Kapitola 6

Enigma

Když se Německo začalo chystat ve třicátých létech minulého století na novou válku, hledalo velení ozbrojených sil nový šifrovací systém. Vedly je k tomu nejenom nezdary v průběhu první světové války, ale i plány na *blitzkrieg,* bleskovou válku. Ta vyžaduje pečlivou koordinaci činnosti jednotlivých částí armády a z toho vyplývá nutnost zajistit efektivní a spolehlivé spojení. V tehdejší době bylo nejúčinnější radiové spojení, které je ale možné odposlouchávat. Kvalitní šifrovací systém byl proto naprostou nezbytností.

Velení německé armády nakonec vybralo a upravilo původně komerční šifrovací přístroj, jehož vynálezcem a výrobcem byl německý podnikatel *Arthur Schrebius*. Popíšeme si jednu z mnoha vojenských variant tohoto přístroje, pro který se ujal název *Enigma*.

Přístroj fungoval uživatelsky jednoduše, jak se můžeme přesvědčit na následujícím simulátoru.

Na této simulaci vidíme několik částí přístroje. Jsou to klávesnice, žárovky s napsanými písmeny rozmístěné stejně jako jsou rozmístěná písmena na klávesnici, propojovací deska a tři okna nad žárovkami. To jsou viditelné části přístroje. Jejich skutečný vzhled vidíte na prvním obrázku.

Obr. 1

Funkce mnohých z nich je zřejmá. Operátor přístroje dostal otevřený text. Klávesnici přístroje používal stejně jako u psacího stroje. Stisknul klávesu, po jejím stisknutí se rozsvítila jedna ze žárovek. Zapsal si písmeno označující tuto žárovku, stisknul klávesu odpovídající druhému písmenu otevřeného textu, písmeno na rozsvícené žárovce bylo druhým písmenem šifrového textu, atd. Po zašifrování celého textu předal šifrový text radistovi.

Například otevřený text

```
VALKA ZACNE VUTER YRANO
```

po zašifrování mohl vypadat třeba následovně.

```
PHYOF BFXUC YIWJS EFCWN
```

Radista na druhé straně kanálu přijal šifrový text, obsluha šifrovacího přístroje jej přepsala na stejném přístroji stejným způsobem, získala tak otevřený text, který předala adresátovi. Takto dobře to fungovalo za předpokladu, že obsluha přístroje na straně adresáta měla přístroj nastavený stejně jako obsluha na straně odesílatele.

Jaké možnosti nastavení přístroj poskytoval? *Propojovací deska* umožňovala pomocí kabelů propojit dvojice písmen. V počátcích používání Enigmy bylo používáno šest kabelů, později deset. Tak například můžeme udělat propojení LV, AC, DP, RM, IT, HN. Potom zašifrováním stejného otevřeného textu dostaneme šifrový text

```
NJSOL BZLCA DTOJN ENCIH
```

Dešifrování proběhne bez problémů za předpokladu, že přijímací strana používá stejné propojení kabelů. Pokud by žádné kabely nepoužívala, tak odšifrování posledního šifrového textu při jinak stejném nastavení přístroje by dalo nesmyslný text

```
JCVKR ZCSMG KVIEG YDAGI
```

Stejně tak by dalo nesmyslný výsledek propojení jiných dvojic písmen pomocí kabelů. Propojení pomocí kabelů není jediná možnost nastavení přístroje. Propojovací deska byla ale novinkou u vojenské Enigmy, původní Scherbiova Enigma určená pro komerční využití ji neobsahovala. Další části přístroje se ale do určité míry shodovaly s komerčním přístrojem, který mnozí kryptoanalytici znali. Tyto části jsou ale skryté a viditelné až po otevření přístroje.

Obr. 2

Vidíme, že uvnitř přístroje je několik rotorů. Elektrický proud z propojovací desky přicházel napřed do *vstupního kruhu,* který se nepohyboval. V komerčním přístroji bylo propojení takové, že z jednotlivých kláves klávesnice uspořádané následujícím způsobem

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

vstupoval proud do vstupního kruhu ve stejném pořadí jako na klávesnici, a to po směru hodinových ručiček, v pořadí

```
QWERTZUIOASDFGHJKPYXCVBNHML
```

Ve vojenské Enigmě toto propojení bylo samozřejmě jiné a jeho odhalení bylo jedním z velkých úspěchů polských kryptologů ještě v období před začátkem druhé světové války.

Ze vstupního pevného kruhu proud procházel třemi *rotory,* uvnitř kterých docházelo k permutování vstupního signálu. Každý rotor měl totiž na vstupu 26 kolíků, kterými do něho proud vstupoval. Uvnitř bylo 26 vzájemně izolovaných drátů, které vedly ke kontaktním plochám na opačné straně rotoru. Toto propojení tak uvnitř každého rotoru provádělo určitou neznámou permutaci. Je skoro zbytečné dodávat, že permutace prováděné v rotorech vojenské Enigmy byly jiné než u veřejně dostupné komerční Enigmy. Vnější detaily rotorů vidíte na následujícím obrázku.

Obr. 3

Po průchodu třemi rotory proud vstoupil do *reflektoru*, který byl v přístroji pevně umístěn. Aspoň tomu tak bylo v době před druhou světovou válkou, pozdější verze Enigmy obsahovaly vyměnitelné reflektory, které bylo možné do přístroje vložit několika způsoby. My se ale budeme zabývat variantou s pevným reflektorem. Uvnitř tohoto reflektoru bylo třináct propojení pomocí izolovaných drátů, které spojovaly vždy dva různé vstupní/výstupní kolíky reflektoru. Poté proud prošel zpět třemi rotory, vstupním kruhem, propojovací deskou až nakonec rozsvítil příslušnou žárovku. Schématicky je cesta proudu přístrojem znázorněna na následujícím obrázku.

Obr. 4

Takto sestavený přístroj by při pevném zapojení kabelů na propojovací desce nedělal nic jiného než jednoduchou záměnu, snadno řešitelnou šifru. V tomto okamžiku vstupuje do hry hlavní rys Enigmy. Rotory se během šifrování pootáčí. Po stisknutí jakékoliv klávesy se pravý rotor napřed pootočí o 1/26 celého úhlu a pak teprve proud projde celým obvodem. Nejen to, všechny tři rotory byly propojené tak, aby fungovaly jako tři kolečka tachometru. Na určitém místě se pohyb pravého rotoru přenesl na střední rotor, který se také pootočil o 1/26 celého úhlu. A stejně tak se při určité poloze středního rotoru jeho pohyb přenesl rovněž na levý rotor. Také ten se pak pootočil o 1/26 celého úhlu. Zatímco u tachometru se pohyb nějakého kolečka přenáší na kolečko vlevo vždy v okamžiku, kdy na pravém kolečku dochází k výměně cifry 9 za cifru 0, u Enigmy to bylo zařízeno jinak. Na obvodu každého rotoru bylo cosi jako malá pneumatika, *kroužek,* který bylo

možné posouvat po obvodu příslušného rotoru. Byla na něm také úchytka, která umožnila kroužek k rotoru pevně uchytit. A na každém kroužku byl jeden zářez, který udával místo, kdy se pohyb tohoto rotoru přenášel na sousední rotor vlevo. Tak například pohyb z rotoru označovaného jako I se přenášel na rotor vlevo v okamžiku, kdy v okénku nahoře bylo vidět písmeno R (zářez byl ve skutečnosti u písmene Y).

Rotory bylo navíc možné vyjmout a změnit jejich pořadí. Nyní tedy můžeme spočítat počet možných nastavení varianty Enigmy, která byla v používání až do 15. září roku 1938. Ta měla pouhé tři rotory, pozdější varianty jich měly pět až osm.

Počet možných pořadí tří rotorů:

$$6,$$

počet možných počátečních poloh rotorů:

$$26 \cdot 26 \cdot 26 = 17576,$$

počet možných uchycení kroužků na obvodu rotorů:

$$26 \cdot 26 \cdot 26 = 17576,$$

počet možných propojení na propojovací desce při použití 6 kabelů:

$$\binom{26}{2} \cdot \binom{24}{2} \cdot \binom{22}{2} \cdot \binom{20}{2} \cdot \binom{18}{2} \cdot \binom{16}{2} =$$

$$= \frac{26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15}{2^6} \sim 2,89 \cdot 10^{14}.$$

Celkový počet možných nastavení této základní předválečné Enigmy se tak rovná přibližně

$$6 \cdot 26^3 \cdot 26^3 \cdot 2,89 \cdot 10^{14} \sim 5,36 \cdot 10^{23}.$$

Nejvíc možností tak vnášela do systému propojovací deska. Později bylo používáno 10 kabelů, čímž se počet možných propojení zvýšil na $2,19 \cdot 10^{21}$. Také počet rotorů se zvyšoval, při použití 5 rotorů se počet možností pro jejich výběr a pořadí rovnal

$$\binom{5}{3} \cdot 6 = 60,$$

při použití 8 rotorů to bylo

$$\binom{8}{3} \cdot 6 = 336.$$

Někdy kolem roku 1930 začala polská odposlouchávací služba zachycovat šifrované signály německých vojenských jednotek. První věcí, které si polští kryptoanalytici všimli, byla skutečnost, že pokud se dvě šifrové zprávy zachycené stejný den shodovaly na prvních šesti místech, pak se jejich index koincidence prudce zvýšil a rovnal se přibližně indexu koincidence němčiny. To napovídalo, že prvních šest písmen jsou indikátorem, který udává nastavení šifrovacího systému, počínaje sedmým písmenem pak začíná vlastní šifrový text. Navíc to napovídá, že pro šifrování otevřeného textu byla použita polyalfabetická záměna, tj. každé písmeno textu bylo šifrováno pomocí nějaké permutace abecedy, tyto permutace se lišily v závislosti na poloze písmena v otevřeném textu (a samozřejmě také na indikátoru – počáteční šestici písmen). Polská tajná služba rovněž znala komerční Enigmu, která byla na trhu od roku 1926, a měla tedy důvody uvažovat o tom, že bylo použito nějaké mechanické zařízení podobné Enigmě. Tehdy dostalo vedení polské tajné služby originální nápad. Na luštění takových mechanických šifrových systémů najalo matematiky. Do té doby tajné služby vyhledávaly hlavně lingvisty, křížovkáře, šachisty, apod. Matematici ale v hledáčku tajných služeb nebyli.

Nepodařilo se mi najít, v kterém okamžiku zasáhla do hry francouzská špionáž. Prostřednictvím svého agenta Hans-Thilo Schmidta získala instrukce pro používání šifrovacího systému Enigma. Ani francouzská ani anglická tajná služba si s návodem k použití nevěděly rady, považovaly Enigmu za nerozluštitelný šifrový systém. Na základě dohody o spolupráci potom Francouzi tyto informace předali polské tajné službě. Tím se Poláci dozvěděli o existenci propojovací desky, kroužcích na obvodu jednotlivých rotorů, a také hlavně o způsobu předávání informací o nastavení přístroje. To se dělo pomocí *denního klíče*. Tyto denní klíče byly obsluze jednotlivých stanic Enigmy předávány vždy ve vytištěné podobě pomocí kurýrů na celý měsíc dopředu a obsahovaly následující informaci. Především *pořadí rotorů (Walzenlage)* v přístroji (později i jejich výběr v době, kdy bylo používáno více rotorů než tři) zleva doprava. Dále *natočení kroužků (Ringstellung)* na obvodu jednotlivých rotorů. Zde bylo udáno písmeno, které mělo být přichyceno úchytem na obvodu příslušném rotoru. Potom *základní nastavení rotorů (Grundstellung)*, které udávalo, jaké písmeno příslušného kroužku mělo být na počátku vidět v okénku v horní desce přístroje. Kromě toho obsahoval

denní klíč informaci o *propojení na propojovací desce (Steckerverbindungen)* v podobě zpočátku šesti dvojic písmen, později deseti dvojic písmen.

Při šifrování zprávy obsluha napřed nastavila přístroj podle denního klíče. Pak zvolila náhodně trojici písmen, které měly tvořit klíč pro konkrétní zprávu. Tuto trojici si napsala dvakrát po sobě a zašifrovala ji pomocí přístroje nastaveného podle denního klíče. Poté natočila jednotlivé rotory tak, aby v okéncích v horní desce přístroje byla vidět tři zvolená písmena a pokračovala v šifrování zprávy pomocí zvoleného klíče pro tuto konkrétní zprávu.

Obsluha na straně příjemce zprávy také začínala dešifrovat s přístrojem nastaveným podle denního klíče. Pokud při přenosu nedošlo k žádné chybě, získala tak z prvních šesti písmen přijaté zprávy opakující se trojici písmen. Podle ní si natočila rotory a dále pokračovala v dešifrování pomocí nově nastaveného přístroje. Klíče pro konkrétní zprávy se měnily s každou další zprávou.

Toto tedy byly informace, které dostala polská tajná služba k dispozici od francouzské. Nic nevěděla o vnitřním propojení v jednotlivých rotorech, o propojení v reflektoru ani o propojení mezi propojovací deskou a vstupním kruhem. Tyto informace špion s krycím jménem *Asché* nemohl poskytnout. Potvrdilo se ale aspoň podezření, že prvních šest písmen každé zprávy je indikátor udávající informaci o klíči pro konkrétní zprávu, zatímco vlastní šifrový text začíná sedmým písmenem. Německá armáda zvolila dvojí opakování klíče z obav před možnými poruchami při přenosu rádiového signálu. Kdyby přijímací strana špatně přijala trojici klíče pro konkrétní zprávu, nastavila by přístroj jinak a dešifrování by vedlo k nesrozumitelnému textu. Proto zvolila tento jednoduchý samoopravný kód. Tím ale také vnesla do šifrového systému vrátka k jeho prolomení. Když 1.května 1940 konečně opustila dvojí opakování indikátoru zprávy, celý systém fungoval dále bez velkých problémů. Bylo ale už pozdě, protože Enigma byla v té již době prolomena a opuštění dvojího opakování indikátoru zprávy nepředstavovalo pro spojence žádný problém.

Do luštění šifrového systému Enigma se také pustila trojice mladých polských matematiků *Marian Rejewski* (1905-1980), *Jerzy Różycki* (????) a *Henryk Zygalski* (1906-1978). Marian Rejewski se pustil do zkoumání toho, jak využít dvojího opakování klíče pro jednotlivou zprávu. Jeho postup je překrásnou ukázkou použití matematického uvažování v kryptoanalýze.

Němečtí kryptografové nepochybně věděli, že dvojí opakování trojice písmen v indikátoru zprávy představuje riziko. Stejně tak museli vědět, že používání stejného denního klíče pro šifrování všech klíčů pro konkrétní zprávy během jednoho dne také představuje riziko. Byli ale přesvědčeni, že složitost

Enigmy je taková, že opakování klíče pro denní zprávy k šifrování pouhých šestic písmen a dvojí opakování trojice písmen představující klíč pro konkrétní zprávu nebude stačit k prolomení. Jak moc se mýlili!

Ještě než se pustíme do sledování Rejewského úvah, uvědomíme si další zvláštnosti vyplývající z konstrukce Enigmy. Kvůli vnitřnímu propojení v reflektoru se nemůže žádné písmeno zašifrovat stejným písmenem. Dále ze stejného důvodu byla permutace použitá na každém místě tvořena třinácti cykly délky 2. To znamená, že pokud bylo otevřené písmeno `u` zašifrováno třeba písmenem `q`, pak otevřené písmeno `q` na stejném místě bylo šifrováno písmenem `u`. Tato zvláštnost Enigmy vyplývá z elektrického schématu na Obr. 4.

Při volbě denního klíče pro jakoukoliv polohu kroužku-pneumatiky na pravém rotoru pouze šest počátečních základních nastavení tohoto rotoru způsobilo, že se během šifrování indikátoru pootočil také prostřední rotor, případně rovněž levý rotor. U zbývajících 20 možných základních nastavení pravého rotoru se při šifrování pootáčí pouze pravý rotor. Následující úvahy jsou v pořádku, pokud se při šifrování šesti písmen indikátoru libovolné denní zprávy otáčí pouze pravý rotor. Protože ale denní klíče byly generovány náhodně, byl tento předpoklad použitelný pro přibližně tři čtvrtiny dní.

Při použití stejného denního klíče (který ovšem kryptoanalytik neznal) bylo k zašifrování prvních šesti písmen každé zprávy použito stejné základní nastavení Enigmy a tedy stejných šest neznámých permutací, které si označíme postupně A, B, C, D, E, F. Protože se ale první a čtvrté písmeno otevřeného indikátoru rovnalo, bylo možné ze zachycených zpráv, pokud jich bylo během stejného dne dostatek, zjistit *složení permutací* AD. Pokud totiž otevřené `x` na prvním místě bylo zašifrováno jako $\mathtt{x}A = \mathtt{y}$ a totéž otevřené `x` na čtvrtém místě jako $\mathtt{x}D = \mathtt{z}$, pak (protože každá z permutací A, B, C, D, E, F byla tvořena samými dvojcykly, tj. platí $A^{-1} = A$, $B^{-1} = B$, atd.) rovněž $\mathtt{y}A = \mathtt{x}$ a $\mathtt{z}D = \mathtt{x}$. Proto $\mathtt{y}AD = \mathtt{z}$. Permutaci AD tak vyčteme z prvních a čtvrtých písmen indikátorů. Podobně permutaci BE vyčteme z druhých a pátých písmen indikátorů a permutaci CF ze třetích a šestých písmen indikátorů. Permutace AD, BE a CF proto známe, pokud se během jednoho dne podařilo zachytit dostatek zpráv.

Tak například během jednoho dne cvičení Wehrmachtu bylo zachyceno 64 zpráv s indikátory v následující tabulce. Z nich tedy můžeme vyčíst permutace (v cyklickém zápisu)

$$\begin{aligned} AD &= (\mathtt{a}), (\mathtt{s}), (\mathtt{bc}), (\mathtt{rw}), (\mathtt{dvpfkxgzyo}), (\mathtt{eijmunqlht}), \\ BE &= (\mathtt{axt}), (\mathtt{blfqveoum}), (\mathtt{cgy}), (\mathtt{d}), (\mathtt{hjpswizrn}), (\mathtt{k}), \\ CF &= (\mathtt{abviktjgfcqny}), (\mathtt{duzrehlxwpsmo}). \end{aligned}$$

1.	AUQ AMN	17.	KHB XJV	33.	RJL WPX	49.	VII PZK
2.	BNH CHL	18.	KHB XJV	34.	RFC WQQ	50.	VII PZK
3.	BCT CGJ	19.	LDR HDE	35.	SYX SCW	51.	VQZ PVR
4.	CIK BZT	20.	LDR HDE	36.	SYX SCW	52.	VQZ PVR
5.	DDB VDV	21.	MAW UXP	37.	SYX SCW	53.	WTM RAO
6.	EJP IPS	22.	MAW UXP	38.	SYX SCW	54.	WTM RAO
7.	GPB ZSV	23.	NXD QTU	39.	SYX SCW	55.	WTM RAO
8.	GPB ZSV	24.	NXD QTU	40.	SJM SPO	56.	WKI RKK
9.	HNO THD	25.	NLU QFZ	41.	SJM SPO	57.	XRS GNM
10.	HNO THD	26.	OBU DLZ	42.	SJM SPO	58.	XRS GNM
11.	HXV TTI	27.	PVJ FEG	43.	SUG SMF	59.	XOI GUK
12.	IKG JKF	28.	QGA LYB	44.	SUG SMF	60.	XYW GCP
13.	IKG JKF	29.	QGA LYB	45.	TMN EBY	61.	YPC OSQ
14.	IND JHU	30.	RJL WPX	46.	TMN EBY	62.	ZZY YRA
15.	JWF MIC	31.	RJL WPX	47.	TAA EXB	63.	ZEF YOC
16.	JWF MIC	32.	RJL WPX	48.	USE NWH	64.	ZSJ YWG

Permutacím AD, BE a CF Marian Rejewski říkal *charakteristiky dne*.

Dále si označíme neznámé permutace prováděné jednotlivými rotory odleva doprava L, M, N, neznámou permutaci prováděnou reflektorem R, (je $R^{-1} = R$, neboť R je tvořena třinácti cykly délky 2), neznámou permutaci prováděnou propojovací deskou S (také platí $S^{-1} = S$, protože S je tvořena šesti nebo deseti cykly délky 2 a zbývající cykly mají délku 1), a permutaci prováděnou propojením mezi propojovací deskou a vstupním kruhem jako V. Pokud by se pravý rotor neotáčel, platila by rovnost

$$A = SVNMLRL^{-1}M^{-1}N^{-1}V^{-1}S^{-1}.$$

Musíme ale pootáčení vzít v úvahu. Označíme si proto cyklickou permutaci

$$P = (\texttt{abcdefghijklmnopqrstuvwxyz}).$$

Pak, pokud odhlédneme od (nepříliš častého) pootáčení středního a levého rotoru, platí

$$\begin{aligned}
A &= SVP^{1}NP^{-1}MLRL^{-1}M^{-1}P^{1}N^{-1}P^{-1}V^{-1}S^{-1},\\
B &= SVP^{2}NP^{-2}MLRL^{-1}M^{-1}P^{2}N^{-1}P^{-2}V^{-1}S^{-1},\\
C &= SVP^{3}NP^{-3}MLRL^{-1}M^{-1}P^{3}N^{-1}P^{-3}V^{-1}S^{-1},\\
D &= SVP^{4}NP^{-4}MLRL^{-1}M^{-1}P^{4}N^{-1}P^{-4}V^{-1}S^{-1},\\
E &= SVP^{5}NP^{-5}MLRL^{-1}M^{-1}P^{5}N^{-1}P^{-5}V^{-1}S^{-1},
\end{aligned}$$

$$F = SVP^6NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}V^{-1}S^{-1}.$$

Pro složení permutací AD, BE a CF pak platí rovnosti

$$\begin{aligned} AD &= SVPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^3NP^{-4}MLRL^{-1}M^{-1} \\ &\quad P^4N^{-1}P^{-4}V^{-1}S^{-1}, \\ BE &= SVP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^3NP^{-5}MLRL^{-1}M^{-1} \\ &\quad P^5N^{-1}P^{-5}V^{-1}S^{-1}, \\ CF &= SVP^3NP^{-3}MLRL^{-1}M^{-1}P^3N^{-1}P^3NP^{-6}MLRL^{-1}M^{-1} \\ &\quad P^6N^{-1}P^{-6}V^{-1}S^{-1}. \end{aligned}$$

Z těchto permutací známe složení na levých stranách a cyklickou permutaci P. Ostatní permutace S, V, L, M, N, R jsou neznámé. Vyřešit tuto soustavu rovnic je velmi pravděpodobně nemožné i současnými prostředky. Na počátku třicátých let minulého století to zcela určitě nešlo. Bylo třeba ji nějakým způsobem zjednodušit.

První krok spočívá v substituci $Q = MLRL^{-1}M^{-1}$. Tak dostaneme soustavu

$$\begin{aligned} AD &= SVPNP^{-1}QPN^{-1}P^3NP^{-4}QP^4N^{-1}P^{-4}V^{-1}S^{-1}, \\ BE &= SVP^2NP^{-2}QP^2N^{-1}P^3NP^{-5}QP^5N^{-1}P^{-5}V^{-1}S^{-1}, \\ CF &= SVP^3NP^{-3}QP^3N^{-1}P^3NP^{-6}QP^6N^{-1}P^{-6}V^{-1}S^{-1}. \end{aligned}$$

Tato soustava o čtyřech neznámých permutacích S, V, N, Q je stále ještě neřešitelná.

Další krok zjednodušování je mnohem důležitější. Rejewski se snažil ze známých permutací AD, BE a CF získat všechny permutace A, B, C, D, E, F. Uvědomil si platnost následujícího tvrzení.

Věta 6.1 *Pokud dvě permutace na nějaké množině obsahují pouze cykly délky 2, pak jejich složení obsahuje vždy sudý počet cyklů jakékoliv délky.*

Důkaz. Označíme si obě permutace X, Y. Do sloupečků si napíšeme některé z dvojcyklů v obou permutacích. Jsou to ty dvojcykly, které ovlivňují cyklus ve složené permutaci XY obsahující prvek a_1:

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

Složení XY pak obsahuje jeden cyklus $(a_1, a_3, \ldots, a_{2k-3}, a_{2k-1})$ a druhý cyklus $(a_{2k}, a_{2k-2}, \ldots, a_4, a_2)$, oba mají stejnou délku k. Takto postupně vyčerpáme všechny prvky množiny, na které permutace působí. □

Je také dobré všimnout si, že

- prvky stejného cyklu délky 2 se ve složené permutaci XY objevují v různých cyklech stejné délky,
- pokud se dva prvky objevují ve složení XY ve dvou různých cyklech stejné délky a současně tvoří dvojcyklus v jedné z permutací X, Y, pak sousední dvojice prvků (levý a pravý v obou cyklech) také tvoří dvojcyklus v téže permutaci.

Druhá z vlastností vede okamžitě k důkazu opačného tvrzení.

Věta 6.2 *Pokud je v nějaké permutaci Z na množině obsahující sudý počet prvků vždy sudý počet cyklů libovolné délky, pak ji lze vyjádřit jako složení XY dvou permutací, z nichž každá obsahuje pouze cykly délky* 2.

Nás zajímá, jak tyto permutace najít. Vybereme-li dva cykly stejné délky k v permutaci Z, pak můžeme zvolit v permutaci X jako jeden cyklus délky 2 libovolnou dvojici prvků patřící do různých z těchto dvou cyklů. Ostatní cykly délky 2 v permutaci X obsahující prvky z těchto dvou cyklů jsou pak podle druhého z uvedených pozorování určené jednoznačně. Dva cykly délky 5 ve složené permutaci Z tak můžeme vyjádřit jako složení permutací složených z cyklů délky 2 celkem pěti způsoby. Podobně pro cykly dalších délek.

Tak například v případě zpráv zachycených během jednoho dne cvičení wehrmachtu můžeme permutaci A zvolit $2 \cdot 10 = 20$ způsoby a permutaci D pak jednoznačně dopočítáme ze vztahu $D = A(AD)$. Permutaci B můžeme zvolit $3 \cdot 9 = 27$ způsoby a permutaci C celkem 13 způsoby. Permutace E a F opět jednoznačně dopočítáme. Celkem tak bylo pro daný den, kdy se konaly manévry wehrmachtu, $20 \cdot 27 \cdot 13 = 7020$ možností pro permutace A, B, C, D, E, F. Jejich složení odpovídalo charakteristikám tohoto dne vyčteným z odposlechnutých zpráv.

Marian Rejewski si dále všimnul, že rozložení jednotlivých písmen v šifrových indikátorech odposlechnutých zpráv není vůbec rovnoměrné. To odpovídá tomu, že operátoři Enigmy nevolili hesla pro jednotlivé zprávy náhodně. Zaměřil proto svoji pozornost na podezřelé vzory v šifrových indikátorech. Ze zachycených indikátorů je nejpodezřelejší indikátor `SYX SCW`, který se opakuje pětkrát. Co kdyby si němečtí operátoři usnadňovali práci tak, že za klíč k jednotlivým zprávám často zvolili trojici opakujících se písmen? Co by to znamenalo pro permutace A, B, C, D, E, F, kdyby šifrový indikátor odpovídal otevřenému indikátoru `aaa`?

V permutaci A by potom musel být dvojcyklus (`as`), v permutaci B dvojcyklus (`ay`), v permutaci C tomuto předpokladu odpovídá dvojcyklus (`ax`), v permutaci D dvojcyklus (`as`), v permutaci E dvojcyklus (`ac`) a v permutaci F dvojcyklus (`aw`). Pro permutaci CF tak víme, že se rozkládá tak, že v permutaci C je dvojcyklus (`ax`) a v permutaci F je dvojcyklus (`aw`). Tím už dostaneme jednoznačně určené permutace

$$\begin{aligned} C &= \texttt{(ax)(bl)(vh)(ie)(kr)(tz)(ju)(gd)(fo)(cm)(qs)(np)(yw)}, \\ F &= \texttt{(xb)(lv)(hi)(ek)(rt)(zj)(ug)(df)(oc)(mq)(sn)(py)(wa)}. \end{aligned}$$

V permutaci BE leží prvky `y`, `c` také v témže cyklu, zatímco `a` leží v jiném cyklu stejné délky 3. To znamená, že v permutaci B by měly být dvojcykly (`ay`), (`xg`) a (`tc`) a v permutaci E by měly být dvojcykly (`yx`), (`gt`) a (`ca`). V permutaci AD jsou jediné dva cykly délky 1 cykly `a`, `s`, což dává jedinou možnost pro dvojcyklus `as` v obou permutacích A a D.

V permutaci C je jiný dvojcyklus `qs`. To napovídá, že šifrový indikátor `AUQ AMN` by mohl odpovídat otevřenému indikátoru typu `**s`. Protože A obsahuje dvojcyklus `as`, měl by být otevřený indikátor typu `s*s`. Typneme si, že šifrový indikátor `AUQ AMN` odpovídá otevřenému indikátoru `sss`. To znamená, že v permutaci B musí být rovněž dvojcyklus `su`. Tím z cyklů délky 9 v permutaci BE dostaneme zbývající dvojcykly v permutacích B, E:

$$\begin{aligned} B &= \texttt{(ay)(xg)(tc)(bj)(ln)(fh)(qr)(vz)(ei)(ow)(us)(mp)(dk)}, \\ E &= \texttt{(yx)(gt)(ca)(jl)(nf)(hq)(rv)(ze)(io)(wu)(sm)(pb)(kd)}. \end{aligned}$$

Další často frekventovaný šifrový indikátor je `RJL WPX`, který se vyskytuje čtyřikrát. Vzhledem k již objeveným permutacím B, C, E, F musí mít otevřený indikátor typ `*bb`. Pro permutaci A tak zbývají možnosti pro dvojcykly (`rb`) a (`rc`). Pravděpodobnější se zdá otevřený indikátor `bbb`, proto by měla permutace A obsahovat dvojcyklus (`br`) a D dvojcyklus (`rc`). Nakonec, abychom správně propojili dva cykly délky 10 v permutaci AD, použijeme šifrový indikátor `LDR HDE`. Z již zjištěné podoby permutací B, C, E, F

zjistíme typ odpovídajícího otevřeného indikátoru `*kk`. To opět napovídá stereotypní indikátor `kkk`, což znamená, že by A měla obsahovat dvojcyklus (`lk`) a D dvojcyklus (`kh`). Tím známe i permutace

$$\begin{aligned} A &= (\texttt{as})(\texttt{br})(\texttt{cw})(\texttt{di})(\texttt{ve})(\texttt{pt})(\texttt{fh})(\texttt{kl})(\texttt{xq})(\texttt{gn})(\texttt{zu})(\texttt{ym})(\texttt{oj}), \\ D &= (\texttt{sa})(\texttt{rc})(\texttt{wb})(\texttt{iv})(\texttt{ep})(\texttt{tf})(\texttt{hk})(\texttt{lx})(\texttt{qg})(\texttt{nz})(\texttt{uy})(\texttt{mo})(\texttt{jd}). \end{aligned}$$

Nyní se pokusíme ověřit, jestli takto zjištěné permutace A, B, C, D, E, F odpovídají zachyceným šifrovým indikátorům. A skutečně, dostaneme tak tabulku

```
AUQ AMN:  sss   IKG JKF:  ddd   QGA LYB:  xxx   VQZ PVR:  ert
BNH CHL:  rfv   IND JHU:  dfg   RJL WPX:  bbb   WTM RAO:  ccc
BCT CGJ:  rtz   JWF MIC:  ooo   RFC WQQ:  bnm   WKI RKK:  cde
CIK BZT:  wer   KHB XJV:  lll   SYX SCW:  aaa   XRS GNM:  qqq
DDB VDV:  ikl   LDR HDE:  kkk   SJM SPO:  abc   XOI GUK:  qwe
EJP IPS:  vbn   MAW UXP:  yyy   SUG SMF:  asd   XYW GCP:  qay
FBR KLE:  hjk   NXD QTU:  ggg   TMN EBY:  ppp   YPC OSQ:  mmm
GPB ZSV:  nml   NLU QFZ:  ghj   TAA EXB:  pyx   ZZY YRA:  uvw
HNO THD:  fff   OBU DLZ:  jjj   USE NWH:  zui   ZEF YOC:  uio
HXV TTI:  fgh   PVJ FEG:  tzu   VII PZK:  eee   ZSJ YWG:  uuu
```

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

Porovnáme-li zjištěné otevřené indikátory s klávesnicí přístroje Enigma, dojdeme k šokujícímu zjištění, že ze 40 použitých otevřených indikátorů pouze dva, tj. `abc` a `uvw` nejsou trojice sousedních kláves nebo dokonce trojice stejných písmen. Zdá se, že při procvičování komunikačního systému v době míru operátoři rychle něco ťukli levou rukou a pravou rukou si poznamenali výsledek. Nikdo z nich by si asi nedokázal představit, že toto nevinné přehrávání možného scénaře boje mohlo odhalit tolik tajemství Enigmy. Když na jaře roku 1933 předpisy striktně zakázaly používat v otevřených indikátorech opakovaná písmena, bylo už příliš pozdě.

A tak představa o zvycích operátorů spolu s Větou 6.2 umožnily zjednodušit soustavu tří rovnic o neznámých S, N, V, Q na soustavu šesti jednodušších rovnic o stejných neznámých.

$$\begin{aligned} A &= SVP^1NP^{-1}QP^1N^{-1}P^{-1}V^{-1}S^{-1} \\ B &= SVP^2NP^{-2}QP^2N^{-1}P^{-2}V^{-1}S^{-1} \end{aligned}$$

$$\begin{aligned} C &= SVP^3NP^{-3}QP^3N^{-1}P^{-3}V^{-1}S^{-1} \\ D &= SVP^4NP^{-4}QP^4N^{-1}P^{-4}V^{-1}S^{-1} \\ E &= SVP^5NP^{-5}QP^5N^{-1}P^{-5}V^{-1}S^{-1} \\ F &= SVP^6NP^{-6}QP^6N^{-1}P^{-6}V^{-1}S^{-1}. \end{aligned}$$

Ve skutečnosti nebyla Rejewského cesta k uvedeným rovnicím takto přímočará. Naopak obsahovala spoustu slepých uliček, zkoušení, hádání a ověřování.

Ani tato jednodušší soustava ale nevypadá příliš řešitelně. Kryptologům by ale velmi pomohlo, kdyby měli k dispozici dostatek šifrových zpráv z nějakého dalšího dne, kdy byly všechny tři rotory ve stejném základním nastavení. To vypadá fantasticky, neboť počet možných nastavení rotorů je $6 \cdot 26^3 = 105\,456$. Ve skutečnosti teorie pravděpodobnosti ale říká, že dva takové dny by se měly objevit v průběhu několika set dní. Takovou dvojici dní lze rozpoznat tak, že má stejné denní charakteristiky. Stejné charakteristiky ale nemusí znamenat stejné základní nastavení rotorů. Na druhou stranu, až do konce roku 1935 wehrmacht měnil základní nastavení rotorů jednou za tři měsíce, od počátku roku 1936 jenou za měsíc a teprve později jednou denně. Čekání by tak mohlo trvat opravdu dlouho.

Ve skutečnosti potřebná další data poskytnul opět agent *Asché*. V prosinci dostali polští kryptologové od francouzské tajné služby k dispozici denní klíče pro září a říjen roku 1932. To mimo jiné znamenalo znalost permutace S pro uvedené dny. Permutaci S tak bylo možné převést na levou stranu k již známým permutacím A, B, C, D, E, F. Rovnice tak už obsahovaly pouze tři neznámé permutace V, Q, N. Připomeňme, že N je permutace, kterou dělá pravý rotor a odpovídá tedy propojení drátů uvnitř tohoto rotoru.

$$\begin{aligned} S^{-1}AS &= VP^1NP^{-1}QP^1N^{-1}P^{-1}V^{-1} \\ S^{-1}BS &= VP^2NP^{-2}QP^2N^{-1}P^{-2}V^{-1} \\ S^{-1}CS &= VP^3NP^{-3}QP^3N^{-1}P^{-3}V^{-1} \\ S^{-1}DS &= VP^4NP^{-4}QP^4N^{-1}P^{-4}V^{-1} \\ S^{-1}ES &= VP^5NP^{-5}QP^5N^{-1}P^{-5}V^{-1} \\ S^{-1}FS &= VP^6NP^{-6}QP^6N^{-1}P^{-6}V^{-1}. \end{aligned}$$

V této chvíli přišel další ze skvělých nápadů Mariana Rejewského. Všimnul si, že kdyby také znal permutaci V, která byla dána vnitřní konstrukcí

přístroje – propojením mezi propojovací deskou a vstupním kruhem – uměl by už soustavu vyřešit pro zbývající dvě neznámé permutace N a Q. Znal by tak vnitřní propojení pravého rotoru. U komerční Enigmy bylo toto propojení mezi klávesnicí a vstupním kruhem dáno pořadím písmen na klávesnici přístroje, které bylo stejné jako u vojenské Enigmy. Kromě toho pořadí symbolů na kruzích po obvodu jednotlivých rotorů bylo stejné jako pořadí písmen v abecedě. Řekl si tedy, že německému smyslu pro řád by mělo odpovídat propojení z propojovací desky do vstupního kruhu tak, že jednotlivá písmena jsou ke vstupnímu okruhu připojena po obvodu podle abecedy. To znamená, že V je identická permutace. Rejewski tedy permutaci V prostě vynechal. Protože jeho další výpočty vedly ke správnému výsledku, tj. šifrové zprávy se postupně dařilo luštit, byl jeho předpoklad potvrzen jako správný.

V této souvislosti vyprávěl Rejewski o mnoho let později historku o tom, jak seznamoval spolu se svými kolegy v červenci roku 1939 příslušníky francouzských a britských tajných služeb se svými poznatky o Enigmě. V britské delegaci byl také Alfred Dilwyn Knox, přední kryptoanalytik ministerstva zahraničí, který se po řadu let bezvýsledně pokoušel odhalit permutaci V. Když se od Rejewského dozvěděl, jak jednoduché řešení jeho problém měl, tak se prý "rozzuřil".

Rejewskému tak zbyla soustava šesti rovnic o dvou neznámých N, Q, kterou si přepsal do podoby

$$\begin{aligned}
T &= P^{-1}S^{-1}ASP^{1} = NP^{-1}QP^{1}N^{-1},\\
U &= P^{-2}S^{-1}BSP^{2} = NP^{-2}QP^{2}N^{-1},\\
W &= P^{-3}S^{-1}CSP^{3} = NP^{-3}QP^{3}N^{-1},\\
X &= P^{-4}S^{-1}DSP^{4} = NP^{-4}QP^{4}N^{-1},\\
Y &= P^{-5}S^{-1}ESP^{5} = NP^{-5}QP^{5}N^{-1},\\
Z &= P^{-6}S^{-1}DSP^{6} = NP^{-6}QP^{6}N^{-1}.
\end{aligned}$$

Permutace T, U, W, X, Y, Z jsou známé.

Z nich odvodil rovnice

$$\begin{aligned}
TU &= NP^{-1}(QP^{-1}QP)PN^{-1},\\
UW &= NP^{-2}(QP^{-1}QP)P^{2}N^{-1},\\
WX &= NP^{-3}(QP^{-1}QP)P^{3}N^{-1},\\
XY &= NP^{-4}(QP^{-1}QP)P^{4}N^{-1},\\
YZ &= NP^{-5}(QP^{-1}QP)P^{5}N^{-1},
\end{aligned}$$

ze kterých vyloučil společný výraz $QP^{-1}QP$ a dostal tak čtyři rovnice pro jedinou neznámou $H = NPN^{-1}$

$$\begin{aligned} UW &= NP^{-1}N^{-1}(TU)NPN^{-1} = H^{-1}(TU)H, \\ WX &= NP^{-1}N^{-1}(UW)NPN^{-1} = H^{-1}(UW)H, \\ XY &= NP^{-1}N^{-1}(WX)NPN^{-1} = H^{-1}(WX)H, \\ YZ &= NP^{-1}N^{-1}(XY)NPN^{-1} = H^{-1}(XY)H. \end{aligned}$$

Tyto rovnice jsou všechny stejného tvaru

$$J = H^{-1}KH.$$

Toto je známá rovnice z teorie permutací. Splňují-li tři permutace tuto rovnici, říkáme, že permutace J a K jsou *konjugované*. Základní vlastnost konjugovaných permutací je popsána v následující větě.

Věta 6.3 *Dvě permutace (na téže množině) jsou konjugované právě když mají stejnou cyklickou strukturu, tj. stejný počet cyklů téže délky.*

Kdosi nadneseně nazval toto tvrzení *matematická věta, která vyhrála druhou světovou válku.* V každém případě důmyslná aplikace tohoto tvrzení z počátku 19. století zachránila bezpočet lidských životů. Někteří historici odhadují, že rozluštění Enigmy zkrátilo druhou světovou válku zhruba o tři roky.

Z věty o konjugovaných permutacích plyne, že první ze soustavy čtyř rovnic je řešitelná pro neznámou H právě tehdy, když mají obě permutace TU, UW stejnou cyklickou strukturu. Řešení může být mnoho. Ve skutečnosti mají všechny permutace TU, UW, WX, XY, YZ stejnou cyklickou strukturu, protože jsou všechny konjugované s jedinou permutací $QP^{-1}QP$. Každá rovnice zvlášť tak má řešení, musíme ale hledat společné řešení H všech rovnic. Navíc tvaru $H = NPN^{-1}$, tj. konjugované s cyklickou permutací P délky 26. Hledaná permutace H tak musí mít také jeden cyklus délky 26. Pokud by se nám takové společné řešení nepodařilo najít, tak jsme buď někde udělali chybu a nebo bylo denní nastavení kruhů takové, že se při šifrování šesti písmen indikátoru pootočil i prostřední rotor M.

V každém případě se polským kryptoanalytikům podařilo najít vnitřní propojení pravého rotoru N. A protože wehrmacht pravidelně měnil pořadí

rotorů, každý ze tří rotorů se často objevil jako pravý rychlý rotor, a navíc pouze šest z 26 možných nastavení kroužku na obvodu pravého rotoru zapříčinilo to, že se během šifrování indikátoru zprávy pohnul i prostřední rotor. Byla tak pravděpodobnost větší než 75%, že se podaří stejným způsobem odhalit vnitřní propojení každého ze tří rotorů během dne, kdy byl podle denního klíče na pravém místě, a kdy se podařilo zachytit dostatek šifrových zpráv, aby bylo možné spočítat denní charakteristiky AD, BE a CF. A nakonec také vnitřní propojení reflektoru.

A tak se podařilo polským kryptoanalytikům sestrojit kopii vojenské Enigmy používané wehrmachtem už na počátku 30. let minulého století. Pomocí této kopie se jim dařilo luštit německé šifrové zprávy tak, že během 10-20 minut odhalili denní klíč, a poté mohli najít snadno indikátor každé zprávy a rozluštit ji prakticky stejně rychle, jako její dešifrování trvalo německé obsluze na straně adresáta.

Sestrojení kopie Enigmy pouze na základě zachycených šifrových zpráv a pomocí informací od agenta *Asché* je naprosto mimořádným úspěchem v historii kryptoanalýzy.

Dne 15. srpna 1938 Němci změnili šifrovací proceduru, místo šesti propojovacích kabelů jich začali používat 10. A od 15. prosince 1938 začali používat pět rotorů místo tří. Naneštěstí pro polskou tajnou službu se v té době také natrvalo odmlčel agent *Asché*. Život mu to ale nezachránilo. Byl odhalen a roku 1943 popraven.

Naopak štěstí měla polská tajná služba v tom, že německá *Sicherheitsdienst* sice začala používat nové rotory, nezměnila ale šifrovací proceduru. Proto mohli Poláci stejnou metodou rychle odhalit vnitřní propojení nových rotorů.

Přípravy na válku vrcholily a tak se polská tajná služba rozhodla již dále neskrývat, že má kopie Enigmy a velké množství německých šifrových zpráv a jim odpovídajících otevřených zpráv. Pozvala v červenci roku 1939 zástupce francouzských a britských tajných služeb do Varšavy, kde jim předala veškeré informace o Enigmě, které za dlouhá léta nashromáždila. To byla ta schůzka, na které se Alfred Dillwyn Knox rozzuřil.

Britská tajná služba si ze schůzky odnesla hlavní poučení—potřebuje najmout matematiky. A tak po vyhlášení války Německu dne 2. září 1939 nastoupil dne 4. září do britské tajné služby také Alan Turing, který postupy polských matematiků prohloubil a dovedl k dokonalosti. To už je ale jiná historie. Turing mnoho získal ze studia rozluštěných zpráv, které dostala britská tajná služba od polských kolegů.

Marian Rejewski po přepadení Polska počátkem září 1939 spolu se svými dvěma matematickými kolegy uprchnul přes Rumunsko do Francie a po její

porážce přešel do Španělska. Tam byl uvězněn a později vydán do Anglie. Britská tajná služba jej ale k luštění Enigmy nepustila a pověřila jej jinými úkoly. Měla k tomu své důvody. Nechtěla, aby kdokoliv další věděl, jak moc umí německé šifrové zprávy luštit. Důvod k utajování měla i po skončení druhé světové války. Jako válečnou kořist získala několik tisíc přístrojů Enigma a britská koloniální správa je začala používat v koloniích. Po jejich osamostatnění je začaly používat nezávislé vlády bývalých kolonií, a tak byla britská tajná služba i nadále v obraze.

Teprve v roce 1967 byly zveřejněny první informace o britsko-americké operaci ULTRA, která spočívala v luštění nepřátelských šifrových zpráv (německých, japonských, italských, atd.) a současně v zakrývání této skutečnosti před nepřítelem. A tak se Rejewski, který žil v izolaci ve Varšavě, postupně začal dozvídat, jak moc britská tajná služba těžila z výsledků jeho práce a práce jeho kolegů. Začal potom také o svém přínosu více hovořit. Většinu informací v této přednášce jsem čerpal z jeho článku *An application of the theory of permutations in breaking the Enigma cipher*, která vyšla v polském časopise *Applicaciones Mathematicae*, vol. 16, No. 4 v roce 1980, v roce, kdy Rejewski ve věku 75 let zemřel.