

EÖTVÖS LORÁND TUDOMÁNYEGYETEM
TERMÉSZETTUDOMÁNYI KAR

Mérai László

PERMUTÁCIÓK, MELYEK
MEGMENTETTÉK A VILÁGOT

DIPLOMAMUNKA

Témavezető:

Szabó Csaba

Algebra és Számelmélet Tanszék



Budapest, 2006.

Tartalomjegyzék

1. A klasszikus Enigma	4
1.1. Történeti áttekintés az Enigmáról	4
1.2. A katonai Enigma felépítése	6
1.3. Az Enigma működése	7
1.4. A használati utasítás	8
1.5. Az Enigma használata	9
1.6. A titkosírás alapelveinek megszegése	10
1.7. Az Enigma feltörésének kezdetei	10
1.8. Az Enigma matematikai modellje	10
2. Az NP-teljes Enigma	16
2.1. Az Enigma napjainkban	16
2.1.1. A Term-EQ probléma	20

Előszó

Dolgozatom témája az Enigma működésének matematikai modellje. Az Enigma egy német titkosíró gépezet, melyet a két világháború között fejlesztettek ki. Története különösen érdekes, mivel a lengyelek - miután hozzájutottak néhány rejtjelezett szöveghez - a kódfejtéshez mély matematikai módszereket is alkalmaztak, először a történelem folyamán. Munkámat történeti bevezetéssel kezdem, amit az egyenletek vázlatos leírása követ. A dolgozat fő eredményeként két olyan módosítást ismertetek, melyek korunkban is lehetővé teszik az Enigma használatát. Két olyan átalakítást javaslok, melyek számítástudományi értelemben nehezzé teszik az Enigma feltörését a jelenlegi módszerekkel. A felhasznált eszközök segítségével megválaszolom Szabó és Vértesi egy 2001-ben felvetett problémáját.

1. fejezet

A klasszikus Enigma

1.1. Történeti áttekintés az Enigmáról

1928-tól a német hadsereg új titkosírást kezdett használni, ami merőben eltért az addig alkalmazottaktól. Lengyelország az első világháborút követően tisztában volt azzal, hogy a németek továbbra is fenyegetik az ország biztonságát, ezért már a két világháború között lehallgatták és megfejtették a német üzeneteket. '28-tól azonban az addig használt feltörési módszerek, mint a karakterek gyakoriságának vizsgálata, nem vezettek eredményre. Ebből a lengyel titkosszolgálat arra következtetett, hogy a németek gépi titkosításra váltottak [7].

A lengyelek létrehozták saját titkosírási irodájukat, a Biuro Szyfrów-t, és megbízták az új titkosírás tanulmányozásával.

A lengyelek a titkosírás megfejtésével sokáig kísérleteztek eredménytelenül. Eleinte főleg nyelvészek, később látnokok, parapszichológusok vettek részt a kutatásban. Végül elkeseredésükben a matematikusokhoz fordultak. A poznańi egyetemen új kurzus indult, kriptanalízis néven. A tárgy kiemelkedő diákjait, Marian Rejewskit (1905 - 1980), Jerzy Rózyckit (1907 - 1942) és Henryk Zygalskit (1906 - 1978) felkérték a titkosírás tanulmányozására.



1.1. ábra. Jerzy Růzycki, Marian Rejewski, Henryk Zygalski

Munkásságuknak köszönhetően a második világháború évekkor korábban befejeződhetett, mivel a németek legtöbb szigorúan titkos üzenetét az ellentábor el tudta olvasni [7], [9].

Rejewskiék statisztikai teszteket alkalmaztak az elfogott üzeneteken, melyek nyomán kiderült, hogy a szöveg első hat karaktere nem más mint az indikátor. Az indikátor az üzenetnek az a része, mely információt tartalmaz a kulcsról, aminek segítségével visszafejthető a kódolt üzenet. A továbbiakban arra is rájöttek, hogy a titkosírás polialfabetikus [5], vagyis az eredeti szöveg összes betűjét egyszerű megfeleltetéssel egy másik betűre cserélik. A rejtjelezett betű függ az eredeti betű szövegben elfoglalt helyétől is.

1926-ban megjelent kereskedelmi forgalomban az Arthur Scherbius által szabadalmaztatott Enigma. Az Enigmát eredetileg az üzleti szféra számára tervezték, ám nem váltotta be a hozzá fűzött reményeket. A német hadsereg kifejlesztette az Enigma katonai változatát. Rejewskiék számára világossá vált, hogy az új titkosírás a katonai Enigmától származik [9].

1.2. A katonai Enigma felépítése

A szerkezet fontosabb részei a következők [5] [9]:

billentyűzet

kijelző

kapcsolótábla

keverő-berendezés

keverőtárcsa

visszafordító



A keverőtárcsák struktúrája [5] [9]:

1 lánckerék

2 ábécés gyűrű

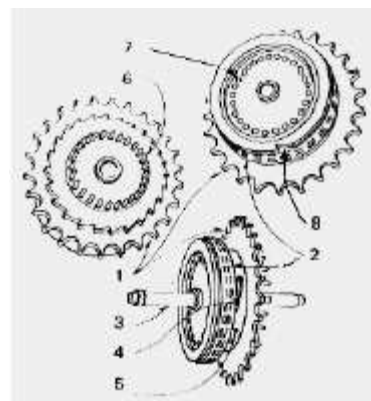
3 tengely

4 retesz

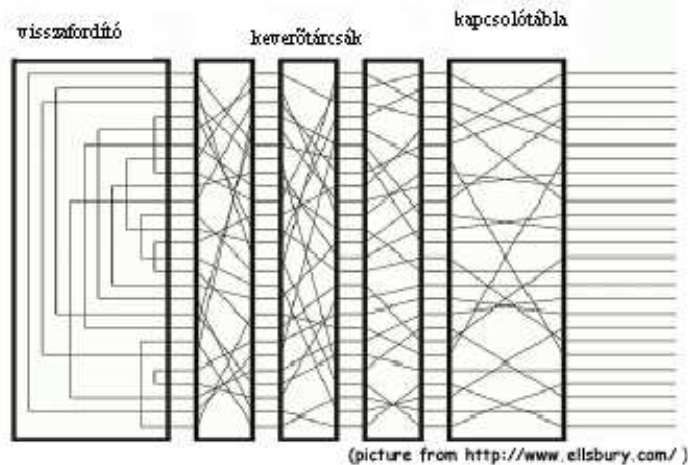
5 kábeltartó

6-7 érintkezőpár

8 továbbító horony



Az Enigma belső szerkezetének sematikus rajza [5]:



1.3. Az Enigma működése

Az Enigma működésének tárgyalása előtt álljanak itt a titkosírás alapelvei. Ezek megszegése adhat alapot a feltöréshez.

A titkosírás alapelvei a következők:

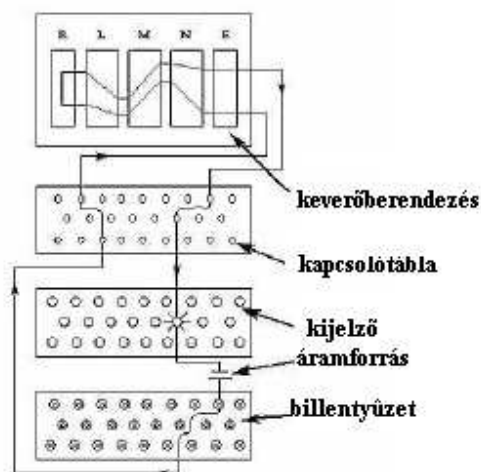
- (1) Nem használható ugyanaz a kulcs különböző szövegek kódolásához.
- (2) Azonos szöveg nem kódolható két különböző kulccsal.

A fentiek megszegésének következtében információ szerezhető a kulcsról. Figyelemre méltó továbbá a következő két „elv” is:

- (3) Feltételezni kell, hogy az ellenség tudja a bekódolási algoritmust.
- (4) Nem szabad alábecsülni az ellenséget.

Lássuk, hogyan is működik az Enigma. Egy billentyű lenyomását követően az áram útja a következő: először a kapcsolótáblán folyik keresztül, mely egy olyan dugaszolótábla, amin a feladó bizonyos betűket felcserélhet. Ezután a három keverőtárcsa következik, melyek egymástól függetlenül permutálják a betűket. A beérkezett jelet a visszafordító egy másik útvonalon juttatja vissza a kijelzőhöz. A keverőtárcsák forgása a következő képpen zajlik: az első helyen lévő tárcsa minden billentyű leütése után fordul egy betű helynyit. A második és harmadik tárcsa akkor fordul egy betű helynyit, amikor az előző körbeért. A keverőtárcsák helyzete nem meghatározott, a tárcsák felcserélhetők egymással, illetve kézzel tetszőleges helyre forgathatók [5].

Az alábbi ábrán megfigyelhető, hogy hogyan folyik keresztül az áram az Enigmán:



1.4. A használati utasítás

A lengyelek kémkedés útján fontos információkhoz jutottak a használati utasításról. Hans-Thilo Schmidt, aki az Enigma parancsnokságán dolgozott, a következő adatokat szolgáltatotta ki a franciáknak, akik aztán átadták a Lengyel Hírszerzésnek: két fotót, melyek a használati utasítást ábrázolták és néhány utalást a gép huzalozásáról. Schmidt révén hét éven át több kódkönyv is

lengyel kézre jutott. A kódkönyvek, melyeket eljuttattak az összes operátornak, negyedévre előre tartalmazták a napi kódokat [9].

A napi kód az az adat, ami meghatározza, hogy az adott napon az Enigmát milyen beállítások szerint kell használni. Részei a következők:

- 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;

A napi kód tehát az első pontban meghatározza, hogy milyen sorrendben legyenek a gépben a tárcsák. A második pontban rögzíti, hogy a tárcsák milyen kezdőállásban legyenek. A harmadik pontban pedig azt határozza meg, hogy a kapcsolótáblán mely betűket kell megcserélni.

1.5. Az Enigma használata

Az üzenetek kódolásához a napi kódon kívül szükség volt egy üzenetkódra is. Ezt az operátornak véletlenszerűen kellett választania minden egyes üzenetnél. Az üzenetkód egy betűhármast (pl.: HTS). Ezt a kezelő kétszer egymás után leírta, majd elkódolta (pl: a HTS HTS -ből NEW GWY lett).

A kétszer bekódolt üzenetkód nem más mint az indikátor, melyet a küldött rejtjelezett szöveg elejére írtak. A gépet ezután úgy kellett beállítani, hogy a tárcsák állása megfeleljen az üzenetkódnak, vagyis az ábécés gyűrűk állása jelen esetben HTS legyen.

Így a HELLO üzenet elkódolva BPTQS lenne. Ebben az esetben a teljes üzenet NEW GWY BPTQS, vagyis az indikátor és a kódolt üzenet egymás után írva [9].

Felmerül a kérdés, hogy miért kellett az üzenetkódot kétszer küldeni, és kétszer kódolni. Mivel az Enigmát hadi célokra használták, számolni kellett a rádiós adás zavarásával. Az emberi tényezőt sem hagyhatták figyelmen

kívül: ha az egyszer kódolt üzenetkódot küldték volna el kétszer, akkor nem derülhetett volna ki, ha az operátor gépelési hibát ejtett.

1.6. A titkosírás alapelveinek megszegése

A fenti példán világosan látszik, hogy két alapelv is sérült. Az első alapelv megszegése: adott napon minden egyes üzenetet azonos kulccsal, nevezetesen a napi kóddal rejtjelezték. A második alapelv ott sérült, hogy az üzenetkódokat minden esetben kétszer, és két különböző kulccsal kódolták. Ezeknek a szabályoknak az áthágása adta az alapot az Enigma feltöréséhez.

1.7. Az Enigma feltörésének kezdetei

1932 decemberében Marian Rejewskinek a következő információi voltak a feltöréshez: ismerte a használati utasítást, rendelkezett a szeptemberi és októberi napi kódokkal, valamint birtokában volt az Enigma kereskedelmi forgalomban kapható változata. (A kereskedelmi Enigmán nem volt kapcsolótábla, és a keverőtárcsái, valamint a visszafordítója is különbözött a katonai Enigmáétól.) Ezen kívül tudta még, hogy a szeptemberi és októberi napi kódok az év két különböző negyedéből származnak, valamint számos elkapott üzenete is volt az év más hónapjaiból.

1.8. A keverőtárcsák, a visszafordító és a keverőberendezés matematikai modellje

Az Enigma feltörése a gyakorlatban a három keverőtárcsa (N , M , L) és a visszafordító (R) permutációinak megfejtését jelenti. Az eddigiekből világos, hogy R diszjunkt cserék szorzataként áll elő. A tárcsák forgásának leírása érdekében legyen $P := (a, b, c, \dots, x, y, z)$ 26 hosszú ciklus. A keverőberendezés modelljét ezen permutációk segítségével kapjuk:

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

S -sel jelölve a kapcsolótábla permutációját, megkapjuk az Enigma teljes matematikai modelljét:

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

Az elkapott üzenetek első hat karakterét egy adott nap folyamán azonos módon kódolták. Legyen A az első, B , C , D , E , F , a második, a harmadik, a negyedik, az ötödik és a hatodik karakterek permutációja.

A fentiek alapján az első hat karakter permutációjára a következő egyenleteket kapjuk:

$$\begin{aligned} A &= S^{-1}P^{-1}N^{-1}PM^{-1}L^{-1}RLMP^{-1}NPS \\ B &= S^{-1}P^{-2}N^{-1}P^2M^{-1}L^{-1}RLMP^{-2}NP^2S \\ C &= S^{-1}P^{-3}N^{-1}P^3M^{-1}L^{-1}RLMP^{-3}NP^3S \\ D &= S^{-1}P^{-4}N^{-1}P^4M^{-1}L^{-1}RLMP^{-4}NP^4S \\ E &= S^{-1}P^{-5}N^{-1}P^5M^{-1}L^{-1}RLMP^{-5}NP^5S \\ F &= S^{-1}P^{-6}N^{-1}P^6M^{-1}L^{-1}RLMP^{-6}NP^6S \end{aligned}$$

P kivételével az összes permutáció ismeretlen volt Rejewski számára.

Tudjuk, hogy az R permutáció diszjunkt cserék szorzata, így $R^2 = I$. Mivel az A , B , C , D , E és F mind konjugáltak az R -rel, így megkapjuk, hogy

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

Ezen permutációk még ismeretlenek voltak, de a DA , EB , FC szorzatok nem. Rejewski ezeket hívta a nap karakterisztikájának.

Az említett szorzatokat az indikátorból kaphatjuk meg:

Legyen az üzenetkód az xyz betűhármás. Az indikátor az $rtsuvw$, az $xyzxyz$ kódolt vátozata. Ekkor $Ax = r$ és $Dx = u$, így $DAr = u$. Amennyiben elég üzenetet kapunk el egy adott nap során, ismertté válnak a DA , EB , FC permutációk.

Így előállnak a karakterisztikák, például:

$$\begin{aligned} DA &= (a), (s), (bc), (rw), (dvpfkxgzyo), (eijmnuqlht); \\ EB &= (axt), (blfqveoum), (cgy), (d), (hjpswizm), (k); \\ FC &= (abviktjgfcqny), (duzrehlxwpsmo). \end{aligned}$$

A korábbiak szerint a karakterisztikákra a következő egyenletek kaphatóak:

$$\begin{aligned} DA &= S^{-1}P^{-4}N^{-1}P^4M^{-1}L^{-1}RLMP^{-4}NP^3N^{-1}PM^{-1}L^{-1}RLMP^{-1}NPS \\ EB &= S^{-1}P^{-5}N^{-1}P^5M^{-1}L^{-1}RLMP^{-5}NP^3N^{-1}P^2M^{-1}L^{-1}RLMP^{-2}NP^2S \\ FC &= S^{-1}P^{-6}N^{-1}P^6M^{-1}L^{-1}RLMP^{-6}NP^3N^{-1}P^3M^{-1}L^{-1}RLMP^{-3}NP^3S \end{aligned}$$

A $Q := M^{-1}L^{-1}RLM$ jelölést bevezetve kapjuk a következőket:

$$\begin{aligned} DA &= S^{-1}P^{-4}N^{-1}P^4QP^{-4}NP^3N^{-1}PQP^{-1}NPS \\ EB &= S^{-1}P^{-5}N^{-1}P^5QP^{-5}NP^3N^{-1}P^2QP^{-2}NP^2S \\ FC &= S^{-1}P^{-6}N^{-1}P^6QP^{-6}NP^3N^{-1}P^3QP^{-3}NP^3S \end{aligned}$$

Ezt továbbra sem tudjuk megoldani, mivel R illetve Q ismeretlenek.

Rejewski pszichikai tényezőik segítségével tudta egyszerűsíteni a feladatot. Észrevette, hogy az elkapott üzenetek indikátorai közül sok megegyezik,

ezért azt feltételezte, hogy az operátorok az üzenetkódokat nem választották véletlenszerűen. A kezelők munkája monoton, unalmas és fárasztó volt, s talán sokukban fel sem merült, hogy a véletlenszerű választás fontos.

Hogyan választottak tehát az operátorok? Rejewski egyik nagyszerű ötlete, hogy feltételezte, az operátorok az egyszerűség és gyorsaság kedvéért háromszor ugyanazt a billentyűt, vagy három egymás melletti billentyűt ütnek le üzenetkód gyanánt. Ezt arra alapozta, hogy az operátorok egyszerű emberek lévén nem voltak tudatában a véletlenszerűség fontosságának. Vegyünk egy példát: Megvizsgálta, hogy az SYX SCW indikátor eredhet-e az AAA üzenetkódból. Mivel *FC* két 13 hosszúságú ciklus szorzata, ez egyértelműen meghatározza *C*-t és *F*-et. Másik két hasonló sejtés segítségével Rejewski meghatározta az *A*, *B*, *C*, *D*, *E* és *F* permutációkat. Példaként az alábbi táblázat egy adott nap indikátorait, és az azokból visszafejtett 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: llj	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

Kiderült, hogy, szinte minden üzenetkód megfelel a Rejewski által feltételezett szabálynak. Két kivétel azért akad (*abc* és *uvw*), ám látható, hogy ezek választása is távol áll a véletlentől [9].

Rejewski birtokában volt a napi kódnak (ismerte az *S*-et), s ezzel tovább csökkent a feladat bonyolultsága :

$$\begin{aligned}
SAS^{-1} &= P^{-1}N^{-1}PM^{-1}L^{-1}RLMP^{-1}NP \\
SBS^{-1} &= P^{-2}N^{-1}P^2M^{-1}L^{-1}RLMP^{-2}NP^2 \\
SCS^{-1} &= P^{-3}N^{-1}P^3M^{-1}L^{-1}RLMP^{-3}NP^3 \\
SDS^{-1} &= P^{-4}N^{-1}P^4M^{-1}L^{-1}RLMP^{-4}NP^4 \\
SES^{-1} &= P^{-5}N^{-1}P^5M^{-1}L^{-1}RLMP^{-5}NP^5 \\
SFS^{-1} &= P^{-6}N^{-1}P^6M^{-1}L^{-1}RLMP^{-6}NP^6
\end{aligned}$$

Már csak az N és Q permutációk ismeretlenek:

$$\begin{aligned}
T &= P^1SAS^{-1} = N^{-1}P^1QP^{-1}N \\
U &= P^2SAS^{-2} = N^{-1}P^2QP^{-2}N \\
W &= P^3SAS^{-3} = N^{-1}P^3QP^{-3}N \\
X &= P^4SAS^{-4} = N^{-1}P^4QP^{-4}N \\
Y &= P^5SAS^{-5} = N^{-1}P^5QP^{-5}N \\
Z &= P^6SAS^{-6} = N^{-1}P^6QP^{-6}N
\end{aligned}$$

Az egymás alatt elhelyezkedő egyenleteket összeszorozva megkapta a következő egyenletrendszer:

$$\begin{aligned}
UT &= N^{-1}P(PQP^{-1}Q)P^{-1}N \\
WU &= N^{-1}P^2(PQP^{-1}Q)P^{-2}N \\
XW &= N^{-1}P^3(PQP^{-1}Q)P^{-3}N \\
YX &= N^{-1}P^4(PQP^{-1}Q)P^{-4}N \\
ZY &= N^{-1}P^5(PQP^{-1}Q)P^{-5}N
\end{aligned}$$

Miután kiküszöbölte a $PQP^{-1}Q$ kifejezést, Rejewski a következő egyenletrendszerhez jutott, melyben már csak az N volt ismeretlen.

$$\begin{aligned}
WU &= N^{-1}P^2(PQP^{-1}Q)P^{-2}N \\
XW &= N^{-1}P^3(PQP^{-1}Q)P^{-3}N \\
YX &= N^{-1}P^4(PQP^{-1}Q)P^{-4}N \\
ZY &= N^{-1}P^5(PQP^{-1}Q)P^{-5}N,
\end{aligned}$$

ahol $V = N^{-1}P^{-1}N$

Az összes egyenlet azonos alakú: $J = V^{-1}KV$, ahol J és K ismert. Innen már egyszerűen meghatározható az N permutáció [5], [9].

2. fejezet

Az NP-teljes Enigma

2.1. Az Enigma napjainkban

Az eddigiekből világosan látszik, hogy az Enigma feltörése egy véges probléma, vagyis a számítógépek fejlődésével egyre könnyebben feltörhető, egyre védtelenebb rendszer.

Például, ha a három tárcsa különböző beállításait vesszük figyelembe, akkor $26^3 = 17576$ esetet kell kipróbálni, s ezt egy mai számítógép másodpercek alatt végre tudja hajtani. Ha a kapcsolótábla különböző beállításait is figyelembe vesszük, melyek könnyen visszafejthetők egyszerű betűgyakorosságvizsgálattal, a feltörési időre a perces nagyságrend is óvatos felső becslés.

Szeretnénk úgy módosítani az Enigmát, hogy minél biztonságosabb legyen. Nem várható, hogy bármiféle módosítással feltörhetetlen rendszert kapunk. Azt szeretnénk elérni, hogy a lehető legnehezebb legyen a titkosírás megfejtése.

Az Enigma problémáját bonyolultságelméleti szemszögből érdemes vizsgálni, mely azzal foglalkozik, hogy egy adott matematikai probléma mennyire könnyen oldható meg.

Olyan módosítást szeretnénk vérehajtani az Enigmán, hogy feltörése minél nagyobb bonyolultság-osztályba essen. Ilyen problémakör az NP-teljes problémák osztálya, melynek elemei a gyakorlatban megoldhatatlanok. Bo-

nyolultságelméleti-osztályokba azonban csak olyan problémákat tudunk besorolni, melyek eldöntendő kérdések.

Szeretnénk átfogalmazni a feltörési problémát valamely "igen-nem" kérdésre. Tegyük fel, hogy vannak bizonyos információink az aznapi beállításokról. Például egy kémünk megszerezte a kódkönyvet, vagy bizonyos kódolt szövegeknek ismerjük a tartalmát. Feltehető az is, hogy egy korábbi Enigma-változatot már sikerült feltörni, így azok az alkatrészek, melyeket a németek csak ritkán vátoztattak — például a visszafordító — már ismertek.

Valószínűsíthető, hogy a megszerzett információ töredékes. Például csak a tárcsák sorrendjét ismerjük, a napi beállítás többi részét nem.

Ekkor már értelmes kérdés, hogy az adott információk megfelelnek-e a valóságnak, azaz van-e olyan tárcsabeállítás, mely szinkronban van a kém által megszerzett információkkal, és az elkapott üzenetekkel. Ez a feltörés szempontjából fontos kérdés, mert nem várható, hogy meg tudjuk fejteni az Enigma-kódot, ha még azt sem tudjuk leellenőrizni, hogy igazat mond-e a kém.

Feltehető, hogy a németek a feltörés nehezítésének érdekében további tárcsákat is használatba helyeznek. Ezért tegyük föl, hogy minden egyes permutációhoz létezik egy azt leíró tárcsa. A bonyolultság további fokozásáért a németek azonos típusú tárcsákat különbözően is jelölhetnek. Attól, hogy két tárcsa sorszámja különböző, nem biztos, hogy más permutációt írnak le.

A valóságban a kém nem feltétlenül ismeri a tárcsák által leírt permutációkat, csak a tárcsák számozását. Csupán olyan ismereteink vannak, hogy bizonyos helyeken levő tárcsák típusai megegyezhetnek.

A tárcsák forgási sebessége is változhat a kódolás során, azaz a keverőtárcsák nem feltétlenül csak egy ütemet fordulnak minden billentyű lenyomásakor. A forgás mértéke is változhat bizonyos időközönként. Ezek alapján a korábbi eszközökkel csak az első betű permutációja határozható meg.

Matematikailag az Enigma tárcsái különböző változókkal jelölhetők. Így az első karakter permutációjára a következő egyenlet adódik:

$$A = (x_1x_2 \cdot \dots \cdot x_n)^{-1}Rx_1x_2 \cdot \dots \cdot x_n,$$

ahol az operátor az adott nap során n darab tárcsát használt. Erre a későbbiekben az alábbi jelölés használható:

$$R^{x_1x_2\cdots x_n}$$

Azt is tudjuk, hogy egyes tárcsák megegyeznek. Ekkor például a következő típusú egyenlethez juthatunk:

$$A = (x_1x_2x_1x_7x_4)^{-1}Rx_1x_2x_1x_7x_4,$$

ha az 5-tárcsás Enigmát tanulmányozzuk.

Kétféle módosítás lehetséges, hogy a megszerzett információ helyességének ellenőrzése NP-teljes probléma legyen.

Az első módosításnál tetszőleges számú tárcsa használata megengedett. Az információ pontosan akkor felel meg a valóságunk, ha az

$$R^{x_1x_2\cdots x_n} = A$$

egyenletnek létezik megoldása. Itt A (az első karakter permutációja) és R ismertek. A megoldás létezésének leellenőrzése nem egyszerű feladat:

1. Tétel. *Legyen G nem feloldható csoport. Legyen továbbá $T(\vec{x})$ tetszőleges term, és legyenek $A, R \in G$ tetszőleges konjugált elemek. Annak eldöntése, hogy létezik-e olyan \vec{g} vektor, hogy*

$$T(\vec{g})^{-1}RT(\vec{g}) = A, \tag{2.1}$$

NP-teljes feladat.

A tétel bizonyításánál fontos szerepet játszanak a *verbális* részcsoportok:

2. Definíció. *Legyen G tetszőleges csoport. $H \leq G$ verbális részcsoport, ha létezik olyan t term, melynek képe H .*

A tételt elég speciális rész- és faktorcsoportokra igazolni:

3. Lemma. *Legyen G tetszőleges csoport, és legyen $H \triangleleft G$ tetszőleges verbális normálosztó. Ekkor igazak a következők:*

- *Ha annak eldöntése, hogy az 2.1. egyenlet G/H fölött megoldható, NP-teljes, akkor G fölött is az.*
- *Ha annak eldöntése, hogy az egyenlet megoldható H fölött NP-teljes, akkor G fölött is az.*

Bizonyítás. Az első rész bizonyításához tekintsük az egyenletet G/H fölött:

$$(x_1H \cdot x_2H \cdots x_nH)^{-1}Rx_1H \cdot x_2H \cdots x_nH = A$$

Ekkor léteznek olyan $h_1, \dots, h_n \in H$, hogy

$$(x_1h_1 \cdot x_2h_2 \cdots x_nh_n)^{-1}Rx_1h_1 \cdot x_2h_2 \cdots x_nh_n = A.$$

Másrészről létezik olyan $h \in H$, hogy

$$x_1h_1 \cdot x_2h_2 \cdots x_nh_n = h \cdot x_1x_2 \cdots x_n.$$

Így az eredeti egyenlet a következővel ekvivalens:

$$(x_1x_2 \cdots x_n)^{-1} \cdot h^{-1}Rh \cdot x_1x_2 \cdots x_n = A.$$

H verbális, azaz létezik olyan t term, melynek értékészlete a H csoport.

Az egyenletnek így pontosan akkor van megoldása, ha az

$$(x_1x_2 \cdots x_n)^{-1} \cdot t(\vec{y})^{-1}Rt(\vec{y}) \cdot x_1x_2 \cdots x_n = A$$

egyenlet megoldható.

A második rész bizonyításához tekintsük az egyenletet H fölött:

$$(x_1 \cdot x_2 \cdots x_n)^{-1}Rx_1 \cdot x_2 \cdots x_n = A.$$

Mivel H verbális, ezért létezik olyan $t = t(y_1, \dots, y_k)$ G fölötti term, melynek képe H . Minden x_i változóhoz definiáljunk $y_{i,1}, \dots, y_{i,k}$ G fölötti változókat, amivel $x_i = t(y_{i,1}, \dots, y_{i,k})$. Ezzel az egyenlet a következő alakba írható:

$$\begin{aligned} & (t(y_{1,1}, \dots, y_{1,k}) \cdot t(y_{2,1}, \dots, y_{2,k}) \cdots t(y_{n,1}, \dots, y_{n,k}))^{-1}R \\ & t(y_{1,1}, \dots, y_{1,k}) \cdot t(y_{2,1}, \dots, y_{2,k}) \cdots t(y_{n,1}, \dots, y_{n,k}) = A. \end{aligned}$$

Belátható, hogy ennek az egyenletnek pontosan akkor létezik megoldása G fölött, ha az eredeti egyenletnek létezik megoldása H fölött.

Az új egyenlet hossza a t term hosszának $2n$ -szerese. Mivel t hossza csak a G csoporttól függ, a visszavezetés polinomiális. \square

A lemma segítségével elég a tételt olyan csoportokra bizonyítani, melyekben nincs nem triviális verbális normálosztó. Ez utóbbi feladatot a termek azonosságának vizsgálatára vezethetjük vissza.

2.1.1. A Term-EQ probléma

A Term-EQ(G) probléma esetén két csak változókból álló kifejezésről kell eldönteni, hogy azonosan egyenlők-e G -ben, azaz minden G -beli helyettesítés esetén ugyanazt az értéket veszi-e fel. Például A_4 -ben, a 4-ed fokú alternáló csoportban $x^6 = ([x_1, x_2])^2$ azonosság, mivel minden A_4 -beli helyettesítés esetén mindkét oldal az egységelemet veszi fel értéként. Véges csoportok esetén ez a probléma mindig eldönthető, ám nem mindegy, hogy az azonosság hosszától függően mennyi időre van ehhez szükség. Ennek a problémának a bonyolultságát jelöljük Term-EQ(G)-vel. Azonban ha t, s két term, akkor $t \equiv s$ pontosan akkor teljesül, ha $ts^{-1} \equiv id$, ahol id a csoport egységeleme. Így a továbbiakban az utóbbit fogjuk vizsgálni.

Nem feloldható csoportok fölött igaz a következő tétel [2]:

4. Tétel. *Legyen G véges, nem kommutatív, nem feloldható csoport. Ekkor G -ben a Term-EQ feladat coNP-teljes.*

Tekintsük a tételt először egyszerű csoportokra:

5. Állítás. *Legyen G egyszerű, nem kommutatív csoport. Ekkor G -ben a Term-EQ feladat coNP-teljes.*

Bizonyítás. Legyen $k = |G|$. G nem kommutatív, egyszerű csoport, így $k \geq 60$. Polinomiálisan visszavezetjük a gráf k -színezhetőségét a Term-EQ

problémára. Minden gráfhoz mutatunk egy w termet G fölött, melyre pontosan akkor $w(g_1, \dots, g_n) \neq id$, ha a gráf k -színezhető.

Legyen $\Gamma = (V, E)$ egy egyszerű gráf, $V = \{v_1, \dots, v_n\}$ és $E = \{e_1, \dots, e_m\}$. Γ pontjait a G elemeivel szeretnénk „kiszínezni”.

Minden $g \in G$ esetén $[\{g\}, G] \triangleleft G$, és $g \neq id$ esetén $[\{g\}, G] = G$, mivel G egyszerű. Így létezik olyan d , csupán G -től függő konstans, hogy minden $g \in G$ esetén

$$G = [\{g\}, G] = \left\{ \prod_{i=1}^d [g, y_i], y_i \in G \right\}.$$

Legyen

$$S(x, y_1, \dots, y_d) = S(x, \bar{y}) = \prod_{i=1}^d [x, y_i].$$

Minden $v_l \in V$ csúcshoz hozzárendelünk egy x_l változót. Minden $e = (v_i, v_j)$ élhez definiáljuk az $S_{i,j}$ kifejezést:

$$S_{i,j}(\bar{y}) = S(x_i x_j^{-1}, \bar{y}).$$

Ezzel $S_{i,j}(G) = id$, ha $x_i = x_j$ -et helyettesítünk, míg $x_i \neq x_j$ esetén $S_{i,j}(G) = G$. $S_{i,j}$ hossza csupán a G csoporttól függ: minden kommutátor 3 változót tartalmaz, ezt kétszer ismételve a d tag összesen $6d$ hosszú.

Vezessük be továbbá a következő jelölést: legyen c_l az l . kommutátorszó, azaz $c_1(x_1, x_2) := [x_1, x_2]$ és minden további $l > 1$ esetén c_l 2^l változós $c_l(x_1, x_2, \dots, x_{2^l}) = [c_{l-1}(x_1, \dots, x_{2^{l-1}}), c_{l-1}(x_{2^{l-1}+1}, \dots, x_{2^l})]$ szó. Ezzel

$$c_1(G) = \{[a, b] \mid a, b \in G\}$$

és

$$\langle c_l(G) \rangle = G^{(l)}.$$

Most már definiálhatjuk a w kifejezést. Legyen $e = (v_i, v_j)$ Γ egy éle, és

$$w_e(\bar{y}) = S(x_i x_j^{-1}, \bar{y}).$$

Legyenek e_1, e_2, \dots, e_m a Γ élei és r olyan, hogy $2^{r-1} < m \leq 2^r$.

Továbbá legyen

$$w = c_r(w_{e_1}, w_{e_2}, \dots, w_{e_{m-1}}, w_{e_m}, w_{e_m}, \dots, w_{e_m}).$$

(Itt w_{e_m} $2^r - m$ -szer szerepel.) A w_{e_i} kifejezésben \bar{y} változói különbözőek, így összesen $d2^r$ „ y ” és inverzeik szerepelnek. A w szó hossza $6d \cdot 4^r \leq 6d(m+1)^2$, így Γ méretének polinomja.

Igazoljuk, hogy w nem identitás G fölött pontosan akkor, ha Γ k -színezhető. Először tegyük fel, hogy Γ k -színezhető a G elemeivel. Legyen g_i a v_i színe. Ezzel az $x_i = g_i$ helyettesítéssel Γ minden e élére azt kapjuk, hogy $w_e(G) = G$. Mivel G nem feloldható, így c_k nem az identitás, és w sem az. Másodszor, ha Γ nem k -színezhető, akkor minden színezésnél létezik olyan $e = (v_i, v_j)$ él, melynek végpontjai azonos színűek, azaz $w_e = id$, ennélfogva $w \equiv id$. \square

A 3. lemmához hasonlóan könnyen belátható a következő állítás:

6. Lemma. *Legyen G tetszőleges csoport, és legyen $H \triangleleft G$ tetszőleges verbális normálosztó. Ekkor igazak a következők:*

- *Ha a Term-EQ feladat G/H fölött coNP-teljes, akkor G fölött is az.*
- *Ha a Term-EQ feladat H fölött coNP-teljes, akkor G fölött is az.*

Most már igazolhatjuk a 4. tételt.

Bizonyítás. A bizonyítás a csoport rendje szerinti indukcióval történik.

1. eset: Ha van $H \triangleleft G$ nem feloldható verbális normálosztó, akkor $|H| < |G|$, így az indukció alapján a Term-EQ feladat H fölött coNP-teljes. Ám ekkor a 6. lemma alapján G fölött is az.

2. eset: Minden nem triviális verbális normálosztó feloldható. Ekkor az őket tartalmazó legszűkebb H részcsoport is verbális feloldható normálosztó. A G/H faktor nem feloldható, $|G/H| < |G|$, így az indukció alapján a Term-EQ G/H feladat coNP-teljes. A 6. lemmát alkalmazva azt kapjuk, hogy a Term-EQ G feladat is coNP-teljes.

3. eset: Nincsen nem triviális verbális normálosztó. Ha G egyszerű akkor az 5. tétel alapján készen vagyunk. Feltehetjük tehát, hogy $G' = G$, ugyanis

G' verbális, és van egy H valódi normálosztó. Ez esetben G/H nem feloldható, ugyanis ellenkező esetben van olyan m , hogy

$$1 = (G/H)^{(m)} = G^{(m)}/H = G/H,$$

amiből adódik, hogy $G = H$. Másrésztől $|G/H| < |G|$, így az indukció alapján a Term-EQ G/H probléma coNP-teljes. Polinomiálisan visszavezetjük a Term-EQ G/H problémát Term-EQ G -re. Legyen t egy G/H fölötti term, melyről el akarjuk dönteni, hogy $t \equiv id$. Belátjuk, hogy $t \equiv id$ pontosan akkor teljesül G/H fölött, ha $t \equiv id$ G fölött. Ha ugyanis $t \equiv id$ G/H fölött, akkor t képe G fölött egy $N \leq H$ verbális normálosztó, így a feltételek miatt t képe csak id lehet, így $t \equiv id$ G fölött. Másrésztől ha $t \not\equiv id$ G/H fölött, akkor t képe G -ben egy olyan N normálosztó, melyre $N \not\leq H$, így $N = G$, azaz $t \not\equiv id$ G fölött. Így az indukció alapján adódik, hogy Term-EQ G coNP-teljes. \square

E kitérő után már bizonyíthatjuk a 1. tételt.

Bizonyítás. A problémát Term-EQ G -re vezetjük vissza. A 3. lemma alapján feltehetjük, hogy G -ben nincs nem triviális verbális normálosztó.

Legyen $S(\vec{x}) = x_1 \cdots x_n$ tetszőleges term, melyről szeretnénk eldönteni, hogy $S \equiv id$ teljesül-e (itt az egyes x_i változók megegyezhetnek). Legyenek továbbá A és R nem egyenlő, egymással konjugált csoportelemek.

Legyen $N := \{S(\vec{a}) \mid a_i \in G\}$. Ha $a \in N$, akkor tetszőleges $g \in G$ elem esetén $gag^{-1} \in G$ is teljesül. Vegyük észre ugyanis, hogy ha

$$a = S(\vec{a}) = a_1 \cdots a_n \in N,$$

akkor

$$gag^{-1} = gS(\vec{a})g^{-1} = ga_1 \cdots a_n g^{-1} = ga_1 g^{-1} \cdots ga_n g^{-1} \in N.$$

Így megállapíthatjuk, hogy N konjugált osztályok egyesítése.

Legyen $M := \{b_1 \cdots b_l \mid b_i \in N\}$ az N -et tartalmazó legszűkebb részcsoporthat. Mivel N konjugált osztályok egyesítése, így $M \triangleleft G$. $M = G$ pontosan

akkor, ha $S(\vec{x}) = x_1 \cdots x_n \neq id$. Ez esetben létezik olyan K , hogy

$$\prod_{i=1}^K S(\vec{x}_i)$$

term előállítja a G csoportot.

Így pontosan akkor léteznek olyan $\vec{g}_1, \dots, \vec{g}_K$ vektorok, hogy

$$\prod_{i=1}^K S(\vec{g}_i) R \prod_{i=1}^K S(\vec{g}_i)^{-1} = A$$

teljesül, ha $S(\vec{x}) \neq id$. \square

A másik módosításnál az operátor csak korlátos számú tárcsát használhat, de ezeket gyakran kell cserélnie, ezért egy adott tárcsabeállításról kevés információnk van. Nem csak egy, hanem több ilyen beállításról is ismerjük ezt a kevés információt. Feltehető, hogy időnként átszámozzák a tárcsákat, hogy ezzel is korlátozzák a kiszivárogtatható információkat. Az eddigi eszközökkel így csak korlátos számú egyenlethez juthatunk, kizárólag addig lehet az egyenleteket szimultán vizsgálni, míg meg nem változik a tárcsák számozása. A rendszert a következő általános alakba írhatjuk:

$$\begin{aligned} R^{X_1} &= A_1 \\ R^{X_2} &= A_2 \\ &\vdots \\ R^{X_k} &= A_k \end{aligned}$$

ahol az R és A_i -k ismertek (az R a visszafordító, az A_i -k pedig a megfelelő tárcsabeállítás mellett az első karakterek permutációi). $X_i = x_{i,1}x_{i,2} \dots x_{i,n_i}$ adott termék, ahol $x_{i,j}$ a i -edik napon a j -edik helyen levő tárcsához tartozó változó, k pedig azt jelöli, hogy hány napig volt változatlan a tárcsabeállítás.

Például, ha négy napról vannak ismereteink, akkor a következő egyenletrendszer kaphatjuk:

$$\begin{aligned}
R^{x_1x_2x_1x_7x_4} &= A_1 \\
R^{x_3x_1x_9x_3x_5} &= A_2 \\
R^{x_{16}x_5x_4x_1x_{16}} &= A_3 \\
R^{x_8x_2x_8x_6x_{11}} &= A_4,
\end{aligned}$$

az 5-tárcsás Enigmát vizsgálva.

Már annak leellenőrzése, hogy megfelelnek a valóságnak az információink, sem egyszerű feladat:

7. Tétel. *Legyen G nem kommutatív csoport. Ekkor létezik olyan d_G konstans, hogy legfeljebb d_G tárcsát használva annak meghatározása, hogy van egy adott rendszernek megoldása a G csoport fölött, NP-teljes feladat.*

Először nézzük a $G = S_4$ speciális esetet.

8. Állítás. *Létezik olyan d konstans, hogy legfeljebb d_G tárcsát használva annak meghatározása, hogy van egy adott rendszernek megoldása S_4 fölött, NP-teljes feladat.*

Ehhez felhasználjuk a következő könnyen ellenőrizhető lemmát:

9. Lemma. *Minden $u, v \in S_4$ elempárhoz pontosan akkor létezik olyan $c \in S_4$ elem, ahol $[c, uv^{-1}]$ nem K -beli, ha u és v a K különböző mellékosztályában van.*

A 8. állítás bizonyítása. A problémát a gráf 6-színezés problémájára veztjük vissza. Ehhez rögzítsünk egy $\Gamma = (V, E)$ gráfot. A gráf csúcsai legyenek $\{v_1, v_2, \dots, v_n\}$, az élei $\{e_1, e_2, \dots, e_k\}$. Minden v_i csúcshoz hozzárendelünk egy x_i , e_j élhez pedig egy c_j változót. Tudjuk, hogy a visszafordító diszjunkt cserék szorzata. A bizonyítást az $R = (1, 2)(3, 4)$ esetben vázoljuk. Legyen

$$K = \{(1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), id\}.$$

Minden élre írjuk fel a következő egyenletet:

$$[c_l, x_i x_j^{-1}](1, 2)(3, 4)[c_l, x_i x_j^{-1}]^{-1} = (1, 3)(2, 4)$$

ahol az e_l él két végpontja v_i és v_j .

Mivel az $(1, 2)(3, 4)$ centralizátora K , pontosan akkor oldható meg az egyenletrendszer, ha $[c_l, x_i x_j^{-1}] \in K\sigma$, ahol $((1, 2)(3, 4))^\sigma = (1, 3)(2, 4)$.

A 9. lemma szerint az x_i, x_j párhoz pontosan akkor létezik olyan c_l , hogy $[c_l, x_i x_j^{-1}] \in K\sigma$, ha x_i és x_j a K csoport különböző mellékosztályaiban vannak. Ez azt jelenti, hogy az egyenletrendszer pontosan akkor oldható meg, ha minden csúcshoz hozzárendelhető egy mellékosztály úgy, hogy a szomszédos pontokhoz különbözőeket rendelünk. Ez pont a gráf hat színnel való kiszínezését jelenti.

Megfordítva, amennyiben adott a gráfnak egy hat színnel való színezése, ezt tekinthetjük úgy, mint a mellékosztályok egy hozzárendelését a csúcsokhoz. A változókhoz a megfelelő mellékosztály egy tetszőleges elemét hozzárendelve, a 9. lemma alapján, a c_l értékek megválaszthatóak úgy, hogy az egyenletrendszer egy megoldását kapjuk. \square

Ezek tükrében nézzük az általános eset bizonyítását.

A 7. tétel bizonyítása Az egyenlet megoldhatóságát elég volt a $G = G'$ esetben igazolni. Hasonlóan könnyen ellenőrizhető, hogy a tételt elég olyan csoportokra igazolni, melyekre $(\gamma, G) = G$ tetszőleges $\gamma \notin Z(G)$ esetén.

A általános problémát a gráf $|G : Z(G)|$ színnel való kiszínezésére vezetjük vissza. Mivel $[\gamma, G] = G$, ezért létezik olyan d_G konstans, hogy

$$G = \{[\gamma, y_1][\gamma, y_2] \cdots [\gamma, y_{d_G}] \mid y_i \in G\},$$

feltéve, hogy $\gamma \notin Z(G)$.

A korábbi jelöléseket használva, definiáljuk minden e élre a következő termet:

$$T_e(y) = [x_i x_i^{-1}, y_1][x_i x_i^{-1}, y_2][x_i x_i^{-1}, y_{d_g}].$$

A $T_e \equiv id$, ha $x_i x_j^{-1} \notin Z(G)$, egyébként az értékészlete az egész csoport.

Írjuk fel minden élre a következő egyenletet:

$$R^{T_e(y_e)} = A,$$

ahol az e él két végpontja a v_i, v_j . Pontosán akkor létezik olyan y_e vektor, hogy az egyenlőség fennáljon, ha $x_i x_j^{-1} \notin Z(G)$. Azaz pontosán akkor van megoldása az egyenletrendszernek, ha szomszédos v_i, v_j csúcsok esetén a változók értékei különböző mellékosztályokban vannak. Így a korábbiakhoz hasonlóan a gráf $|G : Z(G)|$ színnel való színezését kaptuk.

Megfordítva, ha a gráf színezhető, akkor az y_e értékei választhatóak úgy, hogy az egyenlőségek teljesüljenek. \square

Az itt felhasznált eszközök segítségével megválaszolható Szabó és Vértesi egy 2001-ben felvetett problémája is [8]:

1. Probléma. *Adott a szavak két halmaza, $\{t_1, t_2, \dots, t_n\}$ és $\{s_1, s_2, \dots, s_m\}$ a $G \leq S_k$ szimmetrikus csoport fölött, mely az $\Omega = \{1, 2, 3, \dots, k\}$ halmazon hat. Minden $l \in \Omega$ esetén legyen $I_l = \{t_1(l), t_2(l), \dots, t_n(l)\}$ és $J_l = \{s_1(l), s_2(l), \dots, s_m(l)\}$. Milyen bonyolultságelméleti osztályba sorolható az $I_1 = J_1, I_2 = J_2, \dots, I_k = J_k$ egyenlőségrendszer teljesülésének ellenőrzése.*

10. Tétel. *Adott a szavak két halmaza, $\{t_1, t_2, \dots, t_n\}$ és $\{s_1, s_2, \dots, s_m\}$ az S_3 szimmetrikus csoport fölött, mely az $\Omega = \{1, 2, 3\}$ halmazon hat. Minden $l \in \Omega$ esetén legyen $I_l = \{t_1(l), t_2(l), \dots, t_n(l)\}$ és $J_l = \{s_1(l), s_2(l), \dots, s_m(l)\}$. Ekkor annak eldöntése, hogy létezik-e olyan behelyettesítése a termeknek, hogy valamely $i \in \Omega$ elemre $I_i \neq J_i$, NP-teljes probléma.*

Bizonyítás. A problémát a gráf 6 színnel való színezésére vezetjük vissza. Ehhez rögzítsünk egy $\Gamma = (V, E)$ gráfot. A csúcsai legyenek $\{v_1, v_2, \dots, v_n\}$, az élei $\{e_1, e_2, \dots, e_k\}$. Minden v_i csúcshoz hozzárendelünk egy x_i minden e_j élhez pedig egy c_j változót. Ekkor minden e_l élre definiálunk egy w_l termet a következő módon: $w_l := [c_l, x_i x_j^{-1}]$ ahol a v_i, v_j az e_l él két végpontja. Legyen a szavak két halmaza $\{w_1, w_2, \dots, w_n\}$, és $\{id, w_1, w_2, \dots, w_n\}$, ahol az id az üres szót jelöli.

Mivel $[c_l, x_i x_j^{-1}] \in S'_3 = A_3$, ezért a w_i lehetséges értékei az $(1, 2, 3)$ az $(1, 3, 2)$ és az id permutációk. Így ha $w_l \neq id$, akkor c_l értéke megválasztható úgy, hogy adott behelyettesítéssel w_l lehetséges értéke az $(1, 2, 3)$ vagy az $(1, 3, 2)$ permutáció legyen.

Ha van olyan behelyettesítése a termeknek, hogy egyikük sem azonosan identitás, azaz $w_l = [c_l, x_i x_j^{-1}] \neq id$, pontosan akkor teljesül, ha $x_i \neq x_j$. Ha az S_3 minden elemét egy-egy színnel jelöljük, akkor ez pont a gráf 6-színezését jelenti. Megfordítva, ha adott a gráf 6 színnel való színezése, akkor a megfelelő színekhez tartozó S_3 beli elemet a termekbe helyettesítve egyikük sem lesz azonosan identitás, feltéve, hogy $c_l \neq id$.

Tehát a gráf pontosan akkor 6-színezhető, ha egyetlen term sem azonosan identitás. Ez pedig pontosan akkor teljesül, ha valamely $l \in \{1, 2, 3\}$ elem egyik termnek sem fixpontja adott behelyettesítésnél. Ez $I_l \neq J_l$ teljesülését jelenti. \square

Irodalomjegyzék

- [1] B. Bauer, Friedrich L. *Decrypteg Secrets, Methods and maxims of cryptology*, Springer-Verlag 2. kiadás, Berlin Heidelberg, (2000)
- [2] Horváth Gábor, Jonh Lawrence, Mérai László, Szabó Csaba, *The complexity of the word problem over finite non-solvable groups*, London Mathematical Society, megjelenés alatt
- [3] Kozaczuk, Wladyslaw, *Enigma*, London: Arms and Armour, (1984)
- [4] Mikael Goldmann, Alexander Russell *The compleyity of solving equations over finite groups*, Information and Computation, (2002) 178:253–262, Fourteenth Annual IEEE Conference on Computational Complexity. Atlanta, Georgia, (1999. május)
- [5] Rejewsky, Marian, *An application of the theory of permutations in breaking the Enigma cipher*, Applicationes Mathematicae XVI. évf. 4. szám, Varsó, (1980), <http://mad.home.cern.ch/frode/crypto/rew80.pdf>
- [6] Rejewsky, Marian, *How Polish mathematicians broke the Enigma cipher*, IEEE Annals of the history of computing, (July, 1981), 213–234
- [7] Singh, Simon *Kódkönyv*, Park Könyvkiadó, Budapest, (2002)
- [8] Szabó Csaba, Vértesi Vera, *The complexity of the word-problem for finite matrix rings*, Proc. Amer. Math. Soc. 132 (2004), 3689–3695
- [9] Tuma, Jiri, *Permutation Groups and the Solution of German Enigma Cipher*, Károly Egyetem, Prága, (2003)