*Index koincidence* je pravděpodobnost, že se u dvou textů v daném jazyce vyskytnou na stejném místě stejná písmena. *Index koincidence* daného jazyka lze zjistit empiricky, například pro němčinu je 0,0824 a pro náhodný text je 0,0385 = 1/26.

V praxi to tedy znamená, že ve dvou jakýchkoliv německých větách délky 100 písmen se vyskytne v průměru 8 stejných písmen na stejném místě. Tato vlastnost zůstane zachována, pokud obě věty zašifrujeme stejným klíčem. Naopak dva náhodné texty (tj. texty ve kterých je frekvence všech písmen více méně stejná) mají přibližně 4 stejná písmena na stejném místě. Této vlastnosti se využívá v postupu určení pravého válce.

Při dostatečném množství zachyceného šifrového materiálu obvykle najdeme několik dvojic zpráv takových, že v každé dvojici jsou první dvě písmena klíče stejné a liší se pouze v třetím písmenu. Nyní obě takové zprávy napíšeme pod sebe tak, aby písmena zašifrovaná stejným nastavením rotorů byla pod sebou. Ukažme si to na příkladě.

Máme dvě zprávy, jednu zašifrovanou klíčem `aaa` a druhou klíčem `aae`.

1. zpráva: `jescx fraud piswb uzyew`
2. zpráva: `rghzx hweio qaser lkmwa`

První písmeno první zprávy je zašifrováno pomocí rotorů v pozici `aaa`, druhé písmeno pomocí rotorů v pozici `aab`, atd. a páté písmeno je zašifrováno pomocí rotorů v pozici `aae`. Tedy se stejnou pozicí rotorů jako první písmeno druhé zprávy. Tyto dvě zprávy napíšeme pod sebe v následujícím pořadí písmen:

1. zpráva: `jescx fraud piqwb uzyew`
2. zpráva: `rghzy xweio qaser lkmwa`

Máme tedy dvě zprávy napsány pod sebou tak, že písmena zašifrovaná stejným nastavením rotorů jsou pod sebou.

Dosud jsme však neuvažovali pootočení prostředního rotoru. Mohou nastat dvě možnosti:

- Zářez k pootočení prostředního rotoru se na pravém rotoru nachází mezi písmeny `a` až `d`. Předpokládejme například, že zářez na pravém rotoru je na pozici `c`. Následující tabulka ukazuje pozice rotorů pro šifrování každého písmene obou zpráv.

| | **aaa** | **aab** | **aac** | **abd** | **abe** | **abf** | **abg** | **abh** | **abi** | **abj** | **abk** | **abl** | **abm** | **abn** | **abo** | **abp** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1. zpráva** | j | e | s | c | x | f | r | a | u | d | p | i | s | w | b | u |
| | | | | | **aae** | **aaf** | **aag** | **aah** | **aai** | **aaj** | **aak** | **aal** | **aam** | **aan** | **aao** | **aap** |
| **2. zpráva** | | | | | r | g | h | z | x | h | w | e | i | o | q | a |

  V tomto případě bude index koincidence těchto dvou zpráv přibližně odpovídat indexu koincidence náhodných textů, neboť obě zprávy jsou šifrovány jiným pootočením rotorů.

- Zářez k pootočení prostředního rotoru se na pravém rotoru nachází mezi písmeny `e` až `z`. Předpokládejme například, že zářez na pravém rotoru je na pozici `f`. Následující tabulka ukazuje pozice rotorů pro šifrování každého písmene obou zpráv.

| | **aaa** | **aab** | **aac** | **aad** | **aae** | **aaf** | **abg** | **abh** | **abi** | **abj** | **abk** | **abl** | **abm** | **abn** | **abo** | **abp** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1. zpráva** | j | e | s | c | x | f | r | a | u | d | p | i | s | w | b | u |
| | | | | | **aae** | **aaf** | **abg** | **abh** | **abi** | **abj** | **abk** | **abl** | **abm** | **abn** | **abo** | **abp** |
| **2. zpráva** | | | | | r | g | h | z | x | h | w | e | i | o | q | a |

  V tomto případě bude index koincidence těchto dvou zpráv stejný jako index koincidence německého jazyka, neboť obě zprávy jsou šifrovány stejným pootočením rotorů.

Takto postupujeme pro další dvojice zpráv, jež mají první dvě písmena klíče stejná a liší se pouze v třetím písmenu. Nakonec získáme správnou polohu zářezu na pravém rotoru. Tyto polohy zářezů jsou jiné pro každý šifrovací rotor a jsou známé (viz kapitola 3.1. Odhalování vnitřního propojení), snadno tedy zjistíme, který rotor se nachází na pozici vpravo.

### 3.2.5. Určování pořadí rotorů

Práce na luštění německých depeší v polském Biurze Szyfrow postupovalo úspěšně. Metody odhalování všech složek denního klíče byly částečně zmechanizovány tak, aby získané šifrované zprávy bylo možno dešifrovat v nejkratším čase. Mohlo by se zdát, že prapor vítězství se naklonil na stranu Poláků, avšak 15. září 1938 Němci, snad z opatrnosti, snad z prozíravosti, změnili postup šifrování.

Do té doby bylo *základní nastavení* (tj. tří písmenný kód udávající orientaci rotorů) součástí denního klíče, nyní toto *základní nastavení* bylo jiné pro každou zprávu. Postup při šifrování každé zprávy byl tedy následující:

- Operátor nastavil Enigmu podle příslušného dennního klíče (již bez *základního nastavení*).
- Pak náhodně zvolil tři písmena jako *základní nastavení* pro šifrování dané zprávy (např. **S-K-R**) a nastavil všechny tři rotory podle této volby.
- Následně znovu zvolil náhodně tři písmena jako klíč dané zprávy (např. **W-T-C**). Zvolená písmena zašifroval dvakrát po sobě. Sekvenci písmen **WTCWTC** tedy zašifroval například jako **KFDLSF**.
- Nakonec nastavil rotory podle zvoleného klíče zprávy tak, aby písmena **W T C** byla vidět v okénkách v krytu rotorů. Nyní byl přístroj připraven pro šifrování vlastní zprávy.

Jak tedy odesílaná zpráva vypadala? Po zašifrování vlastní zprávy umístil operátor na začátek zvolený tří písmenný kód **SKR** v nešifrované podobě, tj. jako otevřený text. Bezprostředně za něj umístil dvakrát zašitrovaný klíč zprávy **KFDLSF**. Tedy začátek zprávy byl tvořen devíti písmeny **SKR KFD LSF**.

Nový způsob šifrování značně ochromil činnost polských kryptoanalytiků. Protože *základní nastavení* již nebylo součástí denního klíče, nebylo možné vytvořit charakteristiky daného dne. Tedy všechny metody získávání jednotlivých složek denního klíče založené na charakteristikách dne (tj. metoda odhalování klíčů zpráv, cyklometr i rošt) byly již dále nepoužitelné. Bylo potřeba najít nové metody zjišťování denního klíče. Než si však nalezené metody uvedeme popišme si nejdříve postup určování *pořadí rotorů*.

Pokud se během dne podařilo zachytit dostatečné množství šifrových zpráv, bylo možné několika jednoduchými postupy zjistit pořadí rotorů na hřídeli přístroje. Ukážeme si to na několika příkladech, stejně jako Rejewski v práci [3].

*Příklad 1*. Předpokládejme, že během daného dne jsme zachytili dvě zprávy s následujícími začátky:

```
tkp  anv ckb
tlr  vts jqm
```

Vidíme tedy, že třetí písmeno klíče první zprávy je zašifrováno jako písmeno `v`, stejně jako první písmeno klíče druhé zprávy. Kdyby došlo k pootočení prostředního rotoru někde mezi pozicemi `p` a `r` pravého rotoru, pak by zakroužkovaná písmena byla šifrována stejným klíčem. Proto by také muselo být stejné šesté písmeno zašifrovaného klíče první zprávy (písmeno `b`) se čtvrtým písmenem zašifrovaného klíče zprávy (písmeno `j`). Ta však nejsou, tedy k pootočení prostředního rotoru nedošlo. Z čehož můžeme usuzovat, že rotor I není na pozici vpravo, protože víme, že rotor I způsobuje pootočení následujícího pomalejšího rotoru právě mezi pozicemi `q` a `r` (viz kapitola 3.1. Vnitřní propojení).

*Příklad 2*. Předpokládejme, že během daného dne jsme zachytili dvě zprávy s následujícími začátky:

```
tkp  anv ckb
tlr  vts bqm
```

Tento příklad je téměř stejný jako první příklad, ale nyní je šesté písmeno zašifrovaného klíče první zprávy stejné jako čtvrté písmeno zašifrovaného klíče druhé zprávy (písmeno `b`). V tomto případě je velice pravděpodobné, že mezi pozicemi `p` a `r` pravého rotoru došlo k pootočení prostředního rotoru. Lze se tedy domnívat, že na pozici vpravo se nachází právě rotor I.

*Příklad 3*. Předpokládejme, že během daného dne jsme zachytili dvě zprávy s následujícími začátky:

```
tkp  anv ckb
tkr  vts bqm
```

Vidíme, že zakroužkovaná písmena jsou v první i druhé zprávě stejná (písmena `v` a `b`), tedy v tomto případě je málo pravděpodobné, že došlo k pootočení prostředního rotoru mezi pozicemi `p` a `r` pravého rotoru. Z čehož lze usuzovat, že na pozici vpravo na hřídeli přístroje není umístěn rotor I.

*Příklad 4*. Předpokládejme, že během daného dne jsme zachytili dvě zprávy s následujícími začátky:

```
tjg  cms pkr
ukg  cwt plj
```

V tomto případě jsou první a čtvrtá písmena obou zpráv stejná (písmena `c` a `p`). Je tedy pravděpodobné, že došlo k pootočení levého rotoru na začátku šifrování klíče první zprávy, tak aby klíče obou zpráv byly šifrovány stejným natočením rotorů. Proto můžeme předpokládat, že na pozici prostředního rotoru je umístěn rotor IV, neboť tento otáčí levým pomalejším rotorem v pozici mezi `k` a `j`.

Podobným způsobem lze určit pozice všech rotorů pro obdobné případy. Pro dostatečné množství zachycených šifrových zpráv během dne bylo tedy možné určit *pořadí rotorů* na hřídeli přístroje pro daný den. Tato část denního klíče nebyla však jediná, kterou bylo třeba určit. Bylo nutné najít nové metody odhalování propojení v propojovací desce.

### 3.2.6. Rejewského bomby

Díky novému způsobu šifrování zpráv známe *základní nastavení* rotorů pro každou zprávu. Protože však neznáme *pozici prstenců* na jednotlivých rotorech, neznáme ani skutečnou pozici rotorů. Pokud se nám podaří tuto skutečnou pozici rotorů najít, snadno pak zjistíme i *pozici prstenců* na jednotlivých rotorech.

Jak již bylo řečeno, metody založené na využití *denních charakteristik* byly dále nepoužitelné. Některé zákonitosti však zůstaly. Pokud máme například klíč zprávy po zašifrování ve tvaru `pst pwa`, vidíme ,že první a čtvrté písmeno je stejné (písmeno `p`). Což tedy znamená, že v součinu permutací $A_1A_4$ pro danou zprávu se objeví jednopísmenný cykl `(p)`, který se nazývá *pevný bod* permutace $A_1A_4$. Obdobně lze také nalézt pervné body permutací $A_2A_5$ nebo $A_3A_6$.

Ukažme si na příkladu jak Rejewského bomby fungovaly. Předpokládejme dále, že při šifrování klíčů zpráv nedošlo k pootočení prostředního rotoru (tj. otáčel se pouze pravý rotor). Z každé zachycené šifrové zprávy zaznamenáme prvních 9 písmen, které charakterizují klíč dané zprávy. Předpokládejme, že během určitého dne získáme zprávy s následujícími počátky:

| | | | | | |
|---|---|---|---|---|---|
| ktl | woc | drb | | gra | fdr | ynd |
| svw | kkm | iys | | kdo | otw | yzw |
| jot | iwa | bwn | | kjc | fsw | nse |
| edc | dsp | ljc | | sgf | tey | asr |
| gkd | wav | wba | | agh | npf | rlf |
| bwx | tca | toc | | jbr | wlt | soq |

Podívejme se podrobněji na zakroužkované písmeno `w` ve zprávě s počátkem `jot iwa bwn`. Všimněme si, že písmeno `w` tvoří v tomto případě *pevný bod*.

Pokud při základním nastavení rotorů `jot` dvakrát zašifrujeme nějaký klíč zprávy (např `xyz`), získáme postupně písmena `iwa bwn`. To tedy znamená, že v pozici `jou` písmeno `y` indukovalo písmeno `w` a v pozici `jox` stejné písmeno `y` indukovalo opět písmeno `w`. Z *Pravidla vzájemnosti* (viz kapitola 3.2.1. Odhalování klíčů zpráv) plyne, že v pozici `jou` písmeno `w` indukovalo `y` a v pozici `jox` písmeno `w` indukovalo opět `y`.

Předpokládejme, že písmeno `w` nebylo změněno permutací *S* (tj. propojením na propojovací desce). Nyní budeme postupně v každé poloze rotorů tisknout klávesu s písmenem `w`. Pozorujeme, zda se při *n*-tém a (*n*+3)-tím stisknutí klávesy `w` zobrazí stejné písmeno. Pokud tato situace nastane, snadno se již přesvědčíme, že daná pozice rotorů je správná.

Uvažujeme-li pouze tento jeden počátek zprávy (tj. prvních 9 písmen) s pevným bodem `w`, nalezneme příliš velký počet zdánlivě správných možností poloh rotorů. Podívjeme se tedy na více počátků zpráv s pevným bodem `w`. Vypišme si všechny takového počátky zpráv:

| | | |
|---|---|---|
| jot | iwa | bwn |
| gkd | wav | wba |
| kdo | otw | yzw |

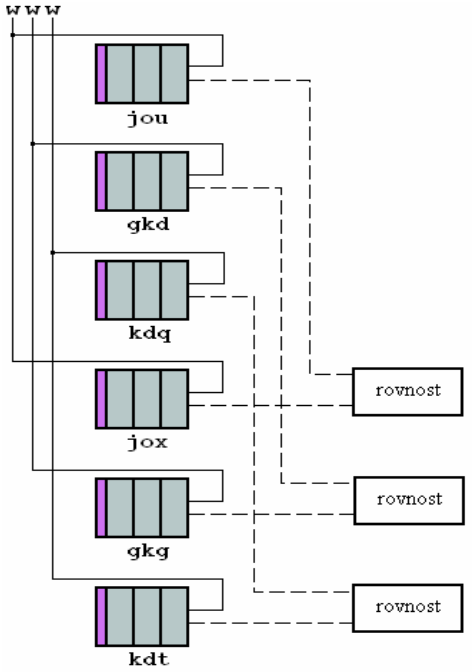
Popišme si nyní, jakým způsobem bychom mohli posupovat dále. Předpokládejme, že bychom měli šest přístrojů Enigma, každý obsluhován jedním operátorem. Operátoři *A* a *B* by měli rotory svých přístojů nastaveny na pozice `jou` a `jox`, operátoři *C* a *D* by měli rotory nastaveny na pozice `gkd` a `gkg` a operátoři *E* a *F* by měli rotory nastaveny na pozice `kdq` a `kdt`. Všichni operátoři zároveň by opakovaně tiskli klávesu `w`, přičemž operátoři *A*, *C* a *E* by po každém stisknutí klávesy hlásili, které písmenko se jim zobrazilo. Naopak operátor *B* by pozoroval, zda na svém přístroji nevidí písmeno diktované operátorem *A*, operátor *D* by pozoroval, zda nevidí písmeno diktované operátorem *C* a operátor *F* by pozoroval, zda nevidí stejné písmeno jako operátor *E*.

Kdyby nastala situace, že by operátoři *A* a *B*, *C* a *D*, *E* a *F* po páru uviděli na svých přístrojích stejná písmena (tj *A* a *B* by viděli oba stejné písmeno, *C* a *D* by viděli oba stejné písmeno, *E* a *F* by viděli oba stejné písmeno, avšak viděná písmena by mohla být navzájem různá), celý proces by se zastavil a bylo by velice pravděpodobné, že jsme našli správnou skutečnou pozici rotorů.

Popsali jsme si tedy princip fungování Rejewského bomby. Samozřejmě, že takto popsaný postup by byl v praxi zdlouhavý a nespolehlivý (kdokoliv se mohl snadno přehlédnout). Rejewski proto těchto šest operátorů a šest přístrojů nahradil jedním velkým přístrojem, který byl schopen projít všechny možnosti rychleji a důkladněji a zastavit se v příslušný okamžik. Takový přístroj byl zkonstruován již v listopadu roku 1938 a nazván bomba.

Bomba se skládala ze tří párů přístrojů Enigma. První pár přístrojů byl nastaven do polohy `jou` a `jox`, druhý pár přístrojů byl nastaven do polohy `gkd` a `gkg` a třetí pár přístrojů byl nastaven do polohy `kdq` a `kdt`. Pak se současně na všech přístrojích tiskla opakovaně klávesa `w`. Pokud přístroj narazil na příznivý výsledek (viz výše), pak se zastavil v určité pozici, jež by mohla být hledaná skutečná pozice rotorů.

Obr.10: Schéma principu Rejewského bomby




Rejewského bomba vyzkoušela všechny možnosti nastavení rotorů zhruba během dvou hodin. Pro rychlejší nalezení správné skutečné pozice rotorů bylo sestrojeno šest bomb, pro každé pořadí rotorů jedna.

Dokud byly používány pouze 3 rotory (tj. 6 možných pořadí rotorů na hřídeli přístroje), pak byly bomby velice rychlé. Později byly přidány další dva rotory, tedy počet možných pořadí rotorů na hřídeli stoupl na 60. Použití bomb se pak stalo nepraktické, protože vyžadovalo mnoho času.

Další slabou stránkou této metody byl předpoklad, že permutace *S* (tj. propojení v propojovací desce) nezmění zvolený pevný bod (v našem příkladě písmeno `w`). Protože však docházelo ke zvyšování počtu kabelů k propojení na propojovací desce (až na deset), pravděpodobnost, že se zvolený pevný bod nezmění klesala. Bylo tedy nutné nalézt novou metodu, která by nezáležela na počtu propojení v propojovací desce.

### 3.2.7. Zygalského plachty

Tato nová metoda byla také založena na existenci *pevných bodů* permutací. Připomeňme, že cyklometr byl založen na faktu, že permutace $S$ (tj. propojení na propojovací desce) nemění počet ani velikost cyklů permutací $A_1A_4$, $A_2A_5$ a $A_3A_6$ (zaměňuje pouze některá písmena). Obdobně permutace $S$ nemá vliv na přítomnost pevných bodů v jednotlivých permutací $A_1A_4$, $A_2A_5$ a $A_3A_6$.

Úvahy polských kryptoanalytiků byly následující. Pokud pro $n$-tou pozici rotorů vyťukáme na klávesnici postupně celou abecedu od `a` do `z`, získáme určitou permutaci abecedy $P_1$. Pokud znovu pro $(n+3)$-tí pozici rotorů vyťukáme celou abecedu, pak obdržíme jinou permutaci abecedy $P_4$.

Pokud obě permutace $P_1$ a $P_4$ napíšeme pod sebe, může se stát, že dvě písmena (nebo i více) se vyskytnou na stejném místě. Vidíme tedy, že součin permutací $P_1P_4$ obsahuje dva (nebo i více) pevné body. Pak řekneme, že pozice rotorů odpovídající permutaci $P_1$ obsahuje pevný bod. Takto bychom mohli projít všechny pozice rotorů přístoje Enigma a zařadit je do jedné ze dvou tříd. Třída I je tvořena pozicemi rotorů obsahujících pevný bod a třída II je tvořena pozicemi rotorů, které neobsahují pevný bod. Jak píše Rejewski v práci [3] poměr velikostí třídy I k velikosti třídy II je přibližně 2:3.

Popišme si postup používání této metody na příkladě. Předpokládejme dále, že při šifrování klíčů zpráv nedošlo k pootočení prostředního rotoru (tj. otáčel se pouze pravý rotor). Uvažujme nyní, že během určitého dne získáme zprávy s následujícími počátky:

| | | | | | |
|---|---|---|---|---|---|
| ktl | woc | drb | | gra | fdr | ynd |
| svw | kkm | iys | | kdo | otw | yzw |
| jot | iwa | bwn | | kjc | fsw | nse |
| edc | dsp | ljc | | sgf | tey | asr |
| gkd | wav | wba | | agh | npf | rlf |
| bwx | tca | toc | | jbr | wlt | soq |

Vidíme, že pozice rotorů `jou`, `gkd`, `bwx`, `kdq`, `kjd` a `ahj` patří do třídy I, protože obsahují pevný bod (zakroužkovaná písmena).

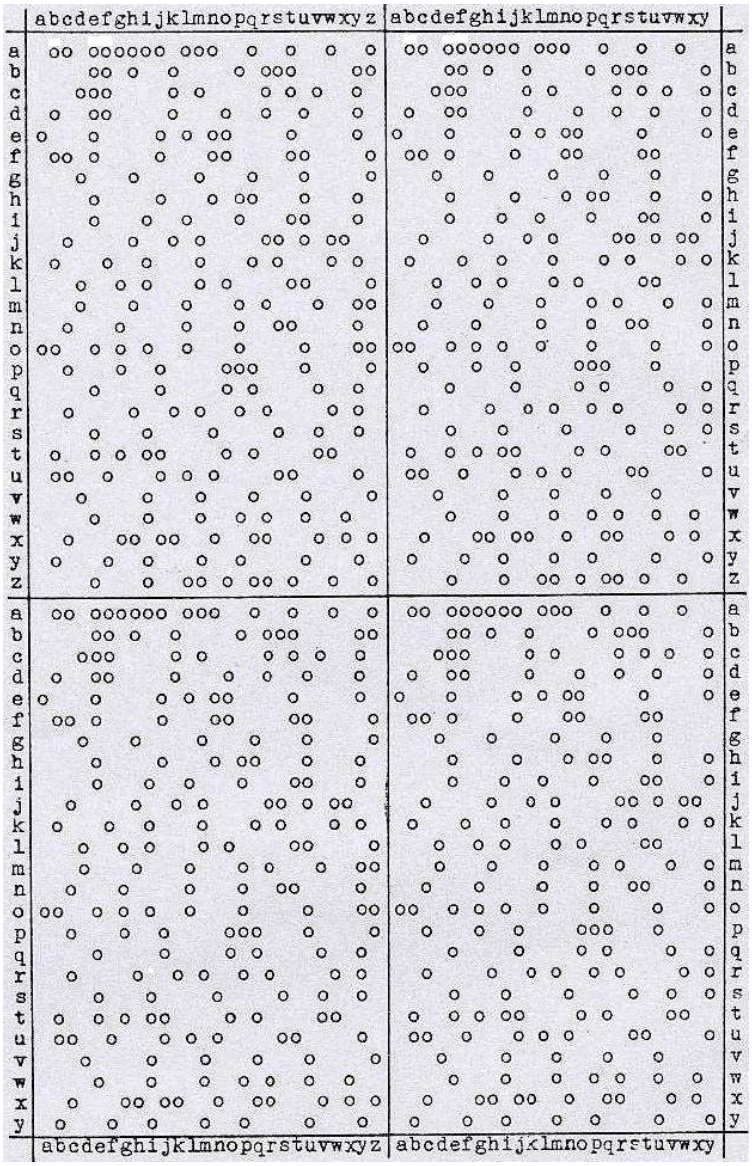
Obdobně jako v kapitole 3.2.2. Cyklometr bychom mohli sestavit *katalog pevných bodů*, tj postupně pro každou pozici rotorů zaznamenat, zda má nebo nemá pevný bod. Protože neznáme pozici prstenců na jednotlivých rotorech, neznáme ani skutečnou pozici rotorů. Díky novému způsobu šifrování, však známe relativní natočení rotorů vůči sobě (první tři písmena každé zprávy). Mohli bychom tedy v katalogu pevných bodů hledat takových šest pozic rotorů, které mají *pevný bod* a jejich vzájemná poloha odpovídá vzájemnému natočení rotorů v pozicích `jou`, `gkd`, `bwx`, `kdq`, `kjd` a `ahj`. Snadno bychom již ověřili, že nalezená skutečná poloha rotorů je správná. Nakonec bychom jednoduše odvodili i pozici prstenců na jednotlivých rotorech.

Tento postup vyhledávání v katalogu byl velice náročný, proto bylo vhodné najít jiný způsob hledání. Řešení jež nalezl Zygalski bylo nazváno *plachty*.

Předpokládejme, že máme tři rotory v pořadí γ, β a α zleva doprava (tj. rotor α je umístěn vpravo, rotor β je uprostřed a rotor γ je vlevo). Pak pro každou pozici rotoru α byl vytvořen speciální list papíru tzv. *plachta*. Každá plachta obsahovala 51x51 čtverečků. Po obvodu takto vzniklého čtverce byla umístěna písmena od `a` do `z` a od `a` do `y`, přičemž svislá osa

představovala pozice rotoru β a vodorovná osa pozice rotoru γ. Tedy každý čtvereček charakterizoval jednu určitou polohu všech tří rotorů. Čtvereček, který odpovídá pozici rotorů obsahující pevný bod je opatřen otvorem, jak můžeme vidět na obrázku.

Obr. 11: Zygalského plachta pro jednu pozici některého rotoru



Nyní si popišme postup hledání skutečné pozice rotorů. Nejprve vybereme plachtu, která přísluší např. pozici `a` rotoru α. Pak se zaměříme na relativní natočení rotorů dané pozicemi `jou`, `gkd`, `bwx`, `kdq`, `kjd` a `ahj`. Písmeno `g` je umístěno v abecedě 23 pozic za písmenem `j` (porovnáváme pozice `jou` a `gkd`). Proto vybereme plachtu příslušící pozici `x` rotoru α. Položíme tuto plachtu na první vybranou následujícím způsobem: protože písmeno `k` je umístěno 22 pozic za písmenem `o`, posuneme druhou plachtu o 22 pozic dolů a protože písmeno `d` je umístěno 9 pozic za písmenem `u`, posuneme druhou plachtu o 9 pozic doprava.

Vybereme třetí plachtu příslušící pozici `s` rotoru α, protože písmeno `b` je umístěno 18 pozic za písmenem `j` (porovnáváme pozice `jou` a `bwx`). Tuto třetí plachtu umístíme na obě vůči sobě posunuté plachty. Protože písmeno `w` je umístěno 8 pozic za písmenem `o`, posuneme třetí plachtu o 8 pozic dolů a protože písmeno `x` je umístěno 3 pozice za písmenem `u`, posuneme

třetí plachtu o 3 pozice doprava.Takto postupujeme dále, až na sebe umísíme všech šest archů papíru odpovídající nalezeným šesti pozicím rotorů s pevným bodem.

Pokud popsaným způsobem umístíme všechny plachty vidíme, že pravá dolní část prvního listu papíru je zcela překryta ostatními listy. To je také důvod, proč je každá plachta tvořena 51x51 čtverečky, když by stačilo pouze 26x26 čtverečků, které reprezentují všechny pozice rotoru β a rotoru γ.

Zbývá již jen najít takovou pozici, kde jsou otvory ve všech šesti plachtách. Předpokládejme, že tato pozice je na prvním vybraném archu `b` pro rotor β a `c` pro rotor γ. Nyní víme, že skutečná pozice rotorů je `abc` a základní nastavení je `jou`. Není již obtížné zjistit také pozice prstenců pomocí rozdílů mezi skutečným nastavením rotorů a základním nastavením.

# 4. Britská šifrovací kancelář

Po několik let se britští a francouzští kryptoanalytici domnívali, že Enigma je neprolomitelná šifra. Poláci jim však dokázali opak. Začínající válka v Polsku sice přerušila práce polských kryptoanalytiků, ukázali však, že Enigma není neporazitelný soupeř.

V Británii funkci tajné kryptoanalytické organizace plnila Kancelář č. 40, jež Rejewského objevy přesvědčily, že by měla ve svých řadách zaměstnat také matematické mozky. Vědci byli přijímáni především na základě známostí.

Noví pracovníci již však nemířili do Kanceláře č. 40 v Londýně, ale do Bletchley Park v Buckinghamshire, kde vznikla nová organizace postupně přebírající úlohu Kanceláře č. 40 tzv. Government Code and Cypher School (GC&CS). Bletchley Park poskytoval dostatek prostoru pro velké množství kryptoanalytiků potřebných pro luštění zachycených německých depeší.

Ve středu Bletchley Parku stálo rozlehlé venkovské sídlo z viktoriánských dob postavené v pseudogotickém stylu, zámeček s knihovnou, jídelnou a zdobeným tanečním sálem. Postupně se vystavělo velké množství nových budov, které se staly sídlem různých kryptoanalytických aktivit. Původně bylo v Bletchley Parku pouze dvě stě zaměstnanců, za pět let však zámeček a provizorní stavby hostily sedm tisíc mužů a žen.

## *4.1. Alan Turing*

Jedním z nejlepších kryptoanalytiků v Bletchley Parku byl bezesporu Alan Turing.

Alan Turing se narodil 23. června 1912 v Londýně. Jeho otec Julius Turing byl úředníkem v Jižní Indii. Alan Turing žil v Londýně a roku 1926 se stal žákem Sherborne School v Dorsetu, kde se zabýval především přírodními vědami. Roku 1931 byl Turing přijat na King's College v Cambridgi. 4. září 1939 se Alan Turing stal kryptoanalytikem v GC&CS v Bletchley Parku.

Turing se snažil vylepšit Rejewského bomby, aby je bylo možno využívat intenzivněji. Rejewského bomby byly založeny na zkoumání jednoho písmene (viz kapitola 3.2.6 Rejewského bomby). Zvýšením používaných kabelů v propojovací desce však pravděpodobnost, že testované písmeno je správné (tj. není změněno v propojovací desce) rapidně klesla. Turingova myšlenka byla testovat všechna písmena zároveň, což v podstatě odpovídalo principu Zygalského plachty (viz kapitola 3.2.7. Zygalského plachty).

Tato Turingova verze polské bomby nebyla nikdy realizována. Všechny metody používané polskými kryptoanalytiky využívaly dvojí šifrování klíče zprávy. Britští kryptoanalytici se snažili najít metodu, která by nebyla založena na tomto faktu, protože se obávali, že by Němci mohli od dvojího šifrování klíčů zpráv upustit. Jejich obavy se naplnily začátkem května roku 1940, kdy Němci zrušili dvojí šifrování klíčů zpráv.

Z tohoto důvodu Turing hledal novou metodu hledání denního klíče, jež by byla účinná i po nechtěné změně způsobu šifrování.

## 4.2. Turingovy bomby

Turing se rozhodl prostudovat velké množství starých rozšifrovaných zpráv. Domníval se, že ze znalosti starších depeší by dokázal někdy předpovědět část obsahu některé šifrové zprávy. Zjistil, že Němci často používají opakující se fráze. Například každý den ve stejný čas Němci posílali informace o počasí vždy ve stejné striktně dané formě. Britští kryptoanalytici se snažili uhodnout použitou frázi a pak ji porovnávali se zachycenou šifrovou zprávou. Takovou část otevřeného textu, kterou lze propojit s šifrovým textem nazývali *tahák*.

Turing si uvědomil, že pomocí takových taháků by mohl zjistit denní klíč. Taháky mohou určovat části *Abeced* (definice viz Dodatek: Kapitola o permutacích). V určitém složení *Abeced* pak lze nalézt pevné body a ty pak využít ke zjišťování správného nastavení rotorů, např. pomocí Rejewského bomby. Celý postup si vysvětleme na příkladu uvedeném v [1].

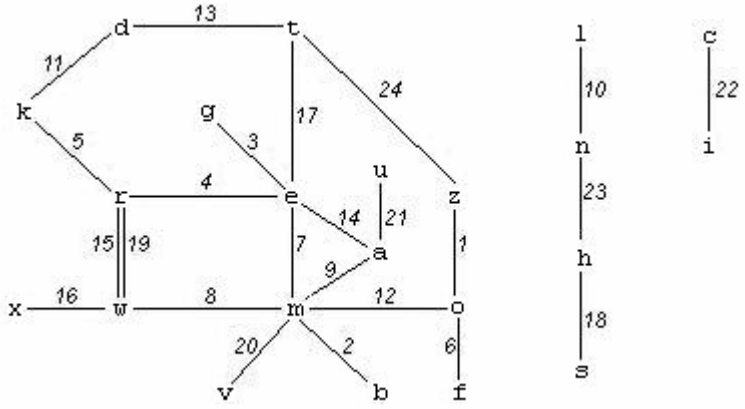
Předpokládejme, že máme k dispozici následující šifrový text: `ovrlj bzmge rfewm lkmta wxtsw vuinz gyoly`... a tahák: `oberkommandoderwehrmacht`.

Nyní potřebujeme tento tahák přiřadit správnému úseku šifrového textu. Pozic taháku v textu je mnoho, ale spoustu z nich lze vyloučit využitím *Pravidla výlučnosti* (viz kapitola 3.2.1. Odhalování klíčů zpráv). Například víme, že tahák nemůže být umístěn hned na začátek šifrového textu, protože pak by se šifrové písmeno `o` zobrazilo na otevřené písmeno `o`, což nelze. Můžeme najít tak správné umístění taháku:

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

Čísly 1, 2, …, 24 označíme postupně pozice pravého rotoru. Označme $P_i$ *Abecedu* příslušící *i*-té pozici pravého rotoru. Pokud by neexistovalo propojení na propojovací desce (permutace *S*), pak transpozice (`o z`) by byla částí *Abecedy* $P_1$, transpozice (`b m`) by byla částí *Abecedy* $P_2$, atd. Tyto informace můžeme zakreslit do grafu.

Obr. 12: Graf všech transpozic




Ve skutečnosti uvažované traspozice budou jiné působením propojovací desky (permutace *S*). Místo písmena `o` pak budeme mít písmeno *S*(`o`), místo písmena `z` písmeno *S*(`z`), atd.

Z uvedeného grafu vidíme, že platí rovnost

$$S(\mathtt{r})P_{15}P_{19} = S(\mathtt{r}).$$

Získali jsme tedy pevný bod složením dvou *Abeced*. Potřebovali bychom ale více takových pevných bodů, abychom mohli použít Zygalského plachty nebo Rejewského bomby (upravené pro testování více písmen zároveň) pro zjištění správného nastavení rotorů. Nemusíme se však omezovat pouze na složení dvou *Abeced*, můžeme hledat pevné body také ve složení tří a více *Abeced*. Což tedy znamená, že nová bomba nebude obsahovat pouze dvojice spřažených přístrojů Enigma, ale celé řetězce příslušného počtu přístrojů.

Zvolme písmeno $S(\mathtt{e})$ a pokusme se pomocí uvedeného grafu nalézt složení několika *Abeced*, tak aby písmeno $S(\mathtt{e})$ bylo pevným bodem.

$$S(\mathtt{e}) = S(\mathtt{e})P_7P_9P_{14}$$

$$S(\mathtt{e}) = S(\mathtt{e})P_7P_8P_{15}P_4$$

$$S(\mathtt{e}) = S(\mathtt{e})P_7P_8P_{19}P_4$$

$$S(\mathtt{e}) = S(\mathtt{e})P_4P_5P_{11}P_{13}P_{17}$$

$$S(\mathtt{e}) = S(\mathtt{e})P_{17}P_{24}P_1P_{12}P_7$$

Najdeme jistě mnohé další rovnice, ty jsou již však závislé na uvedených rovnicích.. Zajímá nás tedy pouze část uvedeného grafu s kružnicemi. Proto můžeme z uvedeného grafu odstranit větve, které nejsou součástí kružnic, tj. větve označeny čísly 2, 3, 6, 10, 16, 18, 20, 21, 22 a 23.

Další problém spočívá v pootočení prostředního rotoru. Známe relativní pozici pravého rotoru a předpokládáme, že nedojde k pootočení levého rotoru. Abychom mohli předpokládat, že nedojde k pootočení prostředního rotoru, museli bychom zvolit kratší tahák. Tím se však zároveň snižuje pravděpodobnost nalezení dostatečného množství kružnic v příslušném grafu.

Turing však nalezl způsob jak se vypořádat s pootočením prostředního rotoru (podrobnosti viz Turingova práce [7]). Písmena taháku rozdělíme do několika skupin, např. (1-5, 6-10, …). V každé skupině mohlo dojít k pootočení prostředního rotoru. Tuto domněnku postupně ověřujeme pro všechny skupiny písmen. Tahák sice také zkracujeme, ale jen o malé skupiny písmen.

V našem příkladě zkrátíme tahák a odstraníme větve grafu označené čísly 1, 19 a 24. Jak vidíme, můžeme také odstranit větev označenou číslem 12, protože již není součástí žádné kružnice grafu.

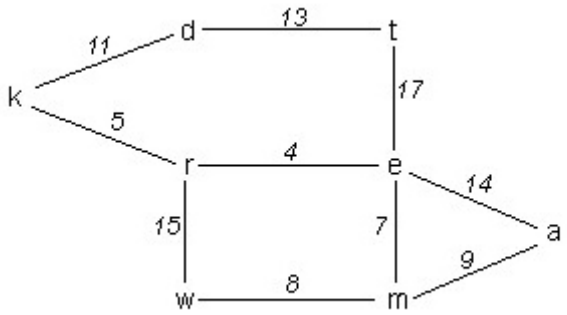
Po těchto úpravách získáme nový redukovaný graf. Počet větví se redukoval na 10, což znamená, že bude potřeba 10 přístrojů Enigma pro konstrukci bomby. Redukovaný graf má 3 kružnice, větev označená nejmenším číslem je 4, větev označená největším číslem je 17 a délka taháku je nyní 14 písmen. Pravděpodobnost pootočení prostředního rotoru je tedy 1/2. Redukuje se také počet rovnic s pevným bodem $S(\mathtt{e})$.

$$S(\mathtt{e}) = S(\mathtt{e})P_7P_9P_{14}$$

$$S(\mathtt{e}) = S(\mathtt{e})P_7P_8P_{15}P_4$$

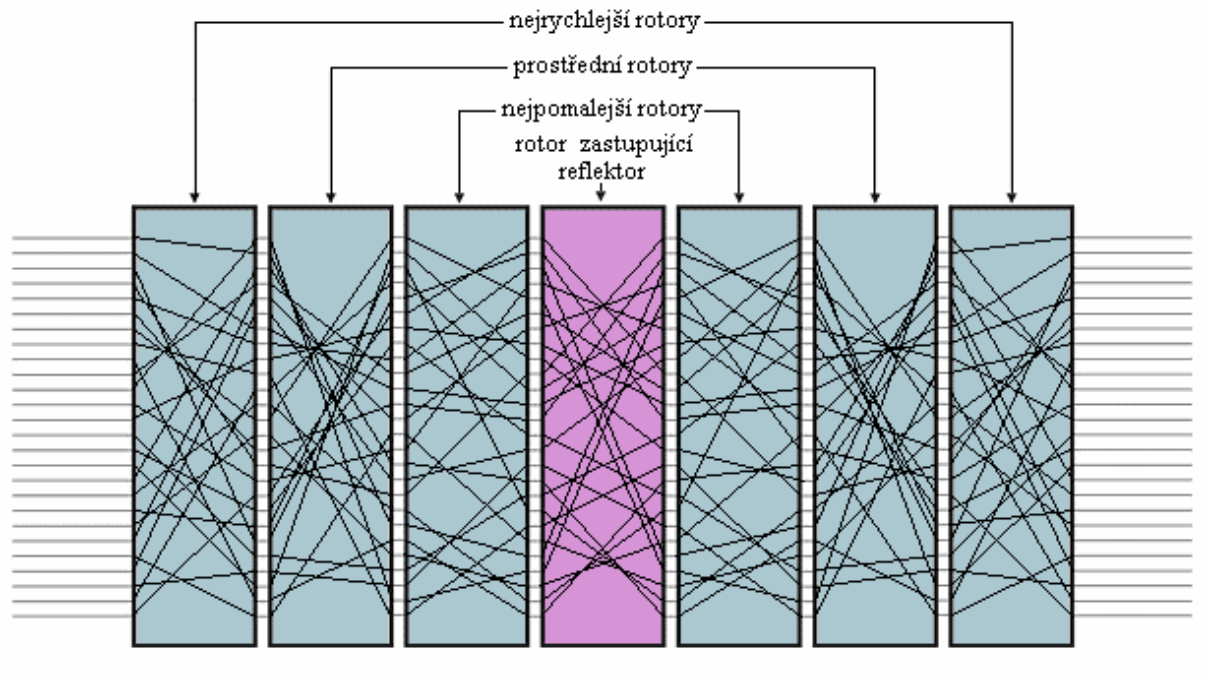
$$S(\mathtt{e}) = S(\mathtt{e})P_4P_5P_{11}P_{13}P_{17}$$

Obr 13: Redukovaný graf




Při konstrukci Turingovy bomby ve skutečnosti nebyly použity přímo přístroje Enigma. Každý přístroj byl zastoupen třemi rotory představující pohyb vpřed a třemi rotory představující pohyb vzad. Obě trojice rotorů byly spojeny prostřednictvím dalšího rotoru zastupujícího reflektor. Všechny rotory měly symetrické vnitřní propojení a prostřední rotor měl propojení stejné jako reflektor. Takto zkonstruované zařízení mělo z jedné strany kontakty pro vstup a z druhé strany kontakty pro výstup, jak můžeme vidět na obrázku. Kontakty pro výstup pak byly propojeny s kontakty pro vstup dalšího zařízení. Tímto způsobem se postupně zřetězilo potřebný počet přístrojů. Nakonec se výstupy posledního zařízení řetězce propojilo se vstupy prvního zařízení řetězce. Technické podrobnosti lze nalézt v Turingově práci [7]. Poznamenejme, že každá kružnice redukovaného grafu byla reprezentována jedním uzavřeným řetězcem přístrojů v Turingově bombě.

Obr 14: Schéma zapojení rotorů v Turingově bombě

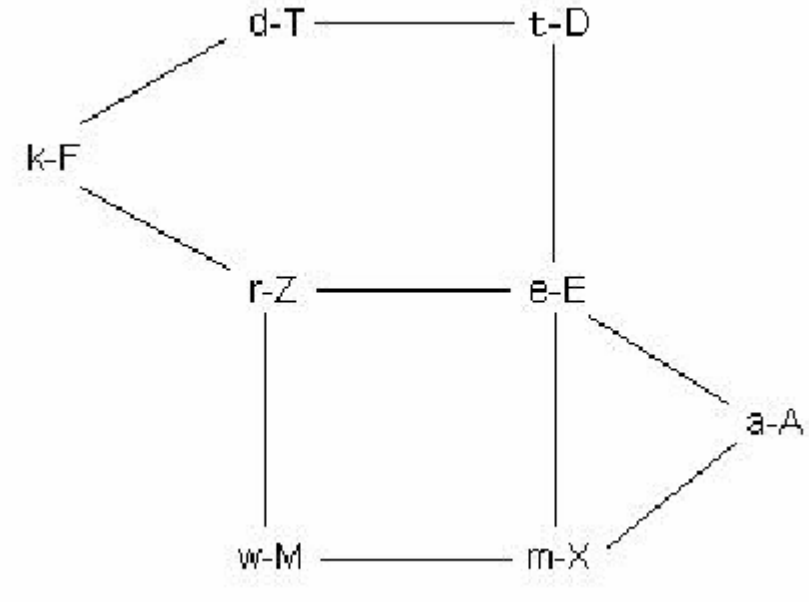


Vraťme se k našemu příkladu. Předpokládejme, že máme správné pořadí rotorů a jejich pozici (pro každé pořadí rotorů byla zkonstruována nezávislá sada přístrojů, tedy nová Turingova bomba). Necháme nyní procházet elektrický proud zastupující námi zvolené centrální písmeno e všemi uzavřenými řetězci přístroje. Pokud písmeno e nebylo změněno propojením v propojovací desce (tj. $S(\mathtt{e}) = \mathtt{e}$), pak výstupní písmeno v každém řetězci je opět e. Elektrický proud tedy zůstane izolován pouze v této jedné větvi a rozsvítí se jediná žárovka zapojená v tomto elektrickém obvodu. V tomto případě se Turingova bomba zastaví. Pokud písmeno e bylo změněno propojením v propojovací desce na písmeno $S(\mathtt{e}) \neq \mathtt{e}$ (tj. e je na propojovací desce spojeno s $S(\mathtt{e})$), pak se proud rozšíří celým přístrojem kromě jediné izolované větve se vstupním písmenem $S(\mathtt{e})$. Rozsvítí se tedy všechny žárovky zapojené do každého elektrického obvodu, kromě jediné a Turingova bomba se opět zastaví.

Turingova bomba je tedy zkonstruovaná tak, že se zastaví, kdykoliv v celém zařízení zůstane jediná izolovaná větev s elektrickým proudem nebo bez něj. Informace o této větvi nám může poskytnout informaci o propojení v propojovací desce. Pokud je v izolované větvi se vstupním písmenem e elektrický proud, pak víme, že písmeno e není permutací $S$ (tj. propojením na propojovací desce) změněno. Na druhou stranu, pokud se proud rozšíří všemi větvemi až na izolovanou větev se vstupním písmenem např. x, pak víme, že písmeno x je na propojovací desce spojeno s písmenem e (tj. $S(\mathtt{e}) = \mathtt{x}$).

Lze však získat i další informace plynoucí ze zastavení Turingovy bomby. Z uvedeného redukovaného grafu můžeme vyčíst teoretickou cestu elektrického proudu zařízením. Speciálně vidíme, že platí $S(\mathtt{e})A_7 = S(\mathtt{m})$, $S(\mathtt{e})A_7A_9 = S(\mathtt{a})$, atd. Hodnoty $S(\mathtt{m})$, $S(\mathtt{a})$, atd. lze jednoduše zjistit umístěním žárovek mezi jednotlivé přístroje Enigma. Takto můžeme najít všechna propojení na propojovací desce pro každé písmeno vyskytující se v redukovaném grafu. Následující obrázek ukazuje jednu z možností zapojení na propojovací desce v případě zastavení Truringovy bomby. Malá písmena na tomto obrázku označují původní písmena redukovaného grafu a velká písmena označují příslušná s nimi spojená písmena na propojovací desce (např. původní písmeno r je spojeno s písmenem z).

Obr 15: Graf s propojením na propojovací desce



Z tohoto obrázku s propojením na propojovací desce snadno vidíme, že tato pozice rotorů není správná (tj. došlo k zastavení Turingovy bomby při nesprávném nastavení rotorů). Situace $S(\mathtt{w}) = \mathtt{m}$ a zároveň $S(\mathtt{m}) = \mathtt{x}$ nemůže nastat, protože to nedovoluje konstrukce propojovací desky (písmeno m nemůže být spojeno s písmenem w a s písmenem x zároveň).

V listopadu roku 1939 Gordon Welchman, spolupracovník Alana Turinga v Bletchley Parku, navrhl jednoduchou elektrickou realizaci detekování chybného zastavení Turingovy bomby. Sloužila k tomu speciální součást tzv. *diagonální deska*. Diagonální desku představovaly konektory rozmístěné do 26 řad a 26 sloupců označené písmeny abecedy. Vodiče mezi každou dvojicí přístrojů Enigma v Turingově bombě byly spojeny se všemi 26 písmeny v řádku označeném odpovídajícím písmenem z redukovaného grafu. Například vodiče mezi přístroji označené čísly 11 a 13 byly spojeny s písmeny ve čtvrté řadě označené písmenem d. V této řadě byla ostatní písmena, která se objevila v redukovaném grafu spojená s písmenem d v odpovídajícím sloupci. Například písmeno t ve čtvrtém řádku bylo spojeno s písmenem d ve dvacátém řádku označeném písmenem t.

Vysvětleme si nyní na dvou příkladech jak toto zapojení diagonální desky funguje.

*Příklad 1*. Předpokládejme, že žárovka spojená s písmenem t mezi přístroji označené čísly 11 a 13 se rozsvítí. Což znamená, že platí $S(\mathtt{d}) = \mathtt{t}$. Proto také platí $S(\mathtt{t}) = \mathtt{d}$ a žárovka spojená s písmenem d mezi přístroji označené čísly 13 a 17 se také rozsvítí. Diagonální deska zaručuje, že elektrický proud projde od písmene t mezi přístroji 11 a 13 k písmeni d mezi přístroji 13 a 17. Tedy v tomto případě diagonální deska nic nemění.

*Příklad 2*. Předpokládejme, že žárovka spojená s písmenem x mezi přístroji označené čísly 7 a 8 se rozsvítí. Což znamená, že platí $S(\mathtt{m}) = \mathtt{x}$. Avšak žárovka spojená s písmenem m mezi přístroji označené čísly 8 a 15 se taká rozsvítí. Platí tedy také $S(\mathtt{w}) = \mathtt{m}$, což nemůže nastat. Na diagonální desce je vodičem spojeno písmeno m (v řádku označeném písmenem w) s písmenem w (v řádku označeném písmenem m). Elektrický proud prochází písmenem x mezi přístroji označené čísly 7 a 8, ale díky diagonální desce prochází také písmenem w a tedy se neuzavře izolovaná větev a Turingova bomba se nezastaví.

Díky tomuto vylepšení Turingovy bomby se hledání denních klíčů značně zrychlilo. Pokud šlo vše dobře byla bomba schopna nalézt správný klíč již za hodinu. Do konce války bylo pomocí Turingových bomb každý den rozšifrováno velké množství zachycených německých depeší. Druhá světová válka tedy skončila velkým úspěchem nejen britských ale i polských kryptoanalytiků.

# Dodatek: Kapitola o permutacích

Tato kapitola shrnuje poznatky z teorie permutací potřebné pro korektní rozluštění přístroje Enigma.

Dále uvažujeme, že množina $M$ je nějaká podmnožina všech písmen abecedy. Pro větší názornost volíme množinu $M = \{\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}, \mathtt{e}, \mathtt{f}\}$.

**Definice.** *Permutací S na množině* $M = \{\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}, \mathtt{e}, \mathtt{f}\}$ rozumíme každé prosté zobrazení množiny $M$ na ni samu. Permutaci $S$ zpravidla zapisujeme v tzv. *základním tvaru*, tj. ve tvaru tabulky, kde prvky množiny $M$ jsou v horním řádku v abecedním pořadí:

$$S = \begin{pmatrix} \mathtt{a} & \mathtt{b} & \mathtt{c} & \mathtt{d} & \mathtt{e} & \mathtt{f} \\ \mathtt{e} & \mathtt{f} & \mathtt{d} & \mathtt{b} & \mathtt{c} & \mathtt{a} \end{pmatrix}.$$

Je-li pořadí prvků množiny $M$ v horním řádku libovolné, říkáme, že permutace $S$ je v tzv. *obecném tvaru*, např.

$$S = \begin{pmatrix} \mathtt{c} & \mathtt{e} & \mathtt{b} & \mathtt{d} & \mathtt{f} & \mathtt{a} \\ \mathtt{d} & \mathtt{c} & \mathtt{f} & \mathtt{b} & \mathtt{a} & \mathtt{e} \end{pmatrix}$$

Vidíme tedy, že permutace $S$ může být zapsána různými způsoby, vždy však musí platit: $S(\mathtt{a}) = \mathtt{e}$, $S(\mathtt{b}) = \mathtt{f}$, $S(\mathtt{c}) = \mathtt{d}$, $S(\mathtt{d}) = \mathtt{b}$, $S(\mathtt{e}) = \mathtt{c}$, $S(\mathtt{f}) = \mathtt{a}$.

**Definice.** Permutaci $I$ množiny $M$ nazýváme *identickou*, tj. každý prvek množiny $M$ se v permutaci $I$ zobrazí sám na sebe

$$I = \begin{pmatrix} \mathtt{a} & \mathtt{b} & \mathtt{c} & \mathtt{d} & \mathtt{e} & \mathtt{f} \\ \mathtt{a} & \mathtt{b} & \mathtt{c} & \mathtt{d} & \mathtt{e} & \mathtt{f} \end{pmatrix}.$$

Permutace můžeme také umocňovat.

**Definice.** Nechť $S$ je permutace na množině $M$ a prvek $x$ patří do množiny $M$. Pak permutace $S^2$ je dána předpisem

$$S^2(x) = S(S(x)),$$

pro každý prvek $x$ množiny $M$.

Vidíme, že v našem příkladě permutace $S$ zobrazuje písmeno $\mathtt{a}$ na písmeno $\mathtt{e}$ a písmeno $\mathtt{e}$ zobrazuje na písmeno $\mathtt{c}$. Pak tedy permutace $S^2$ zobrazuje písmeno $\mathtt{a}$ na písmeno $\mathtt{c}$, tj. platí

$$S^2(\mathtt{a}) = \mathtt{c}.$$

Obdobně můžeme také definovat mocniny permutací vyšších řádů.

**Definice.** Permutaci

$$S^{-1} = \begin{pmatrix} \mathtt{e} & \mathtt{f} & \mathtt{d} & \mathtt{b} & \mathtt{c} & \mathtt{a} \\ \mathtt{a} & \mathtt{b} & \mathtt{c} & \mathtt{d} & \mathtt{e} & \mathtt{f} \end{pmatrix}$$

nazýváme *inverzní permutací* k permutaci

$$S = \begin{pmatrix} \mathtt{a} & \mathtt{b} & \mathtt{c} & \mathtt{d} & \mathtt{e} & \mathtt{f} \\ \mathtt{e} & \mathtt{f} & \mathtt{d} & \mathtt{b} & \mathtt{c} & \mathtt{a} \end{pmatrix}.$$

Analogicky jako umocňování permutací na kladné mocniny, lze také definovat umocňování permutací na záporné mocniny.

**Definice.** Nechť $S$ a $T$ jsou dvě permutace na množině $M$. Pak rovnost permutací $S = T$ nastává právě, když platí

$$S(x) = T(x)$$

pro každý prvek $x$ množiny $M$.

**Definice.** Nechť $S$ a $T$ jsou dvě permutace na množině $M$. Permutaci $ST$ nazveme součinem permutací $S$ a $T$ pokud platí

$$ST(x) = T(S(x))$$

pro každý prvek $x$ množiny $M$.

Součin $ST$ není obecně roven součinu $TS$.

$$TS = \begin{pmatrix} \mathtt{a} & \mathtt{b} & \mathtt{c} & \mathtt{d} & \mathtt{e} & \mathtt{f} \\ \mathtt{b} & \mathtt{e} & \mathtt{a} & \mathtt{d} & \mathtt{f} & \mathtt{c} \end{pmatrix} \neq ST = \begin{pmatrix} \mathtt{a} & \mathtt{b} & \mathtt{c} & \mathtt{d} & \mathtt{e} & \mathtt{f} \\ \mathtt{b} & \mathtt{e} & \mathtt{c} & \mathtt{a} & \mathtt{f} & \mathtt{d} \end{pmatrix}$$

Vidíme tedy, že pro násobení permutací obecně neplatí *komutativní zákon*.

Permutaci $S$ můžeme zapsat také v tzv. *cyklickém tvaru*, který se často používá v celém textu. Tento zápis spočívá v tom, že zvolíme libovolné písmeno z horního řádku permutace $S$ (např. a) a vpravo od něj napíšeme příslušné písmeno nacházející se v dolním řádku permutace $S$ (písmeno e). Toto písmeno pak vyhledáme v horním řádku a připíšeme příslušné písmeno v dolním řádku (písmeno c). Takto pokračujeme dále až narazíme na první zvolené písmeno, které již znovu nezapisujeme.Výslednou posloupnost písmen uzavřeme do závorek a nazveme jej *cyklem*.Pokud v získaném cyklu nejsou všechna písmena množiny $M$, pak zvolíme další písmeno a opět stejným postupem získáme druhý a další cykly.

*Příklad:*

$$S = \begin{pmatrix} \mathtt{a} & \mathtt{b} & \mathtt{c} & \mathtt{d} & \mathtt{e} & \mathtt{f} \\ \mathtt{e} & \mathtt{f} & \mathtt{d} & \mathtt{b} & \mathtt{c} & \mathtt{a} \end{pmatrix} = (\mathtt{a}\ \mathtt{e}\ \mathtt{c}\ \mathtt{d}\ \mathtt{b}\ \mathtt{f})$$

$$T = \begin{pmatrix} \mathtt{a} & \mathtt{b} & \mathtt{c} & \mathtt{d} & \mathtt{e} & \mathtt{f} \\ \mathtt{d} & \mathtt{a} & \mathtt{f} & \mathtt{c} & \mathtt{d} & \mathtt{e} \end{pmatrix} = (\mathtt{a}\ \mathtt{d}\ \mathtt{c}\ \mathtt{f}\ \mathtt{e}\ \mathtt{b})$$

$$Q = \begin{pmatrix} \mathtt{a} & \mathtt{b} & \mathtt{c} & \mathtt{d} & \mathtt{e} & \mathtt{f} \\ \mathtt{f} & \mathtt{a} & \mathtt{e} & \mathtt{d} & \mathtt{c} & \mathtt{b} \end{pmatrix} = (\mathtt{a}\ \mathtt{f}\ \mathtt{b})(\mathtt{c}\ \mathtt{e})(\mathtt{d})$$

$$R = \begin{pmatrix} \mathtt{a} & \mathtt{b} & \mathtt{c} & \mathtt{d} & \mathtt{e} & \mathtt{f} \\ \mathtt{a} & \mathtt{f} & \mathtt{d} & \mathtt{e} & \mathtt{c} & \mathtt{b} \end{pmatrix} = (\mathtt{a})(\mathtt{b}\ \mathtt{f})(\mathtt{c}\ \mathtt{d}\ \mathtt{e})$$

**Definice.** Dvě permutace $S$ a $T$ na množině $M$ nazveme *podobné*, pokud mají stejnou cyklickou strukturu, tj. v obou permutacích se vyskytují cykly stejné délky.

Vidíme, že v předchozím příkladě jsou permutace $S$ a $T$ podobné, neboť každá se skládá z jednoho šesti písmenného cyklu. Podobně také permutace $Q$ a $R$ jsou podobné.

Můžeme říci, že délka a počet cyklů v určitém smyslu charakterizuje permutace. Permutace tedy lze rozdělit do tříd podle podobnosti.

*Poznámka.* Cykl délky 2 se nazývá *transpozice*.

**Věta.** *Pokud dvě permutace X, Y na nějaké množině M jsou tvořeny pouze disjunktními transpozicemi, pak jejich součin XY obsahuje vždy sudý počet cyklů stejné délky.*

*Důkaz.* Předpokládejme, že velikost množiny $M$ je $2n$ (velikost množiny $M$ musí být sudá, neboť permutace $X$ a $Y$ se skládají z disjunktních transpozic).

Pokud permutace $X$ obsahuje stejnou transpozici jako permutace $Y$, např. $(a, b)$, pak součin $XY$ bude obsahovat vždy dva cykly délky 1 $(a)$ a $(b)$. Tedy každá stejná transpozice je v součinu reprezentována dvěma cykly délky 1.

Můžeme tedy předpokládat, že permutace $X$ a $Y$ nemají žádné stejné transpozice. Bez újmy na obecnosti předpokládejme, že v jednotlivých permutacích se vyskytují následující transpozice

| permutace $X$ | permutace $Y$ |
|---|---|
| $(a_1, a_2)$ | $(a_2, a_3)$ |
| $(a_3, a_4)$ | $(a_4, a_5)$ |
| … | … |
| $(a_{2k-3}, a_{2k-2})$ | $(a_{2k-2}, a_{2k-1})$ |
| $(a_{2k-1}, a_{2k})$ | $(a_{2k}, a_1)$ |

pro nějaké $k \leq n$. Počáteční písmeno $a_1$ se musí nakonec objevit v permutaci $Y$ (z definice permutace). Vidíme, že součin $XY$ pak osahuje jeden cykl $(a_1, a_3, \ldots, a_{2k-3}, a_{2k-1})$ a druhý cykl $(a_{2k}, a_{2k-2}, \ldots, a_4, a_2)$ oba stejné délky $k$.

Takto postupně vyčerpáme všechny prvky množiny $M$, přičemž vždy dostaneme sudý počet cyklů stejné délky. ■

Poznamenejme, že tato věta je jedna ze stěžejních, jež pomohly Marianu Rejewskému v odhalování denních klíčů.

*Příklad:*

$$V = (\texttt{a f})(\texttt{b d})(\texttt{c h})(\texttt{e g})(\texttt{i j})$$

$$W = (\texttt{a e})(\texttt{b h})(\texttt{c j})(\texttt{d i})(\texttt{f g})$$

$$VW = (\texttt{a g})(\texttt{b i c})(\texttt{d h j})(\texttt{e f})$$

**Důsledek.** Prvky stejné transpozice se v součinu $XY$ objevují v různých cyklech stejné délky.

**Důsledek.** Pokud se dva prvky objevují v permutaci $XY$ ve dvou různých cyklech stejné délky a současně tvoří transpozici v některé z permutací $X$, $Y$, pak sousední dvojice prvků (levý a pravý v obou cyklech) také tvoří transpozici ve stejné permutaci.

**Definice.** Nechť $A$, $B$ a $C$ jsou tři permutace na množině $M$. Pokud tyto permutace splňují rovnici

$$A = C^{-1}BC,$$

pak řekneme, že permutace $A$ a $B$ jsou *konjugované*. Říkáme také, že permutace $A$ je *konjugovaná* s permutací $B$ pomocí permutace $C$.

**Lemma.** *Dvě permutace X, Y na množině M jsou konjugované právě, když mají stejnou cyklickou strukturu.*

*Příklad:*

$$A = (\texttt{b e a})(\texttt{c f})(\texttt{d})$$

$$B = (\texttt{a d f})(\texttt{b e})(\texttt{c})$$

$$C = (\texttt{a b c d e f})$$

Vidíme, že permutace splňují rovnost

$$A = C^{-1}BC.$$

Na tomto příkladě jednoduše vidíme dva důsledky:

- Konjugované permutace *A* a *B* jsou podobné.
- Permutaci *C* získáme tak, že permutaci *A* zapíšeme pod permutaci *B* v cyklickém zápisu tak, aby se cykly stejné délky nacházely pod sebou a ihned vidíme permutaci *C* (obraz každého písmene je písmeno nacházející se pod ním).

**Důsledek.** *Nechť A, C a X jsou tři permutace na množině M, přičemž permutace X je neznámá. Pak rovnice*

$$C = X^{-1}AX$$

*je řešitelná právě, když permutace A a C jsou podobné.*

Pokud je daná rovnice $C = X^{-1}AX$ řešitelná, pak permutací *X*, které tuto rovnici řeší je více.

*Příklad:*

$$X_1 = \begin{pmatrix} \texttt{a d f b e c} \\ \texttt{b e a c f d} \end{pmatrix} = (\texttt{a b c d e f})$$

$$X_2 = \begin{pmatrix} \texttt{a d f b e c} \\ \texttt{e a b c f d} \end{pmatrix} = (\texttt{a e f b c d})$$

$$X_3 = \begin{pmatrix} \texttt{a d f b e c} \\ \texttt{a b e c f d} \end{pmatrix} = (\texttt{a})(\texttt{d b c})(\texttt{f e})$$

$$X_4 = \begin{pmatrix} \texttt{a d f b e c} \\ \texttt{b e a f c d} \end{pmatrix} = (\texttt{a b f})(\texttt{d e c})$$

$$X_5 = \begin{pmatrix} \texttt{a d f b e c} \\ \texttt{e a b f c d} \end{pmatrix} = (\texttt{a e c d})(\texttt{b f})$$

$$X_6 = \begin{pmatrix} \texttt{a d f b e c} \\ \texttt{a b e f c d} \end{pmatrix} = (\texttt{a})(\texttt{d b f e c})$$

Vidíme, že pouze řešení $X_1$ je shodné s permutací *C* z předchozího příkladu.

Poznamenejme, že uvedené Lemma Rejewski nejvíce využil při rekonstruování vnitřního propojení přístroje Enigma.

**Definice.** *Abecedou* nazveme nějakou permutaci množiny 26 písmen {a, b, …, z} obsahující 13 disjunktních transpozic.

# Příloha: Model roštu

# Literatura


[1] Bauer F. L.: *Decrypted secrets: Methods and Maxims of Cryptology*, *second edition*, Springer-Verlag, Berlín, 2000.

[2] Rejewski M.: *An Application of the Theory of Permutations in Breaking the Enigma Cipher*, Applicationes Mathematicae 16, No. 4, Waršava, dostupný na: http://mad.home.cern.ch/frode/crypto/rew80.pdf

[3] Rejewski M.: *Enigma (1930 – 1940), Metoda i historia rozwiazania Niemieckiego szyfru maszynowego (w zarysie)*, nepublikovaný rukopis, dostupný na: http://www.spybooks.pl/en/enigma.html

[4] Rejewski M.: *Jak matematycy polscy rozszyfrowali Enigmę*, Roczniki polskiego towarzystwa matematycznego, seria II: Wiadomości matematyczne XXIII, 1980, dostupný na: http://www.spybooks.pl/en/enigma.html

[5] Rejewski M.: *Wspomnienia z mej pracy w Biurze Szyfrów Oddziału II Sztabu Głównego w latach 1930 – 1945*, nepublikovaný rukopis, dostupný na: http://www.spybooks.pl/en/enigma.html

[6] Singh S.: *Kniha kódů a šifer, Tajná komunikace od starého Egypta po kvantovou kryptografii*, Dokořán, Praha, 2003.

[7] Turing A. M.: *Turing's Treatise on Enigma*, NARA College Park, Maryland, Record Group 457, Historic Cryptographic Collection, Box 201, NR 964, 1940. Tento dokument vydali Weirud F., Erskine R. a Marks P. na internetových stránkách Froda Weiruda: http://frode.home.cern.ch/frode/crypto/Turing

[8] Vábek J.: *Diplomová práce: Kryptoanalýza německé vojenské šifry Enigma*, Matematicko-fyzikální fakulta Univerzity Karlovy, Praha, 2005.

[9] http://www.ellsbury.com/enigmabombe.htm