Lengyelek az Enigma ellen

Készítették:
Mérai László alkalmazott matematikus szak IV. évfolyam, ELTE TTK
és Kékesi Júlia óvodapedagógus szak III. évfolyam, ELTE TÓFK

Témavezető:
Dr. Szabó Csaba, egyetemi docens,
ELTE TTK, Algebra és Számelmélet Tanszék

Dolgozatunk témája az Enigma története, és működésének matematikai modellje. Az Enigma egy német írástitkosító-gépezet, melyet a két világháború között fejlesztettek ki. Története különösen érdekes azért, mert miután a lengyelek kezére jutott néhány rejtjelezett szöveg, ezek megfejtéséhez, először a történelem folyamán, matematikusok segítségét is igénybe vették.

Az Enigmával kapcsolatos információk a hetvenes évekig titkosak voltak. Rejewskinek 1980-ban jelenhettek meg a témáról írt cikkei, jegyzetei. Rejewski, Zygalski és Rúzycki az Enigma feltöréséért 2000-ben poszthumusz kitüntetést kaptak a Lengyel Államtól.

A kevés eredeti forrás alapján sokan próbálkoztak az Enigma problémájának matematikai formába öntésével, közöttük Simon Singh, a CNN tudományos riportere is, ám egyik kísérlet sem tekinthető pontosnak. Singh például a pontosság helyett inkább a népszerűségre törekszik. Dolgozatunkban matematikailag korrekt formában ismertettük az Enigma problémáját.

Munkánkat történeti áttekintéssel kezdtük, melyet a konkrét matematikai modellek leírása és megoldása követ.

Történeti áttekintés az Enigmáról

A két világháború közötti években, 1928-tól, a német hadsereg (a Wehrmacht) katonai célokra elkezdett tesztelni egy új titkosírási rendszert, és ez pánikot keltett a lengyel titkosszolgálat embereinek körében. Ahogy '20-as években a német hadsereg egyre erősödött, úgy vált számára egyre fontosabbá a kommunikáció biztonságának megteremtése. Mivel a rádiós üzenetek könnyedén lehallgathatók, az üzenetek rejtjelezésével kívánták elérni, hogy az ellenség ne férhessen hozzá az információkhoz. A húszas évek utolsó időszakában a katonai készülődés fokozódott, és ezzel a rejtjelezett üzenetek száma megtöbbszöröződött.

Az első világháború végét követően Franciaország és Nagy-Britannia úgy gondolta, Németország többé már nem fenyegeti biztonságukat, ám Lengyelország nem osztotta ezt a nézetet. A lengyelek már az első világháború befejezésétől is lehallgatták, és megfejtették a német üzeneteket. 1928-ban azonban rájöttek, hogy a németek gépi titkosításra váltottak, mivel az addig alkalmazott módszerek, így a karakterek előfordulási gyakoriságának vizsgálata, nem vezettek eredményre.[5]

A lengyelek, nyugati mintára, létrehozták saját, titkosírással foglalkozó szervezetüket, a Biuro Szyfrów-t. Ezt az irodát bízták meg az új titkosírás tanulmányozásával.

Számos éven át minden, a titkosírás megfejtésére irányuló próbálkozás sikertelennek bizonyult. A lengyelek, végső elkeseredésükben, még látnokok bevonásával is kísérleteztek. Mindhiába. Végül Maksymilian Ciezkinek, a Lengyel Titkosszolgálat századosának, az az ötlete támadt, hogy a megoldás talán a matematikusok kezében lehet. A poznani egyetemen ezért új tárgyat indítottak a matematikus hallgatóknak, kriptoanalízis elnevezéssel. Ez a választás nem nevezhető önkényesnek, mivel Poznan városa a lengyel-német határvonalhoz közel fekszik. Az itt tanuló diákok többsége beszélte a német nyelvet, valamint ismeretekkel rendelkezett a német gondolkodásmódról, így nagyobb eséllyel kezdhettek neki a titkosírás megfejtésének.

A kurzus három legkiemelkedőbb diákjának, **Marian Rejewski** (1905 – 1980), **Jerzy Rúzycki** (1907 – 1942), és **Henryk Zygalski** (1906 – 1978) hallgatóknak felajánlották, hogy az új titkosírással foglalkozzanak.

Jerzy Rúzycki

Marian Rejewski

Henryk Zygalski

Munkásságuknak köszönhetően a második világháború évekkel korábban véget érhetett, hiszen a németek legtöbb szigorúan titkos üzenetét az ellentábor el tudta olvasni.[5], [6]

Ahhoz, hogy az új, gépi titkosírás feltörésének folyamata érthető legyen, nézzük először, a titkosírások általános jellemzőit:

A küldő és a fogadó között egy adott szöveg mások számára nem érthető formába kódolva áramlik. Ehhez a küldő az üzenetet egy kulcs és egy algoritmus segítségével titkosítja. A kulcs az az információ, melynek birtokában egyértelműen megfejthető a

titkosított szöveg. A fogadó fél tudja a kulcsot és az algoritmust, így képes előállítani az eredeti üzenetet a rejtjelezett szövegből.

Lássunk erre egy egyszerű példát.

Julius Ceasar a szenátus tagjaival, és a római sereg vezérével a következő rejtjelezés segítségével váltott üzenetet: A szöveg minden betűjét az ábécében rá következő harmadik betűvel helyettesítette. Például a „menj” szót „phqk”-nak kódolta volna. (Az "m" helyett az utána következő harmadik betűt, a „p”-t írta le, és így tovább.) Ennél a fajta titkosírásnál a kulcs azt mondja meg, hogy hány hellyel kell eltolni a betűket az ábécé sorrendjében, jelen esetben ez három.

Előfordulhat, hogy az ellenség elfogja a kódolt szöveget, és megpróbálja megfejteni, azaz feltörni a kódot. A fenti példában a feltörés azt jelenti, hogy megfejtjük, hány hellyel kell eltolni a betűket. Látható, hogy Ceasar rejtjelezett szövegeit kevés próbálgatással kikódolhatjuk. Az ehhez hasonló, de összetettebb titkosírásokat a nyelvészek a betűk gyakoriságának megfigyelésén alapuló módszerekkel fejthetik meg.

A titkosírási rendszer biztonsága elsősorban a kulcs átjuttatási módjától függ, tehát attól, hogy a küldő és a fogadó hogyan cseréli ki egymással az üzenet kulcsát. Ehhez előzetesen megegyeznek, hogy a kódolt szöveg mely része fog információt tartalmazni az üzenet kulcsáról. Ezt az információt **indikátor**nak nevezzük. Az indikátor leggyakrabban a rejtjelezett szöveg elején található. Általában nem része az eredeti (kódolatlan) üzenetnek, ám maga az indikátor is titkosítva van.

Térjünk most vissza az Enigmához.

Változatos statisztikai tesztek alkalmazásával világossá vált, hogy a szöveg első hat betűje adja az indikátort. A statisztikai tesztek azt is sugallták, hogy a titkosírás nagy valószínűséggel polialfabetikus.[3] Ez azt jelenti, hogy az eredeti szöveg összes betűjét egyszerű megfeleltetéssel egy másik betűre cserélik. Szemben Ceasar módszerével,a rejtjelezett betű itt az eredeti betű szövegben elfoglalt helyétől is függ.

Arthur Scherbius német feltaláló 1918-ban szabadalmaztatta az Enigmát, mely egy üzleti célokra kifejlesztett rejtjelező szerkezet. Ezt a gépet 1926-ban hozták kereskedelmi forgalomba. A lengyel titkosszolgálat arra a következtetésre jutott, hogy az új titkosírás az Enigma katonai változatától származik.[6]

A katonai Enigma felépítése

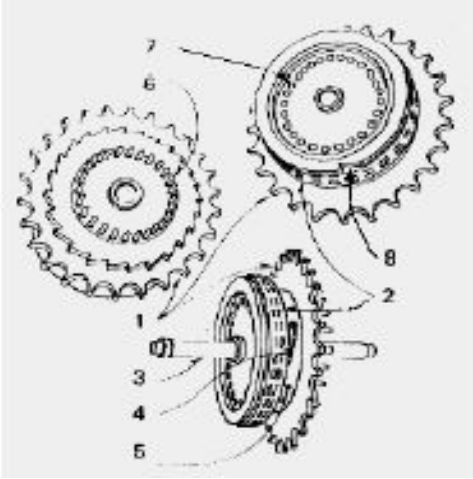
A szerkezet fontosabb részei a következők: [3], [6]

- billentyűzet
- kijelző
- kapcsolótábla
- keverő-berendezés
- keverőtárcsa
- visszafordító

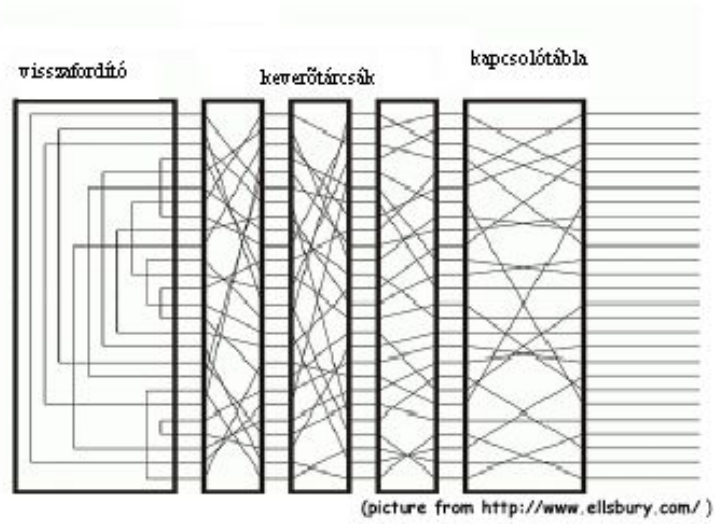
A keverőtárcsák struktúrája: [3], [6]

1. lánckerék
2. ábécés gyűrű
3. tengely
4. retesz
5. kábeltartó
6. – 7. érintkezőpár

8. továbbító horony



Az Enigma belső szerkezetének sematikus rajza: [3]



Az Enigma működése

Mielőtt az Enigma működésére térnénk, foglaljuk össze, hogy milyen biztonsági követelmények támaszthatók a rejtjelezéssel szemben.

A titkosírás alapelvei a következők:

1. Kerülni kell ugyanannak a kulcsnak a használatát különböző szövegek kódolásakor.
2. Kerülni kell továbbá ugyanannak a szövegnek két különböző kulccsal való kódolását.
3. Feltételezni kell, hogy az ellenség tudja a bekódolási algoritmust.
4. Nem szabad az ellenséget alábecsülni.

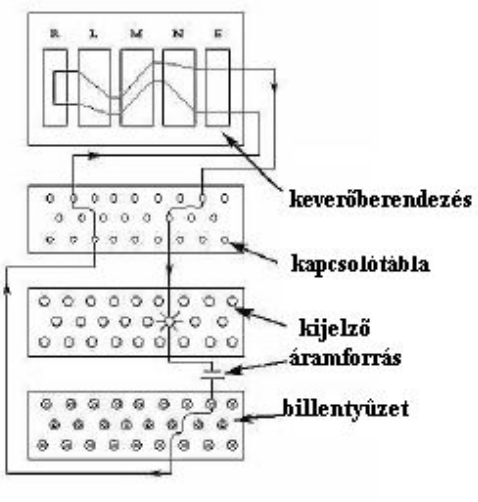
Az első két elvben megfogalmazottak azért lényegesek, mert megszegésükkor olyan információt nyerhetünk a kulcsról, mely annak megfejtésében segít.

Most vázoljuk, hogy mi történik az Enigmában egy billentyű lenyomását követően. A lenyomás után az áram keresztülfolyik a kapcsolótáblán. A kapcsolótábla olyan dugaszolótábla, mellyel a feladó felcserélhet bizonyos betűket. Ha például a kapcsolótáblán összekötik az a-t és a b-t, és a kezelő leüti a b billentyűt, akkor az elektromos jel azon az úton halad tovább, amin eddig az a betű pályája volt, és fordítva.

A kapcsolótábla után a három keverőtárcsán halad keresztül a jel. Ezek egymástól függetlenül permutálják a betűket. Ezek után a visszafordító a beérkezett jelet visszaküldi, egy más útvonalon, a kijelzőhöz.

Az első keverőtárcsa minden billentyű leütése után fordul egy betű helynyit. Miután ez a keverőtárcsa megtett egy teljes fordulatot, a második keverő is egy betű helynyit fordul. Hasonlóan működik ez a harmadik tárcsa esetében is. Ráadásul a keverőtárcsák kézzel manipulálhatók, azaz kicserélhetőek egymással, illetve tetszőleges helyre forgathatóak. [3]

A következő ábra mutatja, hogyan folyik keresztül az áram az Enigmán egy billentyű lenyomását követően:



A használati utasítás

A ’30-as évek elején a pénzügyi gondokkal küszködő Hans-Thilo Schmidt az Enigma titkának áruba bocsátásával próbált pénzhez jutni. Schmidt bátyja révén az Enigma parancsnokságára került, ahol szigorúan bizalmas információkhoz juthatott. 1931-ben Belgiumba utazott, hogy kapcsolatba lépjen egy Rex fedőnevű francia hírszerzővel. Schmidt átadott neki két olyan fotót, melyeken a használati utasítás volt látható, illetve utalásokat tartalmaztak az Enigma huzalozásáról. Az első találkozót követően hét évig szolgált információkkal. Minden találkozóra magával vitt egy vagy több kódkönyvet, melyek egy-egy negyedévre tartalmazták a napi kódokat. Mivel Franciaország nem tartotta lényegesnek a kapott információkat, egy korábbi együttműködési szerződés alapján átadta ezeket a lengyel hírszerzésnek. [6]

A napi kód határozza meg, hogy adott napon az operátoroknak milyen követelmények alapján kell a gépet beállítaniuk. A nap folyamán tehát minden használatban lévő Enigma beállításai azonosak. A napi kód a következő részekből áll [6]:

1. a keverőtárcsák sorrendje, pl.: II,III,I;
2. az ábécés gyűrűk állása, pl.: K,U,B;
3. a kapcsolótábla érintkezései, pl.: AU,CR,DK,JZ,LN,PS.

Az első pont rögzítette, hogy milyen sorrendben kell a tárcsákat a gépbe tenni. Példánkban az első helyen a II-es számú, a második helyen a III-as, a harmadik helyen pedig az I-es számmal jelölt tárcsa áll.

A következő pont az egyes tárcsák helyzetét határozza meg. A tárcsákra sorrendben fel vannak írva az ábécé betűi (ábécés gyűrű). Az operátor úgy forgatja a tárcsát, hogy a napi kód által megadott betűt lássa a fölötte található kis ablakban.

Az utolsó pont pedig azt határozza meg, hogy a kapcsolótáblán mely betűpárokat kell összekötni.

A napi kódokat negyedévente egy füzetbe leírva juttatták el az operátorokhoz.

Az Enigma használata

Az operátor, miután a napi kódnak megfelelően beállította az Enigmát, véletlenszerűen kiválasztott három betűt pl.: HTS. Ezt nevezzük üzenetkódnak. Az operátor kétszer egymás után leírta ezt az üzenetkódot pl.: HTS HTS. Ezután bekódolta ezt a hat karaktert a hat megfelelő billentyű lenyomásával, és lejegyezte a kijelzett betűket. Ezáltal megkapta az üzenetkód (HTS HTS) rejtjelezett változatát (NEW GWY), vagyis az indikátort. Ezt követően úgy fordította a keverőtárcsákat, hogy a kis ablakban az általa választott három betű jelenjen meg. Így például a HELLO üzenet kódolva BPTQS lett. [6]

Az Enigmát katonai célokra, háborús helyzetben használták, ahol számolni kellett a rádiós adás zavarásával, vagyis szükségszerű volt kétszer elküldeni az üzenetkód kódolt változatát. A németek számoltak az emberi tényezővel is, ezért kellett az operátornak az üzenetkódot két különböző módon bekódolnia. Ha ugyanis az egyszer kódolt üzenetkódot küldte volna el kétszer, akkor nem derülhetett volna ki, ha félregépelte azt.

A titkosírás alapelveinek megszegése

Az előbbi példával élve, ha az eredeti üzenet HELLO, akkor a teljes kódolt üzenet NEV GWY BPTQS. Ebben az esetben két alapelv is sérült. Egyrészt adott napon minden üzenetkód azonos napi kód segítségével kódoltatott be. Másrészt minden egyes üzenetkódot kétszer kódoltak be különböző kulccsal. Ennek a két alapelvnek az áthágása volt a kiindulópont az Enigma feltöréséhez.

Az Enigma feltörésének kezdetei

Összegezzük azokat az információkat melyek Marian Rejewski rendelkezésére álltak 1932 decemberében: Birtokában volt az Enigma kereskedelemben kapható változatának (a kapcsolótábla nélkül, és más fajta keverőtárcsával, valamint visszafordítóval); a használati utasításnak; 1932 szeptemberére és októberére vonatkozó napi kódoknak. A Rejewski rendelkezésére álló napi kódok az év két különböző negyedévéből származtak, és sok elkapott kódolt üzenete volt az év más hónapjaiból is.

A keverőtárcsák, a visszafordító és a keverő-berendezés matematikai modellje

Elöljáróban álljon itt egy definíció:

Definíció: Egy H halmaz $P: H \to H$ bijektív függvényét **permutáció**nak nevezzük. Két ilyen függvény kompozíciójaként definiálhatjuk a két permutáció szorzatát (jegyezzük meg, hogy a kompozíció számítási szabályai miatt itt a szorzás jobbról balra végzendő). Mivel ezek a permutációk bijektív függvények, ezért értelmezhető az inverzük, mely szintén permutáció.

Vegyünk néhány egyszerű példát.

1. Az óvodások torna foglalkozáson tetszőleges sorrendben sorban állnak. Az a feladatuk, hogy nagyság szerint sorakozzanak. Ekkor tulajdonképpen a következő permutációt hajtják végre: az első helyhez hozzárendelik a legmagasabb, a második helyhez a második

legmagasabb, az utolsó helyhez a legalacsonyabb gyermeket, és ennek megfelelően helyet cserélnek.

2. Egy játékos kártyát kever. Ekkor valójában megpermutálja a kártyalapokat, azaz megváltoztatja eredeti sorrendjüket. Ha ismerjük az eredeti sorrendet, és figyeljük, hogy a keverő milyen permutációkat, hányszor, és milyen sorrendben hajt végre, következtethetünk a lapeloszlásra.

3. Az Enigma a kódolandó szöveg minden betűjét egy másik betűre cseréli, azaz a szöveg karakterein permutációt hajt végre.

Továbbiakban azt a speciális esetet vizsgáljuk, amikor $H=\{a,b,c,d...y,z\}$. Ekkor egy permutáció minden H-beli betűhöz egyértelműen rendel egy H-beli betűt. A permutációk egy egyszerű fajtáját ciklikus permutációknak nevezzük. Egy ilyen ciklikus permutáció például az (a,b,c,d) ciklus, mely az a-hoz a b-t, b-hez a c-t, c-hez a d-t, d-hez az a-t rendeli. Bizonyítható, hogy minden permutáció megkapható olyan ciklikus permutációk szorzataként, melyeknek nincs közös elemük.

Meg akarjuk határozni a keverőtárcsák által leírt permutációkat. Jelöljük ezeket L, M és N-nel. Hasonlóképpen szeretnénk leírni a visszafordítót, ezt R-rel jelöljük. Ekkor az R permutáció nem lehet tetszőleges, 13 csere szorzataként áll elő.

Ezek segítségével a keverő-berendezés permutációja is leírható:

$$N^{-1}M^{-1}L^{-1}RLMN$$

Fontos megjegyezni, hogy e négy permutáció egyike sem volt ismert Rejewski előtt.
Ez a modell még nem veszi figyelembe a keverőtárcsák forgását. Ennek korrigálása érdekében bevezetjük a $P := (abc...xyz)$ permutációt. (Mely az a-t a b-be, b-t a c-be, és így tovább, végül y-t a z-be és z-t az a-ba viszi.) Így a keverő-berendezés teljes modelljét kapjuk:

$$P^{-1}N^{-1}PM^{-1}L^{-1}RLMP^{-1}NP$$

Elképzelhetőnek tartották, hogy a keverőtárcsák és a kapcsolótábla között van még egy keverő (ma már tudjuk, hogy nem volt ott). Ennek a permutációját H-val jelöljük. S-sel jelölve a kapcsolótábla permutációját, megkapjuk az Enigma teljes matematikai modelljét:

$$S^{-1}H^{-1}P^{-1}N^{-1}PM^{-1}L^{-1}RLMP^{-1}NPHS$$

Jegyezzük meg, hogy ez az *S* permutáció a napi kód függvényében minden nap változik.

Minden ugyanaznap közvetített üzenet első hat karaktere azonos módon kódoltatott be, a gép napi beállításától függően. *A*-val jelöljük az üzenetek első karakterének permutációját, adott nap során. Hasonlóan definiálhatjuk a *B*-t a második *C*-t, a harmadik, *D*-t, *E*-t, *F*-et a negyedik, ötödik, hatodik karakterek permutációjaként. Mind a hat permutáció ismeretlen volt. Ezeket hívták a nap permutációinak. A fentiek alapján az Enigma teljes modelljére egy másik leírást is kapunk:

$$A = S^{-1}H^{-1}P^{-1}N^{-1}PM^{-1}L^{-1}RLMP^{-1}NPHS$$

Hasonlóan kapunk egy kifejezést a második betű permutációjára vonatkozóan. Azonban figyelembe kell vennünk, hogy a második billentyű lenyomása után a jobboldali keverőtárcsa már másodjára fordult egy betű helynyit. Így megkapjuk a következő egyenletet.

$$B = S^{-1}H^{-1}P^{-2}N^{-1}P^{2}M^{-1}L^{-1}RLMP^{-2}NP^{2}HS$$

Ugyanezzel a módszerrel a fennmaradó négy permutációt is hasonlóan kifejezhetjük:

$$C = S^{-1}H^{-1}P^{-3}N^{-1}P^{3}M^{-1}L^{-1}RLMP^{-3}NP^{3}HS$$
$$D = S^{-1}H^{-1}P^{-4}N^{-1}P^{4}M^{-1}L^{-1}RLMP^{-4}NP^{4}HS$$
$$E = S^{-1}H^{-1}P^{-5}N^{-1}P^{5}M^{-1}L^{-1}RLMP^{-5}NP^{5}HS$$
$$F = S^{-1}H^{-1}P^{-6}N^{-1}P^{6}M^{-1}L^{-1}RLMP^{-6}NP^{6}HS$$

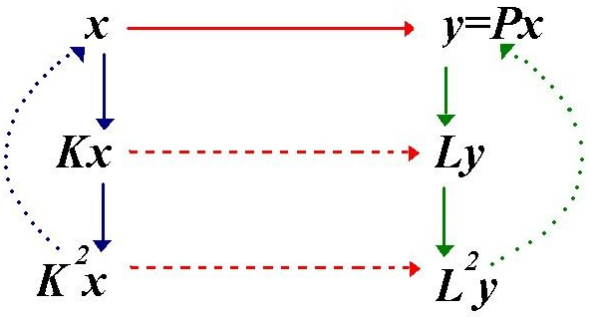
P kivételével az összes permutáció ismeretlen volt Rejewski számára. Van azonban egy fontos tényező, amit tudott róluk.

Ezek részletezése előtt álljon itt egy definíció és egy tétel:

Definíció: *K* és *L* permutáció akkor konjugált, ha létezik olyan V, hogy $K = V^{-1}LV$.

1. Tétel: Két permutáció pontosan akkor konjugált, ha ciklikus struktúrájuk megegyezik, azaz a ciklikus felbontásukban minden hosszúságú ciklusból megegyező számú van.

Bizonyítás: Először tegyük fel, hogy K és L konjugáltak. Szeretnénk belátni, hogy ciklikus felbontásuk megegyezik. Ehhez válaszunk egy tetszőleges $x \in X$ elemet, és tekintsük meg a következő ábrát.



Látható, hogy P a K minden ciklusát az L ciklusába viszi.

A másik irányhoz konstruálunk egy olyan V permutációt, mely kielégíti a $K = V^{-1}LV$ egyenletet. Válasszunk két megegyező hosszúságú ciklust K és L ciklikus felbontásából. Válasszunk ki egy $x \in X$ elemet a K és egy $y \in X$ elemet az L kiválasztott ciklusaiból. Definiáljuk V -t a következő módon: $Vx := y$. Ekkor a $VK = LV$ miatt

$$VK^i x = L^i V x = L^i y$$

ahol $i \in \{1, 2, 3, ..., 26\}$

A tétel figyelembe vételével vizsgálhatjuk a $K = V^{-1}LV$ egyenlet megoldását, ahol K és L ismert. Ha K és L ciklikus struktúrája megegyezik, akkor van megoldás. Vegyük észre azonban, hogy ha V_0 kielégíti az egyenletet és $LZ = ZL$ akkor $V_0 Z$ is megoldás. A megoldás kizárólag $V_0 Z$ alakú lehet. Ilyen V_0 -t könnyen konstruálhatunk a tétel bizonyításában szereplő módon.

Ezek után visszatérhetünk az egyenletek vizsgálatához. Tudjuk, hogy az R permutáció diszjunkt cserék szorzata, így $R^2 = I$, azaz $R^{-1} = R$. Mivel az A, B, C, D, E és F mind konjugáltak az R -rel, így megkapjuk, hogy

$$A^2 = B^2 = C^2 = D^2 = E^2 = F^2 = I$$

Mind a hat permutáció megegyezik az inverzével.

A fentieket még nem ismerték, de a *DA, EB, FC* permutációkat igen. Rejewski ezeket hívta a nap karakterisztikájának.

A szorzatokat a következőképpen kaphatjuk meg: Tudjuk, hogy az indikátor kétszer tartalmazza a rejtjelezett üzenetkódot. Jelöljük *xyz* -vel a véletlenszerűen választott üzenetkódot. Ekkor az indikátor az *xyzxyz* rejtjelezett formája. Ha ennek első betűje u és negyedik betűje v , akkor a definíció szerint $Ax = u$ és

$Dx = v$, így $DAu = v$, mivel $A^{-1} = A$. Amennyiben elég üzenetet kapunk el egy adott nap során, ismertté válnak a DA, EB, FC permutációk.

Az első indikátorból megkaphatjuk például, hogy

$$DAa = a\,,\ EBu = m\,,\ FCq = n\,.$$

Hasonlóan a másodikból adódik:

$$DAb = c\,,\ EBn = h\,,\ FCh = l\,.$$

Így előállnak a karakterisztikák:

$$DA = (a),(s),(bc),(rw),(dvpfkxgzyo),(eijmunqlht)\,,$$
$$EB = (axt),(blfqveoum),(cgy),(d),(hjpswizrn),(k)\,,$$
$$FC = (abviktjgfcqny),(duzrehlxwpsmo)\,.$$

Ha összevetjük az *A, B, C, D, E* és *F* permutációkra korábban felírt egyenleteket, akkor a következőket kapjuk: (A bal oldalon szereplő kifejezések már ismertek.)

$$DA = S^{-1}H^{-1}P^{-4}N^{-1}P^{4}M^{-1}L^{-1}RLMP^{-4}NP^{3}N^{-1}PM^{-1}L^{-1}RLMP^{-1}NPHS$$
$$EB = S^{-1}H^{-1}P^{-5}N^{-1}P^{5}M^{-1}L^{-1}RLMP^{-5}NP^{3}N^{-1}P^{2}M^{-1}L^{-1}RLMP^{-2}NP^{2}HS$$
$$FC = S^{-1}H^{-1}P^{-6}N^{-1}P^{6}M^{-1}L^{-1}RLMP^{-6}NP^{3}N^{-1}P^{3}M^{-1}L^{-1}RLMP^{-3}NP^{3}HS$$

Ez az egyenletrendszer még biztosan megoldhatatlan a keverőtárcsák és a visszafordító szerkezetének ismerete nélkül. A rendszert formálisan egyszerűsíthetjük, ha bevezetjük a $Q := M^{-1}L^{-1}RLM$ jelölést.

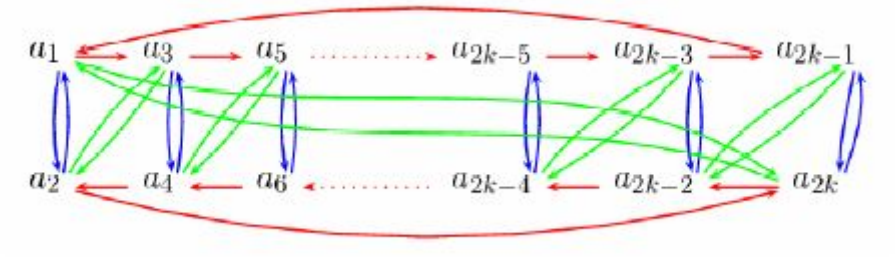
$$DA = S^{-1}H^{-1}P^{-4}N^{-1}P^{4}M^{-1}L^{-1}RLMP^{-4}NP^{3}N^{-1}PM^{-1}L^{-1}RLMP^{-1}NPHS$$
$$EB = S^{-1}H^{-1}P^{-5}N^{-1}P^{5}QP^{-5}NP^{3}N^{-1}P^{2}QP^{-2}NP^{2}HS$$
$$FC = S^{-1}H^{-1}P^{-6}N^{-1}P^{6}QP^{-6}NP^{3}N^{-1}P^{3}QP^{-3}NP^{3}HS$$

Ezt továbbra sem tudjuk megoldani, mivel *R* illetve *Q* ismeretlen. Az egyenletrendszer további egyszerűsödése elengedhetetlen.

Az egyszerűsítéshez Rejewski bebizonyította a következő tételt:

2.TÉTEL: Egy *K* permutáció kifejezhető két, a ciklusfelbontásukban csak cseréket tartalmazó *X, Y* szorzataként, pontosan akkor, ha *K* ciklusfelbontásában minden hosszúságú ciklusból páros sok van.

BIZONYÍTÁS: Tegyük fel, hogy K kielégíti a tételben szereplő feltételt, továbbá, hogy K az $(a_1a_3...a_{2k-3}a_{2k-1})$ illetve az $(a_2a_{2k}a_{2k-4}...a_4)$ két darab k hosszúságú ciklus szorzata. Kiköthetjük, hogy X tartalmazza az (a_1a_2) cserét. Mivel azt szeretnénk, hogy $K = YX$ teljesüljön, Y -nak tartalmaznia kell az (a_2a_3) ciklust. Hasonlóan X-nek (a_3a_4) -et, és így tovább. Itt X és Y kizárólag a_1 és a_2 kiválasztásától függ, így összesen k -féle felbontás létezik.



A másik irány bizonyításához tegyük fel, hogy $K = YX$ és mind X, mind Y cserék szorzataként áll elő. Tekintsük az X (a_1a_2) cseréjét, és vizsgáljuk meg, hogy mi lesz az a_1, illetve az a_2 elemeket tartalmazó ciklusok hossza. Nézzük az ábrát. Látható, hogy ezeket az elemeket a megegyező hosszú $(a_1a_3...a_{2k-3}a_{2k-1})$ és $(a_2a_{2k}a_{2k-4}...a_4)$ ciklusok tartalmazzák. Így adódik, hogy minden hosszúságú ciklusból páros sok lesz a szorzatban.

Ezt a tételt alkalmazhatjuk az előbbi példára:

$$DA = (a),(s),(bc),(rw),(dvpfkxgzyo),(eijmunqlht),$$
$$EB = (axt),(blfqveoum),(cgy),(d),(hjpswizrn),(k),$$
$$FC = (abviktjgfcqny),(duzrehlxwpsmo).$$

Ekkor 13 lehetséges C és F, 3x9 lehetséges B és E, illetve 2x10 lehetséges A és F permutáció létezik. Ezeket összegezve 20x27x13=7020 az összes lehetőség száma, adott nap folyamán. [3]

Rejewski, hogy csökkentse ezt a számot, pszichikai tényezőket vett figyelembe. Mialatt az elkapott üzenetek indikátorait tanulmányozta, észrevette, hogy sok közülük megegyezik. Elképzelte az operátorokat, akik egész nap üzenetek százainak monoton kódolást végezték. Fáradtak voltak. Ilyen körülmények között nehezükre eshetett az üzenetkód véletlenszerű választása, sőt, sokuk egyszerű ember lévén nem feltétlenül gondolt arra, hogy

ez fontos. Ezek alapján feltételezte, hogy az operátorok nem véletlenszerűen választottak. Felmerül a kérdés: akkor minek alapján tették?

Feltételezte, hogy az operátorok üzenetkód gyanánt vagy három ugyanolyan betűt, vagy a billentyűzeten három egymás melletti karaktert választottak. Megvizsgálta például, hogy az SYX SCW indikátor lehet-e az AAA AAA üzenetkód rejtjelezett változata. Ez a következőket jelenti: $Aa = s$, $Ba = y$ és $Ca = x$. Mivel FC két 13 hosszúságú ciklus szorzata, így ez egyértelműen meghatározza C-t és F-et. Másik két hasonló sejtés segítségével Rejewski képes volt meghatározni az A, B, C, D, E és F permutációkat.
Az alábbi táblázat egy adott nap indikátorait, és az azok alapján megfejtett üzenetkódokat mutatja:

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
BBD VDV: ikl	LDR HDE: kkk	SJN 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
GBP 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

A fentiek alapján megfigyelhető, hogy két aznapi üzenetkód (az *abc* és az *uvw*) kivételével az összes többi az általa feltételezett szabály szerint épült fel, ám a két kivétel választása sem mondható véletlenszerűnek. Így a véletlenszerű választottság elhanyagolható tényező. [6]

Ezek alapján az egyenletrendszer tovább egyszerűsödött. Itt a bal oldalon szereplő kifejezések már ismertek.

$$A = S^{-1}H^{-1}P^{-1}N^{-1}PQP^{-1}NPHS$$

$$B = S^{-1}H^{-1}P^{-2}N^{-1}P^{2}QP^{-2}NP^{2}HS$$

$$C = S^{-1}H^{-1}P^{-3}N^{-1}P^{3}QP^{-3}NP^{3}HS$$

$$D = S^{-1}H^{-1}P^{-4}N^{-1}P^{4}QP^{-4}NP^{4}HS$$

$$E = S^{-1}H^{-1}P^{-5}N^{-1}P^{5}QP^{-5}NP^{5}HS$$

$$F = S^{-1}H^{-1}P^{-6}N^{-1}P^{6}QP^{-6}NP^{6}HS$$

Mivel a vizsgált nap 1932 szeptemberére esett, így Rejewski birtokában volt a napi kódnak (ismerte az *S*-et), s ezzel tovább csökkent a feladat bonyolultsága (a bal oldalon álló kifejezések szintén ismertek):

$$SAS^{-1} = H^{-1}P^{-1}N^{-1}PQP^{-1}NPH$$

$$SBS^{-1} = H^{-1}P^{-2}N^{-1}P^{2}QP^{-2}NP^{2}H$$

$$SCS^{-1} = H^{-1}P^{-3}N^{-1}P^{3}QP^{-3}NP^{3}H$$

$$SDS^{-1} = H^{-1}P^{-4}N^{-1}P^{4}QP^{-4}NP^{4}H$$

$$SES^{-1} = H^{-1}P^{-5}N^{-1}P^{5}QP^{-5}NP^{5}H$$

$$SFS^{-1} = H^{-1}P^{-6}N^{-1}P^{6}QP^{-6}NP^{6}H$$

Már csak a *H, N* és *Q* permutációk ismeretlenek. Rejewski első lépésben a *H* kiküszöbölésére törekedett. [3]

Kipróbálta ugyanazt a huzalozást a kapcsolótábla és a keverőtárcsa között, melyet az Enigma kereskedelemben forgalmazott változatánál alkalmaztak, ám ez nem vezetett eredményre. Ez a sikertelen kísérlet arra ösztönözte, hogy megpróbáljon betekinteni az Enigmát kifejlesztő mérnökök fejébe. Rejewski zseniális ötlete a következő volt: kifejezetten szabályosnak találta a tárcsa és a kapcsolótábla közötti huzalozást a kereskedelmi Enigma esetében. A kapcsolók a billentyűzeten található karakterek sorrendjében csatlakoztak a keverőtárcsához. Ennek nyomán kipróbált egy másik, ám hasonlóan szabályszerű huzalozást: az ábécé sorrendjét, és ez sikerre vezetett. A feltételezések ellenére tehát nem volt a kapcsolótábla után olyan szerkezet, mely permutálná a karaktereket, így Rejewski kiiktatta az egyenletből a H-t, azaz $H = I$. [6]

A következő hat egyenlethez jutott, ahol már csak *N* és *Q* volt ismeretlen:

$$T = P^{1}SAS^{-1}P^{-1} = N^{-1}P^{1}QP^{-1}N$$

$$U = P^{2}SBS^{-1}P^{-2} = N^{-1}P^{2}QP^{-2}N$$

$$W = P^{3}SCS^{-1}P^{-3} = N^{-1}P^{3}QP^{-3}N$$

$$X = P^{4}SDS^{-1}P^{-4} = N^{-1}P^{4}QP^{-4}N$$

$$Y = P^{5}SES^{-1}P^{-5} = N^{-1}P^{5}QP^{-5}N$$

$$Z = P^{6}SFS^{-1}P^{-6} = N^{-1}P^{6}QP^{-6}N$$

Az egymás alatt elhelyezkedő egyenleteket összeszorozta, így egy öt egyenletből álló egyenletrendszert kapott.

$$UT = N^{-1}P(PQP^{-1}Q)P^{-1}N$$

$$WU = N^{-1}P^{2}(PQP^{-1}Q)P^{-2}N$$

$$XW = N^{-1}P^{3}(PQP^{-1}Q)P^{-3}N$$

$$YX = N^{-1}P^{4}(PQP^{-1}Q)P^{-4}N$$

$$ZY = N^{-1}P^{5}(PQP^{-1}Q)P^{-5}N$$

Ebből az egyenletrendszerből kiküszöbölte a $PQP^{-1}Q$ kifejezést, és a következő egyenletrendszerhez jutott, melyben már csak az *N* volt ismeretlen. A jobb áttekinthetőség érdekében bevezette a $V = N^{-1}P^{-1}N$ jelölést.

$$WU = N^{-1}PN(UT)N^{-1}P^{-1}N = V^{-1}(UT)V$$

$$XW = N^{-1}PN(WU)N^{-1}P^{-1}N = V^{-1}(WU)V$$

$$YX = N^{-1}PN(XW)N^{-1}P^{-1}N = V^{-1}(XW)V$$

$$ZY = N^{-1}PN(YX)N^{-1}P^{-1}N = V^{-1}(YX)V$$

Vegyük észre, hogy az összes egyenlet azonos alakú: $J = V^{-1}KV$, ahol *J* és *K* ismert. A fenti kifejezés megoldásának módját az 1. tételnél láthatjuk. Az előbbi négy egyenlet mindegyikéhez találhatunk így megoldásokat. Közülük az lesz a valódi *V*, mely az összes egyenletet kielégíti. Ez a megoldás egy ciklikus permutáció, mivel P^{-1} konjugáltja. Ily módon megkaphatjuk *N*-t.

Az egyik keverőtárcsát (a jobboldalit) leíró permutáció így ismertté vált. Ekkortájt a német hadseregnél a tárcsák sorrendjét negyedévente változtatták, a napi kódnak megfelelően. Mivel szeptember és október hónapok az év két különböző negyedévéhez tartoznak, az eddigiekben ismertetett módszerrel egy másik keverőtárcsa permutációját is leírhatták.

Ezek után nem ütköztek nagy nehézségekbe a harmadik keverőtárcsa, valamint a visszafordító permutációinak meghatározásakor. A lengyelek tehát képessé váltak a katonai Enigma másolatának megépítésére. [3], [6]

Az Enigma további sorsa

1934-re a lengyelek megépítették az Enigmát , és az üzenetek többségét el tudták olvasni. Ebben az időben a kémtevékenységnek köszönhetően ismerték a napi kódokat. Tisztában voltak azonban azzal, hogy nem biztos, hogy a napi kódokat mindig sikerül megszerezniük, ezért egy olyan módszert próbáltak kidolgozni, amivel az üzenetek a napi kód megléte nélkül is megfejthetők. Rejewski kifejlesztett egy Ciklométer elnevezésű gépet, mely az Enigma egy módosított változata. A gép segítségével a lehetséges napi karakterisztikák számát csökkentette. A gép megvizsgálta a napi karakterisztikákat (melyeket a korábbiakban AD-vel, BE-vel és CF-el jelöltünk), és a lehetséges esetek többségét kizárta. A maradék esetet a kriptográfusok gépi segítség nélkül elemezték, míg meg nem találták a megfelelő kezdőbeállítást. A Ciklométer jelentőssége abban rejlik, hogy gyorsabban és pontosabban végezte a számításokat.

1938 szeptember 15-től a németek módosították az Enigma használatát: A napi kódban csak a tárcsák sorrendje és a kapcsolótáblán összekapcsolandó betűpárok szerepeltek. A három tárcsa helyzetét az operátornak kellett megválasztania minden egyes üzenetnél. Ez az információ a kódolt szöveg legelején, az indikátor előtt, kódolatlanul szerepelt. Ez újabb nehézséget jelentett, mivel egy adott tárcsabeállításhoz kevés kódolt szöveg tartozott, s így nem volt elegendő információ Rejewskiék kezében a kód feltöréséhez. A probléma kiküszöbölésére a Bomba elnevezésű gépet, (mely nevét egy ekkoriban népszerű süteményről kapta), és a Zygalski által kifejlesztett lyukkártyát használták. A használt módszerek a permutációk fix pontjainak vizsgálatán alapultak.

'38-'39-ben a németek újabb módosítást hajtottak végre, nevezetesen a három tárcsa helyett ötöt használtak. A napi kódban volt meghatározva, hogy ebből az öt tárcsából melyik hármat kell a gépbe tenni. Ezzel a lehetőségek száma megtízszereződött, hiszen három tárcsát hat féle képpen, míg ötöt hatvan féle képpen helyezhettek az Enigmába. A Bombák számát hatról hatvanra kellett volna növelni, ám erre a lengyeleknek nem voltak meg az anyagi forrásaik. [3]

1939 júliusában, mikor világossá vált, hogy Európa újabb háború elé néz, valamint hogy a lengyelek anyagi gondokkal küszködnek, Varsóban találkozót szerveztek (július 25-26), és a katonai Enigma megépített másolatát, valamint a Bombák terveit, további kutatásra átadták a franciáknak, és az angoloknak. A francia – lengyel együttműködési szerződés

ellenére a franciák a továbbiakban nem tájékoztatták a lengyeleket az elért eredményekről, és a megszerzett információkról.

Ekkor került az első katonai Enigma-másolat a Bletchley parkba, ahol a „British Cryptanalysis" központja volt. Itt két angol kriptográfus kezdett el foglalkozni a Bomba tökéletesítésével. Turing a Bomba átalakításával kidolgozta az angol Bombe terveit, míg Welchman újra kitalálta Zygalski lyukkártyáit. Egy Harold „Doc" Keen nevű gépészmérnök, kettejük ötleteit felhasználva megépítette a Bombe-t, mely egy egy tonna súlyú, hat és fél láb magas, hét láb hosszú és két láb széles elektromechanikus szerkezet volt. Jelentősége (az Enigma által generált szövegek feltörésén kívül) abban rejlik, hogy a számítógépek elődjének tekinthető.

Az angolok az Enigmával előállított üzenetek többségét meg tudták fejteni. Nehézségbe ütköztek azonban a német haditengerészet által küldött üzenetek megfejtésénél. Az Enigmát a flottánál szigorított szabályok szerint használták, mivel a német hadsereg egyik legfontosabb haderejét képezték. Figyeltek arra, hogy az üzenetkódokat valóban véletlenszerűen válasszák, és kerülték a sablonos szövegek írását. Ezen felül az öt tárcsa helyett nyolcat használtak, és visszafordítóból is több féle volt. A tengeralattjárók kapitányainak szigorú parancsba adták, hogy az Enigmát, illetve a napi kódokat tartalmazó kódkönyveket semmisítsék meg, ha az a veszély fenyegetne, hogy az ellenség kezére jutnak. Az angolok – mivel a tengerészet által küldött szövegeket nem tudták elolvasni – úgy döntöttek, elrabolnak egy német hajót. Az egyik ötletgazda Ian Fleming, a James Bond történetek írója volt. 1941 májusában az angolok elsüllyesztették a német U-110-es tengeralattjárót. Fritz Julius Lemp, a kapitány, elmulasztotta megsemmisíteni az Enigmát, és a kódkönyveket, ami így angol kézre jutott. Ezután az angolok a tengerészet által küldött üzeneteket is el tudták olvasni.

Az Enigma vizsgálatába később az amerikaiak is bekapcsolódtak, majd attól félve, hogy a maffia kezére kerül, az Enigmával kapcsolatos összes információt titkosították 1987-ig. [5], [7]

Hivatkozások

1. BAUER, FRIEDRICH L., *Decrypted Secrets, Methods and Maxims of Cryptology,* Springer-Verlag második kiadás, Berlin Heidelberg, 2000

2. KOZACZUK, WLADYSLAW, *Enigma,* London: Arms and Armour, 1984

3. REJEWSKY, MARIAN, *An application of the theory of permutations in breaking the Enigma cipher,* Applicationes Mathematicae XVI. évf. 4. szám, 1980 Varsó
in: http://mad.home.cern.ch/frode/crypto/rew80.pdf

4. REJEWSKY, MARIAN, *How Polish mathematicians broke the Enigma cipher,* IEEE Annals of the history of computing, July 1981, 213-234

5. SINGH, SIMON, *Kódkönyv,* Park Könyvkiadó, Budapest, 2002

6. TUMA, JIRI, *Permutation Groups and the Solution of German Enigma Cipher,* Károly Egyetem, Prága, 2003

7. *Solving the Enigma: History of the Cryptanalytic Bombe*
in:ed-thelen.org/comp-hist/NSA-Enigma.html

Enigma szimulátorok:

http://frode.home.cern.ch/frode/crypto/simula/m3
http://www.attlabs.att.cu.uk/andyc/enigma/enigma_j.html
http://www.fizzy.net/~ian/enigma/applet/index.html
http://www.ugrad.cs.jhu.edu/russel/classes/enigma
http://www.xat.nl/enigma

Képek

TUMA, JIRI *Permutation Groups and the Solution of German Enigma Cipher,* Károly Egyetem, Prága, 2003