DOI: https://doi.org/10.12700/btsz.2026.8.3.9

DEVELOPMENT OF SECRET LANGUAGES AND PRACTICAL ASPECTS OF ITS APPLICATION

A TITKOS NYELVEZET ALAKULÁSA ÉS ALKALMAZÁSÁNAK GYAKORLATI SZEMPONTJAI

MONDICS-KURMAY Lívia[1] – RAJNAI Zoltán[2]

Abstract

The concept of a secret language can cover many areas. It can be used for personal purposes, or as a means of secret communication for industrial or military purposes. This study takes a security-scientific approach to the topic of secret language. The first part of the paper introduces three main periods in the evolution of cryptography, followed by a more detailed analysis of three secret languages, where the author aims to examine the different aspects of the effectiveness of secret languages that have emerged in their application. Analysing this experience, the author draws conclusions that can be applied to warfare and security science.

Keywords

encryption, Enigma machine, Navaho, military coding, Caesar-coding, efficient coding

Absztrakt

A titkos nyelvezet, mint fogalom sok területet érinthet. Lehet személyes célokat szolgáló felhasználása, ipari vagy hadi célokból alkalmazott kommunikációs mód. Jelen tanulmányban biztonságtudományi szempontból kerül megközelítésre a titkos nyelvezet tematikája. A tanulmány első részében érintőleges bemutatásra kerül a rejtjelezés evolúciójának három főbb korszaka, majd három titkos nyelvezet kerül részletesebb elemzésre, ahol a szerző célja kivizsgálni a titkos nyelvezetek különböző hatékonysági szempontjait, amik megmutatkoztak alkalmazásuk során. Ezen tapasztalatokat elemezve a hadászat és biztonságtudomány számára is hasznosítható következtetéseket foglal össze.

Kulcsszavak

titkosítás, Enigma-gép, Navaho, katonai rejtjelezés, Caesar-kódolás, hatékony rejtjelezés

[1] m.kurmay.livia@uni-obuda.hu | ORCID: 0009-0000-2455-5148 | PhD Student, Óbuda University Doctoral School of Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] rajnai.zoltan@bgk.uni-obuda.hu | ORCID: 0000-0002-9139-736X | professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering, Budapest, Hungary | egyetemi tanár, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A hadászatban az idők folyamán bevett szokássá vált, hogy jeleket, kódokat, szókapcsolatokat vagy speciális nyelveket használtak az üzenetek titkosítására. Lényeges mozzanat volt a katonai cselekmények lebonyolításánál az üzenetek titkosítása. Bizonyos háborúk kimenetelének alakulását is befolyásolhatta az, hogy az üzenet el tud-e jutni egyik vezetési ponttól a másikig, illetve, hogy az információt meg tudta-e szerezni az ellenség. Az üzenettitkosítás mögötti elsődleges szempont a hatékonyság és az eszközigény volt. Amint a tanulmány során megfigyelhető, a technológia fejlődésével kiszélesedett az eszközhasználat is az adott területen. Míg Julius Caesar matematikusaira és nyelvészeire számíthatott katonai nyelvezetének titkosítása során, addig a II. világháború szereplői már egy komplikált eszközt tudtak igénybe venni. Az eszközök használatánál nagyon sok esetben a betűcserélés módszeréhez nyúltak vissza. Az a nyelvezet élt tovább megfejthetetlenül, melynél a cserélt betűk kombinációja bonyolultabb volt. Ezeken kívül volt még egy feltörhetetlen nyelvezet is. Írásomat tájékoztatásul ajánlom minden érdeklődő és hadi területen tevékenykedő részére.

A KÓDOLÁS FEJLŐDÉSI SZAKASZAI

Egy titkos nyelv értéke akkor mutatkozik meg, amikor éles helyzetben helyt tud állni. Az élet különféle területén tétje van az ilyen helyzeteknek. Gondoljunk egy szerelmes üzenetre, aminek kódolását közösen találták ki az érintettek és ily módon megmenekültek a szülők haragjától. Hadi síkon is megfigyelhető az üzenetek kódolásának fontossága, amiktől egy ország területének hovatartozása és emberek tucatjainak élete függ. Az emberiség titkosírás-evolúciója több szakaszon ment keresztül. Jelen írás szűk keretei miatt – korszakonként – csak néhány titkosítás-típus bemutatására kerül sor azért, hogy az olvasó egy általános képet kaphasson az adott korok titkosítási technikáiról.

Az ókorban többféle rejtjelezést alkalmaztak. A lehetőségeknek csak a rendelkezésre álló anyagok szabhattak határt. Az emberi kreativitás nem volt kérdéses, ezért érdekességképpen néhány példát szeretnék megemlíteni. Ilyen volt a Tűztáviratozás, ahol megfelelő számú fáklyák alkalmazásával üzentek, vagy a szolgák fejére írt üzenetek. Majd idővel egyre nagyobb teret kapott az ábécé betűinek játéka. A titkosítás ezzel a monoalfabetikus (jelentése: egy ábécé) módszer alkalmazása felé haladt. Példa e módszer alkalmazására a görögöknél (Kr.e. III sz.) használt szkütálé nevezetű tárgy, ami feltehetőleg a titkosítás egyik fő eszköze volt. Működése azon az elven alapult, hogy egy vékony bőrszíjat farúdra tekertek úgy, hogy a bőrsávok egymás mellett helyezkedjenek el. Ilyen módon került rá az üzenet, a betűket egymás mellé írták. Az üzenet célba juttatásánál csupán arra kellett ügyelni, hogy az összetekert, betűhalmazt tartalmazó bőrszíj épségben odaérjen. A dekódolása viszont már trükkösebb volt, mivel csak olyan farúdra visszatekerve volt értelmezhető az üzenet tartalma, melynek vastagsága megegyezett az eredeti farúd vastagságával. [1]. Korabeli feljegyzésekből feltehető, hogy Kr. e. 404-ben Lüszandrosz spártai hadvezér időben értesülhetett a perzsa támadásról ennek az eszköznek a segítségével, így fel tudott készülni a támadásra. [2]

1. ábra: Szkütálé
(Forrás:Wikipedia https://hu.wikipedia.org/wiki/Szk%C3%BCtale)

A rómaiaknál a Julius Caesarról elnevezet ún. Caesar-titkosítással juttatták célba a rejtett üzeneteket. Ezt a betűeltoláson alapuló módszert írásomban részletesebben fogom elemezni. Eszközigénye nem túl nagy, ezért feltöréséig jó szolgálatot tehetett. [3]

A középkorban a titkosírás virágkorát élte. A különböző irányú törekvések alapja a betűkkel, számokkal, szimbólumokkal való kísérletezés volt. A titkos nyelvezet alkalmazása olyan méreteket öltött, hogy bizonyos országokban hivatalos titoknoki feladatkörökkel bízták meg az erre rátermetteket. A kor egyik fő iránya a monoalfabetikus módszer alkalmazása volt, és annak tovább gondolása *„az azonos betűk helyett azonos, különböző betűk helyett különböző karakterek állnak a kódolt szövegben."* [4] Ekkor jelent meg az első nyomtatott kriptológia könyv is Johannes Trithemius (1462-1516) tollából. [3, p. 20] Trithemius módszerének tovább gondolása volt a szólajstromok alkalmazása, ahol a szöveg bizonyos szavait szimbólumokkal jelölték. Megfejtéséhez teljes kódkönyvekre volt szükség. Említést érdemel a Nagy Kód, az ún. Grand Chiffre, amit Antoine és Bonaventure Rossignol 1650 körül dolgozott ki és a Napkirály üzeneteit hivatott titkosítani.

Az újkorban a rejtjelezők egyre bonyolultabb kódolásokhoz folyamodhattak. Ennek oka a nagyléptékű tudományos fejlődés, mely érinti a matematika területét is. Továbbá, műszaki szempontból a rejtjelezők felhasználhatták az adott kor vívmányait és ezek segítségével mechanikus titkosító gépeket hozhattak létre. Gyors és hatékony rejtjelezésre volt szükség, melynek segítségével titokban tarthatták a személyes és hadi információn túl az ütemesen fejlődő gazdasági szegmensek információját is. Kiemelhető a polialfabetikus rejtjelezés, melynek alapja a többféle kódábécé egyidejű alkalmazása. Egyik legismertebb példája a Vigenère-kódolás, ami Blaise de Vigenère francia tudós nevéhez fűződik. Kódolását a Traicte de Chiffres című művében. Itt több kódábécé egyidejű használata történik, egy elgondolt rendszernek megfelelően.[5]

További jelentős titkosítási módszer a Morzekódolás, mely Samuel Morse nevéhez kötődik. A módszer abban rejlik, hogy a leggyakrabban előforduló betűknél a leggyorsabban leadható kód alkalmazását használta.[6] Érdekessége ennek a titkosítási módszernek, hogy kinőtte magát egy nemzetközi kommunikációs és hírközlési rendszerré, ugyanis a 19. század végére a „Morze"-kód nemzetközivé vált. Az angol nyelv karakterein kívül egyéb karaktereket is bevontak a kódolásba, ezáltal nem csak egy adott szűk kör hírközlési igényét látta el. A tengerentúlon is alkalmazták. [7]

Az Enigma (gör. rejtély) kódtárcsás gép (1920 körül) feltalálása az újkor kiemelkedő vívmánya lett. Ez a találmány forradalmasította a rejtjelezést. Az elektromosságról és

rádióhullámokról megszerzett tudás ebben az írógép nagyságú gépben ötvöződött. Feltalálója Arthur Scherbius német mérnök volt. Az Enigma-kódolást a későbbiekben részletesebben is bemutatom. [3, pp. 17-18]

A rejtjelezés evolúciójának három főbb korszaka került érintőlegesen bemutatásra tanulmányomban. A fejlődést három nagy csoportra – üzenetrejtés, helyettesítési, illetve keveréses módszerre – oszthatjuk. Napjaink jellemző titkosítási módszere az aszimmetrikus titkosítás, melyre írásomban nem térek ki. [5, p. 476]

TITKOSÍTÁS KÖZELEBBRŐL

A továbbiakban három titkos nyelvezet elemzésére kerül sor. Az üzenet titkosításának célja van, ezért érdemes ebből a szempontból is elemezni a rejtjelezést. Fontos továbbá kitérnünk arra, milyen eszközökre volt szükség az adott titkos nyelv alkalmazása során, illetve az adott titkos nyelvezettel mennyire sikerült a célt elérni élő helyzetekben, és az események menetét hogyan tudta befolyásolni annak alkalmazása.

1. Caesar-titkosítás

A monoalfabetikus betűhelyettesítés ékes példája ez a módszer. Pontos források nincsenek arra vonatkozólag, hogy a kódot személyesen Caesar találta-e fel. Arra vonatkozólag viszont maradtak fenn források, hogy Caesar egyik tanítójától, Marcus Antonius Gnipho-tól sajátította el a nyelvhelyesség és nyelvművelés magas fokát, ami megmutatkozott beszédeiben és írásaiban is. [8]

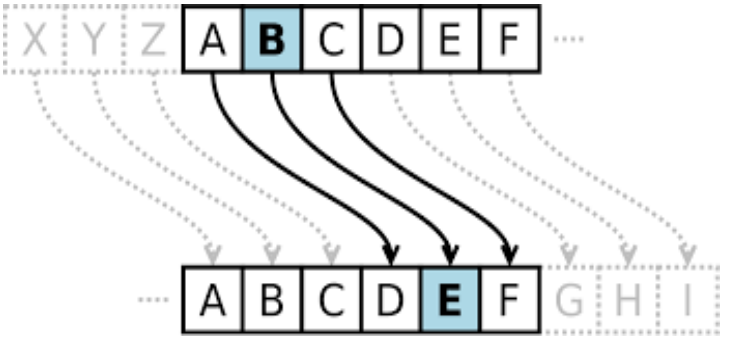
Julius Caesar számos írása közül csak a galliai hadjárata és a polgárháború története maradt fenn az utókornak „Commentarii" címen. (Kiadta újabban Nipperdey, Lipcse 1847, és Schneider, Halle 1855, 2. kötet.) Ezen emlékiratok *„világos, kedves nyelvezetök, s a leírások szemlélhető volta miatt példányszerűek"*. Caesar a hárombetűs eltolást alkalmazta katonai levelezései során.[2]

Tehát ezek alapján következtethetünk arra, hogy a nyelv művelője volt és nem meglepő, hogy a kód kifejlesztésére pont az ő ideje alatt kerülhetett sor.

A Caesar-kód az egyik legrégebbi és legelterjedtebb titkosítási eljárás, mely során egy betű helyettesíti a tőle meghatározott távolságra lévő betűt. A váltás lehet pl. az 5.

abc	5	fgh

Az alábbi ábra szemléltetheti:



2. ábra: Caesar-kódolás
(Forrás: https://s4scoding.com/caesar-cipher-python-code/)

Az adott ábrán a 4-es helyettesítést látjuk. Pl.: Holnap reggel nyolckor találkozunk. CAESAR-KÓDDAL: Ubyancerttryalbypxbegnyáyxbmhax.[9]

Ez a típusú kódolás monoalfabetikus, viszonylag egyszerű, nem eszközigényes és számos további fejlesztésnek szolgált alapul. Egyszerűségéből adódóan a monoalfabetikus kódolás feltörése nem egy bonyolult feladat, csupán okos megközelítést igényel. A kódfeltörőnek arra is oda kell figyelnie, hogy lehetnek megtévesztő betűk, szimbólumok.

3. ábra: Caesar-korong
(Forrás:https://www.cryptomuseum.com/crypto/caesar/linge.htm)

A fenti ábrán látható egy Caesar-korong, amely egy modern eszköz. Ez a korong szemlélteti a Caesar-kódolás alapműködését. A legszélső sor a hagyományos ábécét tartalmazza, az alatta futó sor pedig az adott betű kódolt megfelelőjét.

A monoalfabetikus rejtjelezést sok esetben továbbfejlesztették. A továbbfejlesztések egyik módszere, hogy szimbólumokat helyeztek bizonyos betűk helyett. Egy ehhez hasonló, modernebb Caesar-kódot alkalmaztak az I. Erzsébet angol királynő elleni összeesküvésben is, ahol maradt a monoalfabetikus rejtjel és az egyes szavak helyettesítése. A skót királynő, Stuart Mária ezzel a módszerrel folytatta levelezését Anthony Babingtonnal, aki társaival együtt Stuart Máriát a trónra szerette volna juttatni. Lord Francis Walsinghjamne, az angol királynő kémfőnöke, megszerezte az üzeneteket és matematikusainak tudására támaszkodva megfejtette azokat – a bizonyíték elegendő volt ahhoz, hogy az összeesküvőket kivégezzék. [5, pp. 477-481]

Az amerikai polgárháborúban is ezt a kódot alkalmazták. A déliek csapatüzeneteiket ilyen kódolási módszerrel továbbították. [2]. Ezt bizonyítja a Konföderációs Múzeumban 1896 óta üvegszelencében őrzött üzenet, mely 1863-ban keletkezett és a következőket tartalmazta:

„Pemberton százados, a folyó túloldaláról ne várjon segítséget. Tudassa Johnston tábornokkal, – ha van rá módja – hogy mikor tudná megtámadni az ellenséget vele együtt.

Informáljon engem is, én majd megpróbálok elterelést indítani. Küldtem néhány robbanószerkezetet és mellékelem Johnston sürgönyét." [10]

Valószínűnek tartják, hogy az üzenet küldője John G. Walker főparancsnok volt. Az üzenetben szereplő Joseph E. Johnston tábornok 32 000 fős sereggel Vicksburgtól délre táborozott le, hogy megvédje Pemberton seregét egy másik, 35 000 fős sereg támadásától. A kódolt üzenetet 1863. július 4-én írták, azon a napon, amikor John C. Pemberton megadta magát Ulysses S. Grantnek, az unionista csapatok vezetőjének. Ezzel véget ért a Mississippi mentén fekvő Vicksburg ostroma, mely hetek óta tartott és a háború egyik fordulópontjának számít. Nincsenek források arra vonatkozólag, hogy az említett üzenet eljutott-e a parancsnokhoz. Az üzenetet a konföderációs csapatok vicksburgi parancsnoka azon a napon kellett volna, hogy megkapja, amikor az unionista csapatok bevették a várost.

Az üvegszelence felbontását a múzeum igazgatónője szorgalmazta. A szelence felnyitásánál látták, hogy a papíron szereplő üzenet kódolt. A kódolt írást többen próbálták megfejteni, de sikertelenül. Az írás megfejtője végül David Gaddy volt, a CIA egyik nyugalmazott szakértője. [10]

A Caesar-kód mára inkább érdekesség, mint biztonságos kommunikációt nyújtó rejtjelezési módszer. Mára eléggé közismert és inkább oktatási célokra használható. Gyors és nem túl bonyolult, ami adott körülmények között előnyös, viszont ugyanúgy gyorsan és nem túl sok erőfeszítéssel megfejthető, amennyiben tájékozottak vagyunk e módszer felől. A rejtjelezés fejlődési szakaszának azon módszere, mely sok más módszer alapjául szolgálhatott.

2. Enigma-kódolás

Az I. világháború időszaka a mechanikai fejlődések időszaka is egyben, ami még inkább fellendítette a titkosító eljárások fejlődését. Fontos szempont volt a gyorsaság és a minél kreatívabb alapokon nyugvó megfejthetetlenség. Nyilvánvalóvá vált, hogy a biztonságos, nehezen megfejthető, harctéri körülmények között is jól alkalmazható módszerek jelentősen, akár döntő módon is befolyásolhatják a harctéri helyzetet. Ezen szempontokat figyelembe véve nyújtotta be 1919-ben egy német mérnök, Arthur Scherbius Enigma nevű gépének szabadalmát (Enigma, görögül – titok, szerz.), melyet a tökéletesen biztos kommunikációhoz tervezett. Bármily meglepő, de az akkori katonai hadvezetést nem érdekelte a gép, így néhány éven át a készülék a civil szférát szolgálta ki. Fizikai adottságai eltértek a későbbi, továbbfejlesztett titkosíró Enigma modelltől – súlya 12 kg volt és rendkívül bonyolultnak bizonyult, 7-11 tárcsával rendelkezett a későbbi 3-4 tárcsás géppel szemben. Végül a gép áttervezése után már a német hadi vezetés alkalmazni kezdte. [11]

Az Enigma gépnél alkalmazott módszer a már eddigiek során is ismertetett betűcserélő módszer továbbfejlesztett változata. Az alapvető betűcserés módszernél a cserélt betűk kombinációja nem változik. Az Enigma erőssége pedig pont ebben rejlett – a betűk kombinációjának változásában, ahol a három tárcsa 17 576 lépésben összesen 26x26x26 különböző állásban tudott megállni. Ezen kívül a kivehető-betehető tárcsák sorrendjét is szabadon lehet változtatni. Műszaki szempontból maga a szerkezet nem bonyolult. Elektromos felépítésű készülék, melyet egy elem táplált. Kapcsolók sorából és a rájuk kötött izzólámpákból tevődött össze. *„Az Enigma ezen túlmenően belül huzalozott tárcsák egymásutánja, írógépszerű klaviatúra, amelynek betűinek lenyomásával egy kapcsolót aktiválunk.*

Az áram a tárcsákon keresztül haladva, egy reflektor, azaz visszafordító tárcsán visszaindulva ugyanazokon a tárcsákon keresztül, de már más útvonalon elér az adott lámpáig, amely felvillan"

„A leütött billentyűk mechanikusan egy kilincsszerkezetet mozgatnak meg, ami hatására az elektromos jel már egy teljes más utat fog bejárni (...) a tárcsa huszonhat betű lenyomása után ér el egy teljes fordulatot." [11]

Ami a megfejthetőséget illette, mivel minden tárcsa huzalozása egyedi volt, a két készülék csak akkor tudta értelmezni a kódolt üzenetet, ha mindkét gépben azonos sorszámú és jelzésű tárcsák voltak beépítve, méghozzá megegyező sorrendben. *„Az eszközök tárcsái kiemelt védelmet élveztek az üzemeltető állomány részéről, azok az érvényben lévő szabályok szerint semmiképpen nem kerülhettek ellenséges kézbe."* [11]

Akkor még kevesen gondolták volna, hogy ez a gép lesz talán a leghíresebb eszköz a titkosítások több évezredes története során. A gép használata viszonylag egyszerű, az általa generált kódok viszont nagyon bonyolultak. Ez az oka annak, hogy a német kormány ezt a gépet választotta a második világháború idején a katonai jelentések nagyobb részének a rejtjelezésére. A kódolt üzenetek megfejtése olyan szempontból vált bonyolulttá az ellenség számára, hogy azon kívül, hogy azonos sorszámú, jelzésű, megegyező sorrendben elhelyezett tárcsák kellett, hogy küldjék-fogadják az adott üzenetet, még haderőnemeken belül is eltérő tárcsák kerültek kiosztásra. Például a haditengerészet által használt készülékpár kommunikációját a légierő rejtjelezői nem tudták megfejteni. Ha a két haderőnem egymással kívánt kommunikálni, akkor a vonal mindkét végén azonos jelzésű tárcsákat kellett behelyezni és a többi beállításnak is meg kellett egyeznie. Az eszközhöz társult a kódkönyv, mely egy hónapnyi beállítást tartalmazott.

4. ábra: Enigma M3 használatban
(Forrás: https://www.cryptomuseum.com)

A fenti kép egy Enigma M3-at ábrázol a német U-124 tengeralattjárón. Az Enigma a kép bal alsó részén látható, jobboldalt pedig a kódkönyvet láthatjuk. A fénykép 1941 márciusában készült, rá egy évre már az Enigma M4 volt használatban.[12] (ford. angolról-szerző)

5. ábra: Enigma-tárcsák.
(Forrás: https://www.cryptomuseum.com)

Az Enigma kódjainak megfejtése első ízben lengyel szakemberek munkája volt. Nagy erőfeszítéssel, rögzített üzenetek és régi kódkönyvek alapján reprodukálták a gépet és működésének elvét. Marian Rejewski matematikus vezetésével dolgoztak, eredményeiket pedig 1939. szeptember 1-je előtt adták át az angol és francia szakértőknek. A későbbi események ellehetetlenítették a lengyel siker megkoronázását a kódfejtés terén. A munkát az ULTRA nevű csoport tudta továbbvinni a londoni Blechley Parkban kihelyezett bázisán. A munkacsoport matematikusokból, nyelvészekből és más szakemberekből állt. A lengyel kódfejtő gép mintájára megépült a „Bomba" nevű gép, mely *„az üzenetváltásokban rejlő szokások adta hibákat kihasználva addig pörgette a lehetséges beállításokat, amíg nem talált egy értelmes szót. Ha ez megtörtént, az aznapi összes távirat megfejthetővé vált azzal a beállítással, amelyet a Bomba rögzített"*.[11]

Az Enigma kódok feltörése a II. világháború egész folyamatára hatással volt. Kiemelném a haditengerészet titkos harcát, melynek fordulatait nagy részben az Enigma kódgép használata befolyásolta. Míg az Enigma I kódgép üzeneteit a szövetségesek 1940-től sikeresen feltörték, a német haditengerészet újabb, speciális modelljei nehezen voltak feltörhetőek az angol kódfejtők számára. A HMS Bulldog brit akció után - 1941 májusában -, a Brit Királyi Haditengerészetnek sikerült megszereznie egy Enigma M3 modellt és a hozzá tartozó kódkönyvet egy német tengeralattjáróról. Ennek segítségével sikeresen fel tudták törni az ilyen típusról érkező üzeneteket. A német haditengerészet 1942-ben egy további fejlesztéseken átesett gépet, az Enigma M4-et vetette be.

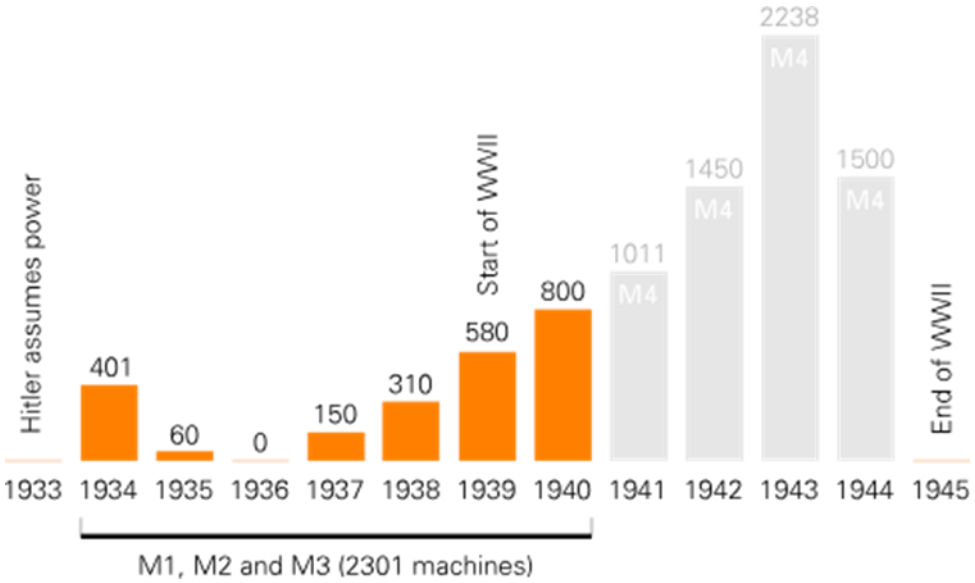
6. ábra: Enigma M3
(Forrás: https://www.cryptomuseum.com)

7. ábra: Enigma M4
(Forrás: https://www.cryptomuseum.com)

Ezeket az üzeneteket a Bletchley Park kódtörői 10 hónapon át nem tudták feltörni. Ezt az időszakot „blackout"-nak (angolul – áramszünet, szerz.) nevezik, mivel katasztrofálisak voltak a brit katonai műveletek, különösen a német tengeralattjárók elleni harc szempontjából, hiszen szó szerint is a „sötétben tapogatóztak". A német hadierő az Enigma M4 modell mellé „Triton kulcshálózat" nevű kódkönyvet készített, mely szigorúan titkos volt. Azért, hogy ne kerüljön az ellenség kezébe, vízben oldódó tintával itatóspapírra nyomtatták, hogy lehetővé tegyék gyors megsemmisítését. A szövetségesek mégis hozzá tudtak jutni a saját kódfejtőik számára fontos információhoz. Az angol erők felszínre kényszerítették az U 559-es német tengeralattjárót 1942. október 30.-án, mely hamarosan süllyedni kezdett a mélységi töltetek által megrongálva. Ennek ellenére a legénység több tagja behatolt a tengeralattjáróba és megmentette az Enigma M4 kódkönyveket (jelzőfüzeteket és az időjárási rövid kulcsot).

Rövid jelzőfüzeteket és időjárási rövid kódokat használtak a gyakran használt kifejezések - például időjárás-jelentések, mondatok, parancsok és hasonlók titkos betűkombinációk - összehasonlítására. Ezek az anyagok elegendőek voltak a Bletchley Park kódtörőinek, így ezt követően már sikeresen fel tudták törni a német haditengerészet rádiókommunikációját. A dokumentumok mentése szigorúan titkos maradt, hogy a németek ne változtassák meg újra a titkosítási rendszerüket. A matrózok bevetése és a kódtörők munkája jelentősen lerövidítette a szövetségesek harcát a német tengeralattjárók ellen és ezzel a II. világháborút.[13] (ford. németről – szerz.)

Az alábbi ábra szemlélteti az évszámokat és az Enigma típus-gyártásoknak a folyamatát.



8. ábra: Enigma gépek gyártása és használata
(Forrás: https://www.cryptomuseum.com)

A leírtak alapján egyértelművé válik, hogy az Enigma megfejtése lehetetlennek bizonyulna, amennyiben a kódfejtők nem rendelkeznek megfejtési támpontokkal, legalább egy megfejtési útvonalat tartalmazó, akár egyetlenegy mondattal. A szövetségesek rendelkezésére állt valamennyi eszköz, visszafejtett üzeneteken kívül kódkönyvek, sőt még Enigma gépek is birtokukba kerültek. Vitathatatlan, hogy rendkívüli és összehangolt munka kellett ahhoz, hogy a tényleges üzenetek értelmezhetőek legyenek. Az olyan intelligens gépek létrehozása, mint a fent említett „Bomba" kódfejtő gép az emberi logikának egyik zseniális találmánya, mely felismerve egy rendszerezettséget meg tudta fejteni a bonyolult kódcsomagokat.

A rendszer mindenhatósága mégis megcáfolható. A következő részben olyan titkosítási módszerre szeretnék kitérni, mely a rendszertelenségnek köszönhette kiváló helytállását.

3. Kódbeszélők

A titkosítás egyik különleges módszere az, amikor egy ritka nyelvet használnak fel titkosítási céllal, az ebben aktívan szereplőket pedig kódbeszélőknek hívják. Több ilyen alkalmazás is előfordulhatott, hiszen a különböző nyelvek dialektusai néha a felismerhetetlenségig meg tudták változtatni az adott nyelvet. Jelen írásomban azonban a titkosításnak egy történelmileg is kiemelkedő példáját szeretném említeni az élő nyelv felhasználásának területéről.

A második világháborúban az USA haditengerészete a Navaho indiánok nyelvét használta biztonsági kommunikációra. Az ötlet Philip Johns mérnöktől származott, aki a Navaho Rezervátumban nőtt fel, mivel édesapja misszionáriusként szolgált ott. Philip Johns egyike volt azon nagyon kevés nem-navahoinak, aki folyékonyan beszélte a nyelvet. Első világháborús veteránként rálátása volt arra, hogy milyen fontos a megfelelő kommunikáció,

és milyen értéke van a titkos rejtjelezésnek. Az amerikai katonai sikertelenségek láttán, melyek javarészt a nem megfelelő kommunikációból eredtek, javasolta, hogy a haditengerészet titkos nyelvezetének alapja a navaho nyelv legyen. Javaslatának egyik meggyőző érve, hogy egyetlen szót, ha négyféleképpen ejtenek, négyféle jelentése lesz. Élőben, navahoi barátain keresztül demonstrálta, hogyan tudtak fordítani angol nyelvről navahói nyelvre és vissza. Ezek után a tengerészgyalogság egy hivatalos programot indított el az új kódok kidolgozására. Huszonkilenc olyan navahói indiánt alkalmaztak, akik angolul és navaho nyelven is folyékonyan beszéltek (volt köztük, aki csak 15 éves volt). Segítségükkel kidolgoztak egy navaho kódnyelvet, melyet kipróbáltak szimulált csatákban. [14] (ford. angolról – szerz.)

A következő tényezők játszottak szerepet a nyelv megfejthetetlenségében: a Navaho nyelv nem rendelkezett írásos elemekkel, sem betűkkel, sem szimbólumokkal. Nyelvtana és a hanglejtésből adódó jelentésbeli különbségek még inkább komplikálttá teszik. A nyelvet csak a navahók lakta területen használták, Amerika dél-nyugati részén. Becslések szerint harminc nem-navaho tudott beszélni ezen a nyelven, viszont közülük senki sem tudott japánul. A tengerészetnél kifejlesztett nyelvezet azonban nem a hétköznapi kommunikációhoz használt navaho nyelvből állt. Az első huszonkilenc kódbeszélővel fejlesztették ki a titkos nyelvezetet. A katonai kifejezésekhez a természetből választottak szavakat, többek között azért is, mert nem volt erre való szókincs – pl. a navahó „bagoly” szó a megfigyelő repülőt jelentette: ne-ahs-jah (navaho) – observationplane (ang.), a navahó „vas hal” a tengeralattjárót jelentette: besh-lo (navaho) – submarine (ang.).

9. ábra: Navahói kódbeszélők
(Forrás: https://www.army.mil/nativeamericans/code_talkers.html)

A kódolást megkönnyítette az is, hogy körülbelül négyszázötven, az előzőekhez hasonló katonai kifejezést alkalmaztak. Ezeken a kifejezéseken kívül a következő rejtjelezést kapták a szavak: amikor a kódbeszélő üzenetet kapott, akkor összefüggéstelen, egymás

mellé rakott navaho szavakat hallott. A kódbeszélőnek először minden navaho szót angolra kellett fordítania. Ezt követően az angol szavaknak csak az első betűit használta úgy, hogy abból értelmes angol szó keletkezzen. Például, az angol NAVY szó navaho kóddal a következőképpen alakul: „tsah (**n**eedle) wol-la-chee (**a**nt) ah-keh-di-glini (**v**ictor) tsah-ah-dzoh (**y**ucca). Az ilyen módon kapott szó volt a megfejtés. A betűk gyakoriságától függően egy betűnek három vagy két navaho szó volt a megfelelője. Ezeket a kódbeszélőknek meg kellett tanulniuk, hogy akadálytalanul folyhasson a kommunikáció. A kódbeszélők rendkívüli precizitással dolgoztak. Az Ivo Dzsima-i csatában hat kódbeszélő dolgozott két napon át, több mint 800 üzenetet fogadtak és továbbítottak hibátlanul. Howard Connor, az 5. Tengerészeti hadosztály egykori vezetője szerint a navahók nélkül ez az akció nem lett volna sikeres. E háborún kívül a kódbeszélőket az 1950-es években Koreában, az 1960-as években Vietnámban is alkalmazták." [15] [16] [17] (ford. angolról – szerz.)

Amint láthatjuk, nem volt elegendő egyszerűen a navaho nyelv a titkos kommunikációhoz. Ezt a nyelvet egy kódnyelv alapjaként használták. Ennek a technikának a segítségével a hadsereg felkészült volt azzal szemben, ha az ellenség esetleg foglyul ejt egy navaho nyelven beszélőt – de nem kódbeszélőt. Egy titkos nyelvezetre nem kiképzett navaho katona nem tudta megfejteni a kódolt üzeneteket. Erre a kódnyelvre speciális képzést kaptak a kódbeszélők. Természetesen az Amerikai Haditengerészet fokozott védelem mellett alkalmazta a kódbeszélőket. Ahogy a németek védték az Enigma gépeiket és a kódkönyveiket, úgy meg kellett védeni a kódbeszélőket is, akik általában két fős csoportban dolgoztak. Telefont vagy walkie-talkie eszközt használtak, jelentették a légicsapásokat és tüzérségi bombázásokat, közvetítették a csapatok mozgásának irányítását, jelentették az ellenséges helyszíneket, irányították a csapásokat az amerikai állásokból, és szenzitív katonai információkat osztottak meg. [14] (ford.angolról-szerz.)

10. ábra: Veterán navaho kódbeszélő
(Forrás: https://www.aarp.org/politics-society/history/info-2021/pearl-harbor-thomas-begay.html)

Jelen szakasznál a három titkos nyelvezet elemzésének végéhez értünk. A leírtak alapján látható, a három kódolásnál a cél ugyanaz, célba juttatni az üzenetet anélkül, hogy arról más tudomást szerezzen. Minden esetnél a kreativitás és az adott körülmények játszottak szerepet. A Caesar-kódolásnál az ábécé matematikai rendszerezésével játszottak, az Enigmánál pedig már szükséges volt az addigra feltalált tudományos vívmányok - elektromágnesesség és mérnöki tudásbázis fejlettsége - alkalmazása, ami adott volt az akkori Európában. A navaho nyelv alkalmazásánál pedig kellett a szikra - az ötlet és a katonai igények ismerete -, hogy a nyelvet alkalmazásba tudják venni és felismerjék a nyelv egyedi adottságait.

KÖVETKEZTETÉSEK ÉS KUTATÁSI EREDMÉNYEK

Kutatásom során a következő következtetésekre jutottam a titkos nyelvezet alkalmazásával kapcsolatosan. Mivel a titkos nyelvezet alkalmazása legtöbbször nehéz és feszült időszakban történik, a legfontosabb szempont a gyorsaság, kevés eszközigénnyel. A három vizsgált nyelv közül az élő nyelv alkalmazása volt a legeredményesebb. A navaho kódbeszélők betanítás után hibátlanul tudták közvetíteni a kódolt üzeneteket. Az Enigma géphez képest, egy háromsoros angol üzenet közvetítése a navaho kódbeszélőknél 20 másodpercbe, míg egy gépnél ugyanez a feladat harminc percbe telt.[18] (ford. angolról – szerz.)

Az alábbiakban a következő szempontokból vizsgáltam meg az eddig részletesebben említett titkosítási eljárásokat: megfejthetetlenség, betaníthatóság, sérülékenység/biztonság, célba érés biztonsága, rugalmasság, használhatóság ideje. Az összehasonlítás alapján az alábbi következtetésekre jutottam:

- **megfejthetetlenség** – a leggyengébb eredményeket az adott esetben a Caesar-kód mutatta, bár abban a korban, amikor feltalálták és alkalmazták, lehetséges, hogy az 1940-es évek Enigma-gépének felelt meg. Az újkorban azonban már nem tudta megállni a helyét, csak olyan környezetben, ahol nem tudtak róla (lásd az amerikai polgárháború, ahol feltehetőleg általánosságban nem sokat tudhattak a Caesar-titkosításról). Az újkorban az európai vezető réteg általános műveltsége magas volt, mivel egyre többet foglalkoztak az ókor vizsgálatával. Tudtak a Caesar-kódolásról és alkalmazták is, és további fejlesztéseknek vetették alá. *Ennél a pontnál úgy vélem, a műveltség, a tudás fontos szempont a titkosítás területén. Hadászati szempontból a hadi elitet fontos kiképezni a titkosírás történetére, hisz az Enigma gép is némileg a Caesar-kódolásnak az alapjait alkalmazta. Az, hogy a jó eséllyel megfejthetetlennek létrehozott Enigma gép mégis megfejthető lett – az a rendszeres előfordulásának az eredménye és annak, hogy megszerezték magát a gépet és a kódkönyveket, így a titkos nyelvezetre fény derült.* A mérnökök, nyelvészek már vissza tudták fejteni, mert rájöttek a rendszerre és rendszerességre, a gyakoriságra, mely zöld utat mutatott a megfejtés és dekódolás felé. Ezzel szemben a navahi nyelv feltörhetetlen volt. A szakképzett japán kódfejtők fel tudták törni az Amerikai Hadsereg és Légierő kódolásait, de a navaho kódbeszélőket alkalmazó hadi tengerészetét nem. A navaho nyelvnek nem volt „nyoma” – hiszen írásnélküliségen alapult, tehát az ellenség nem tudott utána kutatni. *Az emberi nyelv rendszertelenségeket is tartalmaz, melyeket nem lehet kiszűrni, ezzel erősebb, mint egy tökéletes rendszeren alapuló eszköz, mint pl. az Enigma gép. Bonyolult és kis csoportoknál használt élő nyelvek alkalmazása tehát jó alapként szolgálhat egy kódnyelv létrehozásánál. A*

történelem során megmutatkozik, hogy ez volt az egyik leghatékonyabb módszer. Körültekintően lehet csak alkalmazni az adott megoldást, mivel, néprajzkutatókkal fel lehet deríteni a legtávolibb vidékek nyelvi sajátosságait is, ahogyan ezt a német felderítők is tették, ők azonban nem kutattak tengerentúl, továbbá, kevesebb eszközük is volt erre a II. világháború környékén.

- **betaníthatóság** – mennyi időt vesz igénybe egy titkos nyelv megtanulása és alkalmazása ténylegesen, feszült és szoros határidők mellett, mint amikkel meg kell küzdeni a hadseregnél. A Caesar-kódolásnál az idők során kifejlesztettek egy Caesar-korongot is, mely jelentősen lerövidítette a kódolás és dekódolás idejét, Az Enigma gép tette a dolgát, megfelelő tárcsák és kódkönyvek mellett a dekódolás nem jelentett különösebb nehézséget. A gép kezelését és a kódkönyvek alkalmazását kellett megtanulni. A navaho titkos nyelvezetnél a kódbeszélőknek meg kellett tanulniuk a kódszavakat és a kifejezéseket. Az Enigma és a navaho kódolásnál a kiképzési idő maximum egy hónapra tehető. *Tehát fontos az idővel való számolás, a felkészültség és az előre kiképzett szakemberek megléte.*
- **sérülékenység, biztonság** – mind fizikai tárgyaknál, mind emberek alkalmazásánál – fennáll a sérülékenység kérdése. Az Enigma gép meghibásodásai további kutatást igényelnek. Az a tény áll rendelkezésre jelen írás keretein belül, hogy a gépet meg tudták szerezni és ebben az esetben a nyelv titkosságánál vesztett ügyről volt szó. A navaho indiánok sérülékenysége emberi szempontból fennáll, hisz előfordulhat, hogy az ellenség foglyul ejthet egy kódbeszélőt, és a történelem során alkalmazott kegyetlenségekkel szóra bírhatja. Ez történt egy navaho katonával is, aki azonban nem volt kódbeszélő. A katonát a japánok foglyul ejtették Bataan mellett, nem tudták szóra bírni. A katona azonban, mivel nem volt kódbeszélő, ezért nem értette a navahón alapuló kódnyelvet. *Ez az eset arra mutat rá, hogy nem elegendő egy katonai titkosításra alkalmas nyelv, azt tovább kell fejleszteni. A kódbeszélőket pedig minden áron védeni, ahogy ez sikerült is az amerikai tengerészetnél.*
- **célba érés biztonsága** – az Enigma gépnél az üzenet célba érése garantált volt, hiszen két egyforma típusú készülék tudta csak küldeni-fogadni az üzeneteket. A német hadiflotta vezetése azonban nem volt eléggé körültekintő, hiszen a szövetségesek megszerezték az Enigma M4 modellt a németek tudomása nélkül és annyira okosan leplezték, hogy megszerezték, hogy akár saját veszteségeket is elviseltek, csak hogy ne derüljön ki a tény. *Ennél az esetnél láthatjuk, mennyire kétélű a garantált biztonság, amennyiben egy készülék alkalmazására kerül sor. Törekedni kell arra, hogy ellenőrizhető legyen, amennyiben más is hozzáfért a készülékhez. A kódbeszélők esetéből az a tapasztalat, hogy a fogadó környezet biztonsága garantált legyen.*
- **rugalmasság** - rugalmas megoldások alkalmazása – a három vizsgált nyelvből csak is a kódbeszélők esetében tapasztalható – a japánokkal való harcnál egyik esetben az amerikaiak saját csapatukat lőtték, mert azt hitték, hogy azon a bizonyos területen japánok tartózkodnak. Csak a navaho kódbeszélők gyors bevetésével tudták őket megállítani, mert az angol nyelven adott parancsra azt hitték, hogy a japánok trükkje.[15] *Mivel ennél a nyelvnél nincs eszközigény, csupán az adó-vevő készülék, vagy, az adott esetnél – egy-egy kódbeszélő jelenléte, ezért rugalmasabban alkalmazható.*

- **használhatóság ideje**, vagy mennyi ideig tud szolgálni az adott titkos nyelv – a navaho kódnyelv egészen az 1960-as évek végéig szolgálta az amerikai hadsereget, ami azt mutatja, hogy tökéletesen bevált és megfelelt a katonai igényeknek.

Az alábbiakban a 3 titkosítási nyelvezet került összehasonlításra a leghatékonyabb eljárás kimutatására a szerző kutatásai alapján, az MI segítségével:

Szempont	Caesar-kód	Enigma-gép	Navaho kód
Megfejthetetlenség	**Legalacsonyabb.** Az újkorban már ismert volt az általános műveltség miatt. Saját korában alacsony általános műveltség mellett jól alkalmazható lehetett.	**Közepes.** Elméletileg egyik legerősebb, de a rendszeresség és a gép megszerzése miatt feltörhető.	**Legmagasabb.** Feltörhetetlennek bizonyult az élő nyelv rendszertelensége és írásbeliség hiánya miatt.
Betanítható-ság	**Gyors.** A Caesar-korong használatával jelentősen lerövidült az idő.	**Kb. 1 hónap.** A gép kezelését és a kódkönyvek használatát kellett elsajátítani, további eszköz- alkalmazást igényelt felhasználás során (gép, kódkönyvek).	**Kb. 1 hónap.** A speciális kódszavak és kifejezések megtanulása volt szükséges.
Sérülékenység	**Magas.** Elméleti tudás alapú; ha ismerik a módszert, megfejthető.	**Magas - Fizikai.** A gép és a kódkönyvek megszerzése a titkosítás végét jelentette.	**Közepes - Emberi.** A kódbeszélő foglyul ejthető, de a nyelv továbbfejlesztése (kódolt navaho) védelmet nyújtott.
Célba érés biztonsága	**Alacsony** abban az esetben, ha ismert a módszer.	**Kétélű.** A vétel biztonságos, de ha az ellenségnek is van gépe, észrevétlenül lehallgathatja.	**Biztonságos.** Fontos a fogadó környezet védelme.
Rugalmasság	**Közepes** (egyszerű eszközigény).	**Alacsony** (eszközigényes).	**Magas.** Nincs külön eszközigény (csak adó-vevő), gyorsan bevethető kritikus helyzetben.
Használhatóság ideje	Az ókortól az újkor elejéig.	A II. világháború alatt (a feltöréséig).	Az 1940-es évektől 1960-as évek végéig.

A táblázat alapján látható, hogy a három vizsgált nyelv közül az élő nyelv alkalmazása volt a legeredményesebb.

Biztonságos titkos nyelvezet margójára idézném a következőt: „Biztonságosnak a mai körülmények között az az eljárás tekinthető, amelyiknek a feltörése a legjobb gépekkel 10-15 év alatt sem valósítható meg (teljes biztonság nem garantálható, hiszen az összes

lehetőség kipróbálása elvileg lehetséges.) Az erős produkciós titkosítók (pl. AES) ma biztonságosnak számítanak, és a hagyományos eljárások modern utódai (Papp–Szabó 2006). [5, p. 476]

Hagyományos eljárások jó alapként szolgálhatnak a titkosítás területének egyengetéséhez és fejlesztéséhez, a mai kor egyre változatosabb technológiáival élve, egész kiváló készlet-választék tárulhat ezen terület fejlesztői elé.

ÖSSZEFOGLALÁS

Jelen tanulmányban bemutatásra kerültek a titkos nyelvezet általános fejlődési szakaszai, kiemelve három módszer bemutatását – Caesar-kódolás, Enigma gép által alkalmazott titkosítás és az élő emberi nyelv kódnyelvként való alkalmazása. A háromféle nyelvezet elemzését a következő szempontok alapján végeztem – történelmi háttér, keletkezés oka, eszközigény és a titkos nyelvezet általános szerkezete. További célom volt az alkalmazás konkrét környezetének bemutatása példákon keresztül. Ennek azért láttam szükségét, mert az alkalmazás gyakorlati elemzésével további hasznos következtetésekre lehet jutni és a régi tapasztalatokat olyan irányba terelni, hogy az, a mai hazai hadi környezet számára hasznos információként szolgáljon. Végezetül a három bemutatott nyelvezet alapján következtetések levonására került sor, ahol szemügyre vettem a titkos nyelv *megfejthetetlenségét, betaníthatóságát, sérülékenységét, célba érésének biztonságát, rugalmasságát, használhatóságának idejét.*

FELHASZNÁLT IRODALOM

[1] G. Gyurák, *„A kriptográfia és a hírszerzés hadtudományi gyökerei - Military roots of cryptography and intelligence,”* Hadtudományi Szemle 2014, Évfolyam 18, szám 3, pp 15-16.

[2] E. Szigeti, *„Kódfejtés, rejtjelezés történelemórán,”* 10 július 2019. [Online]. Available: www.torizzotthon.hu/modszertan/kodfejtés-rejtjelezés-történelemórán. [Letöltés dátuma: 2024. december 15.].

[3] G. Gyurák, *„A kriptográfia és a hírszerzés hadtudományi gyökerei - Military roots of cryptography and intelligence,”* Hadtudományi Szemle 2014, Évfolyam 18, szám 3, pp 17-18.

[4] B. Láng, *Titkosírás a kora újkori Magyarországon*, Budapest: Balassi Kiadó, 2015.

[5] G. Kallós, *„A titkosítás művészete - Titkosítás és kódfejtés az ókortól napjainkig,”* in XXIV. Apáczai-napok Tudományos Konferencia tanulmánykötete, Győr: Széchenyi István Egyetem Apáczai Csere János Kar, 2021.

[6] „Rejtjelező,” [Online]. Elérhető: www.rejtjelezo.hu/morse-kod-ismerteto. [Letöltés dátuma: 2024. december 18.].

[7] *„Morse-kód fordító, memoriterekkel,”* TrM Fordítóiroda, [Online]. Elérhető: www.tremforditas.hu/morse. [Letöltés dátuma: 2024. december 18.].

[8] „Caesar. Pallas nagy lexikona,” [Online]. Elérhető: www.arcanum.com/hu/online-kiadvanyok/Lexikonok-a-pallas-nagy-lexikona-2/c-4B61/caesar-4BE4/. [Letöltés dátuma: 2024. december 17.].

[9] www.kalkulatorok.net/caesar-titkositas-online-kodolo-dekodolo. [Online] [Letöltés dátuma: 2024. október 10.].

[10] Múlt-kor szerkesztősége, *„Kódolt üzenet az amerikai polgárháború sorsdöntő ostromából*.," Múlt-kor történelmi magazin, január 4, 2011. [Online]. Elérhető: https://mult-kor.hu/20110104_kodolt_uzenet_az_amerikai_polgarhaboru_sorsdonto_ostromabol. [Letöltés dátuma: 2024. november 24.].
[11] P. Snoj, *„Az Enigma rejtélye*", Honvédelem.hu," június 7, 2021. [Online]. Elérhető: https://honvedelem.hu/hirek/az-enigma-rejtelye.html. [Letöltés dátuma: 2024. december 4.].
[12] Crypto Museum, „*Enigma 3*," Crypto Museum Online, Elérhető: https://www.cryptomuseum.com/crypto/enigma/m3/index.htm [Letöltés dátuma: 2024. december 5.].
[13] Deutsches Spionagemuseum, „*Vor 75 Jahren erbeutete ein britischer Zerstörer Enigma M4 Codebücher,"* Deutsches Spionagemuseum Blog, okt. 30, 2017. Elérhető: https://www.deutsches-spionagemuseum.de/2017/10/30/vor-75-jahren-erbeutete-ein-britischer-zerstoerer-enigma-m4-codebuecher. [Letöltés dátuma: 2024. december 5.].
[14] Hirschfelder és M. K. de Montano, „*A Portrait of Native America Today*," in The Native American Almanac: A Portrait of Native America Today, New York, NY, USA: Prentice Hall General Reference, 1993, pp. 232–234.
[15] „*Navajo Code Talkers*," Grand Valley State University Math Department. Elérhető: https://web.archive.org/web/20080506022452/http:/www.gvsu.edu/math/enigma/Navajo/PAGES9-1.HTM. [Letöltés dátuma: 2024. december 5.].
[16] U.S. Navy, „*Navajo Code Talkers: World War II Fact Sheet*," Naval History and Heritage Command. Elérhető: http://www.history.navy.mil/faqs/faq61-4.htm. [Letöltés dátuma: 2024. december 10.].
[17] A.Molnar Jr., „*Navajo Code Talkers: World War II Fact Sheet*," Navy and Marine Corps World War II Commemorative Committee, Published: Thu Apr 16 15:08:36 EDT 2020. Elérhető: https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/n/code-talkers.html. [Letöltés dátuma: 2024. december 10.].
[18] Molnar Jr., „*Navajo Code Talkers: World War II Fact Sheet*," Navy and Marine Corps World War II Commemorative Committee, Washington, DC, USA: Naval Historical Center, Department of the Navy. [Online]. Elérhető: https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/n/code-talkers.html. [Letöltés dátuma: 2024. december 10.].