A titkosítás művészete – Titkosítás és kódfejtés az ókortól napjainkig

Kallós Gábor
Széchenyi István Egyetem, Győr

Bevezetés

Ebben a tanulmányban a titkosítások történetét olyan szempontból vizsgáljuk, hogy az adott korok jellemző módszerei hogyan hordozzák magukban az időszak technológiai fejlettségét, és az újabb koroktól kezdődően hogyan érhető itt tetten az ipari és később az informatikai modernizáció (kutatási kérdés és hipotézisünk az, hogy jelentősen érvényesül mindez).

Az alkalmazott módszertan – a téma jellegéből adódóan – főként forráskutatás saját vizsgálatokkal. A témaválasztást röviden az indokolja, hogy a terület érdekessége ellenére – különösen magyarul – viszonylag kevés az elérhető, a teljes témakört igényesen és szélesebb közönség számára lefedni akaró forrásmunka, illetve ezek nem kellő mértékben ismertek. Tipikus, hogy a jó minőségű irodalmak a nem könnyű matematikai „betétek” miatt nehezen érthetőek a nem szakemberek számára. Gyakori az is, hogy a könnyen elérhető források „pongyola” megközelítést alkalmaznak, vagy nem a lényegre összpontosítanak.

Mint tudjuk, a témakör – jellegénél fogva – matematikai módszerek (elsősorban számelmélet) alkalmazását is igényli. Felidézve, hogy a diákok az iskolában sokszor nem túl nagy szeretettel fordulnak a matematika felé, hasznos alkalmazás lehet az érdeklődés felkeltése ilyen jellegű feladványokkal (pl.: Fejtsük meg a következő titkosírást!). A megoldás során a kisdiák – akaratlanul is – sok olyan matematikai módszerrel megbarátkozhat, amit egyébként nem fogadna túl lelkesen. Ezt a matematikát „burkoltan becsempésző”, megszerettető módszert neves írók is alkalmazták regényeikben, pl. Verne Gyula, Edgar Allan Poe és mások.

1. Rövid áttekintés

A titkos üzenetek létrehozásának a tudománya (kriptográfia, rejtjelezés) már évezredek óta kíséri az emberiség történelmét. A cél tömören megfogalmazva az, hogy csak az értse az üzenetet, akinek valóban szánták. A kriptográfia nyelvén beszélünk eredeti, kódolatlan (nyers) üzenetről (plaintext), és elküldhető/elküldendő titkos üzenetről (ciphertext). Az üzenet kódolása valamilyen eljárás vagy algoritmus segítségével történik, ezt az információt egybefoglalóan (bekódoló) kulcsnak nevezzük. A titkos üzenet szintén egy (kikódoló) kulccsal fejthető meg. Lényeges, hogy a kódolás és a dekódolás a kulcs birtokában egyszerű és gyors legyen. Szintén fontos, hogy utóbbit a kulcs ismerete nélkül viszont lehetőleg ne lehessen elvégezni. (Tehát a titkos üzenetet illetéktelenül megszerző „lehallgató” ne juthasson hozzá a titkos információhoz.)

Kezdve a legrégebbi időktől, a történelmi korokban alapvetően háromféle titkosítási módszert alkalmaztak. Ezek a következők:

- Üzenetrejtés (szteganográfia)
- Helyettesítéses módszerek
- Keveréses módszerek

A legújabb időszak találmánya az aszimmetrikus titkosítás.

A következőkben konkrét példákkal áttekintést adunk a fontosabb módszerekről, és kitérünk a feltörés lehetőségeire is.

2. Üzenetrejtés

Az **üzenetelrejtés** (szteganográfia) lényege az, hogy az üzenetet valami egyedi ötlettel láthatatlanná tesszük. Itt sok érdekes, kreatív, egyedi megvalósítás szóba jöhet.

Hérodotosz a Kr. e. V. századból, a görög–perzsa háborúk idejéből két ilyen nevezetes esetet ír le. Az első történet szerint Hisztiaiosz (Milétosz türannosza) úgy küldött titkos üzenetet Arisztagorász hadvezérnek, hogy leborotváltatta a küldönc haját, és annak fejbőrére tetováltatta az üzenetet. Ezután megvárta, amíg a szolga haja kinő, és elküldte őt a hadvezérhez. Célba érve a küldönc felfedte a titkosítási módszert, így olvashatóvá vált a levél.

A másik történetben Demarátus spártai király hosszasan Xerxész „vendégszeretetét élvezte”, és ezalatt megtudta, hogy a perzsa uralkodó támadást készít elő az övéi ellen. Mivel a figyelmeztetést haza nem tudta egyszerűen elküldeni, ezért cselt alkalmazott: az íráshoz normál esetben használt viasztáblákról leolvasztotta a viaszt, a fafelületre írta az üzenetet, és újra lefedte azt viasszal. Ezek az üresnek látszó táblák a többi csomag között nem keltették fel az őrök figyelmét.

A régi Kínában (ókor, korai középkor) az üzenetrejtést úgy alkalmazták, hogy tojások héja alá juttatták be az üzenetet, és az feltörés után vált olvashatóvá. A nyomtatás elterjedése után a vízjelet is használták üzenetrejtésre (Katzenbeisser–Petitcolas 2000).

Mint ezekből a példákból is látjuk, a módszer kockázatos: ha az ellenérdekelt fél felismeri az alkalmazott eljárást, akkor szinte biztosan meg is fejti az üzenetet. (Ez komoly gyengeség.) Ennek ellenére a szteganográfiát a modern korban is használták, pl. a hidegháború idején is. Ezekkel a sokszor briliáns ötletekkel leggyakrabban a kémfilmekben találkozhatunk (extrém módon lekicsinyített üzenetek, képbe rejtett üzenetek stb.).

3. Egyábécés betűhelyettesítés

A helyettesítéses (felcserélő) módszerek az eredeti szöveg betűit (esetleg betűcsoportjait) más betűkkel vagy más szimbólumokkal helyettesítik.

A klasszikus betűhelyettesítésnél a nyílt szöveg egy adott betűjét mindig ugyanazon kódbetű helyettesíti (egyábécés helyettesítés, monoalfabetikus rejtjel). A Caesar-féle titkosítás egyszerű eltolást alkalmaz. Ha az ábécé betűit 0-tól kezdve sorszámozzuk (A – 0, B – 1, C – 2 stb.), akkor egy fix eltolási értéket használva (mondjuk 3) megkapjuk a betűk új kódját.

1. ábra: Caesar-titkosító (játék korong)
Forrás: https://shopretroworks.com/products (letöltési idő: 2020. november 12.)

A módszer egyszerű, de igen könnyű feltörni: ki kell próbálni a lehetséges eltolásokat, ami angol ábécé esetén összesen csak 26 eset. Az általános betűcsere (direkt csere) alkalmazásával az eredeti betűket titkosított betűknek feleltetjük meg (betűk helyett kódok vagy egyéb szimbólumok is alkalmazhatók). Fontos, hogy **azonos eredeti betűkhöz azonos kódbetűk tartoznak**. Bár ezt a módszert már az ókorban is ismerték (Polübiosz titkosítása), igazi

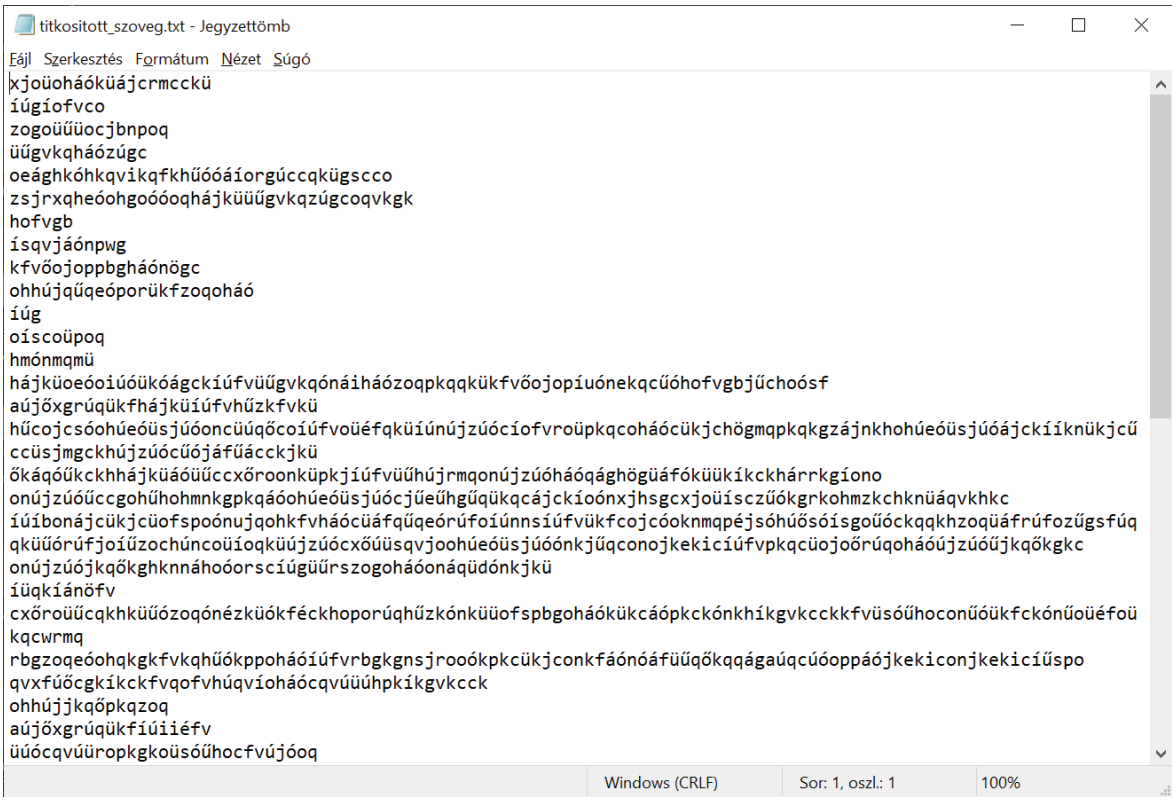
felvirágzása a korai középkorban kezdődött, és egészen az 1500-as évek végéig nagyon széles körben használták.

Híres történelmi példa, hogy Stuart Mária (skót királynő) ilyen titkosítással (monoalfabetikus rejtjel + egyes szavak helyettesítései) levelezett Anthony Babingtonnal, és összeesküvést szőttek I. Erzsébet angol királynő ellen (Babington társaival Stuart Máriát akarta az angol trónra juttatni). Az angol királynő kémfőnöke, Lord Francis Walsinghamne el tudta fogni, és kiváló matematikusával meg is tudta fejtetni az üzeneteket, a bizonyítékok alapján az összeesküvőket kivégezték (Gómez 2016).

Ez a kudarc olyan figyelmeztetés volt, amelyet minden rejtjelezőnek komolyan kellett venni ezután: a hagyományos titkosítási algoritmus már nem biztonságos! Hogyan is lehetséges a feltörés? Bár a teljes kipróbálás – az esetek óriási száma miatt szinte lehetetlen –, a gyakorisági elemzés (betűk), a szótippelés és a nyelvi redundancia mégis lehetővé teszi a megfejtést (kivéve esetleg, ha a szöveg nagyon rövid).

A betűgyakorisági elemzés hosszabb szöveg esetén lényegében biztosan be tudja azonosítani az első néhány leggyakoribb betűt (persze nyelvfüggő módon). Ez a tény már a (korai) középkorban ismert volt (első feljegyzés: IX. század, Al-Kindi arab tudóstól). Ezután a leggyakoribb szavak, ismétlődő minták keresésével mehetünk tovább, és lépésről-lépésre egyre több betűt fejthetünk meg.

Nézzünk meg mi is egy feltörési példát a monoalfabetikus (egyábécés) rejtjelre. A következő titkos szöveget kapjuk:

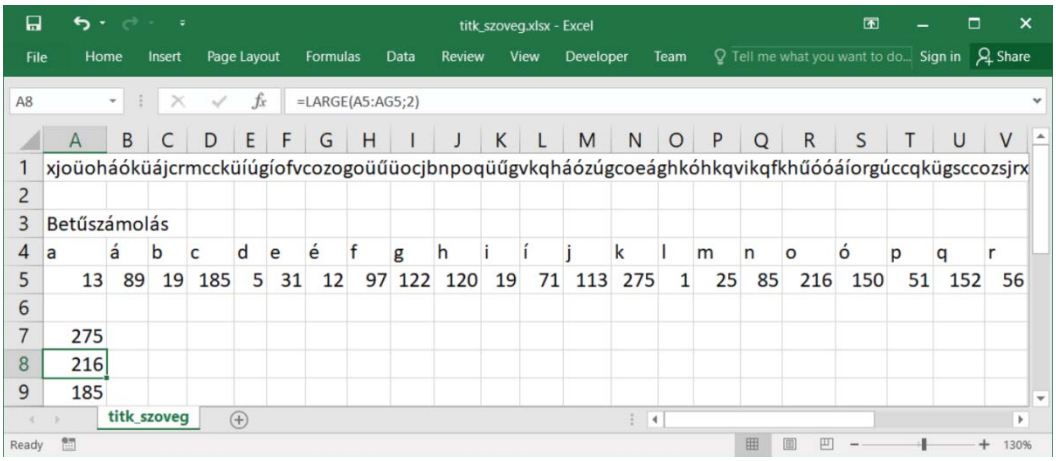


2. ábra: Titkos szöveg
Forrás: saját szerkesztés (2020)

A kódolt szöveg – nem meglepő módon – teljesen értelmetlennek tűnik. Mivel magyar kisbetűket alkalmaztak a kódolásnál, **feltehetjük, hogy az eredeti szöveg is magyar**. A szöveg logikáját elemezve arra a következtetésre juthatunk, hogy a kódolás szóköz nélkül történt (a leggyakoribb betűk mind szerepelnek a sorok elején, továbbá szerepelnek párosával is a szövegben – ez szóközre nem teljesülhet). A sorok különböző hosszúak, ez adódhat

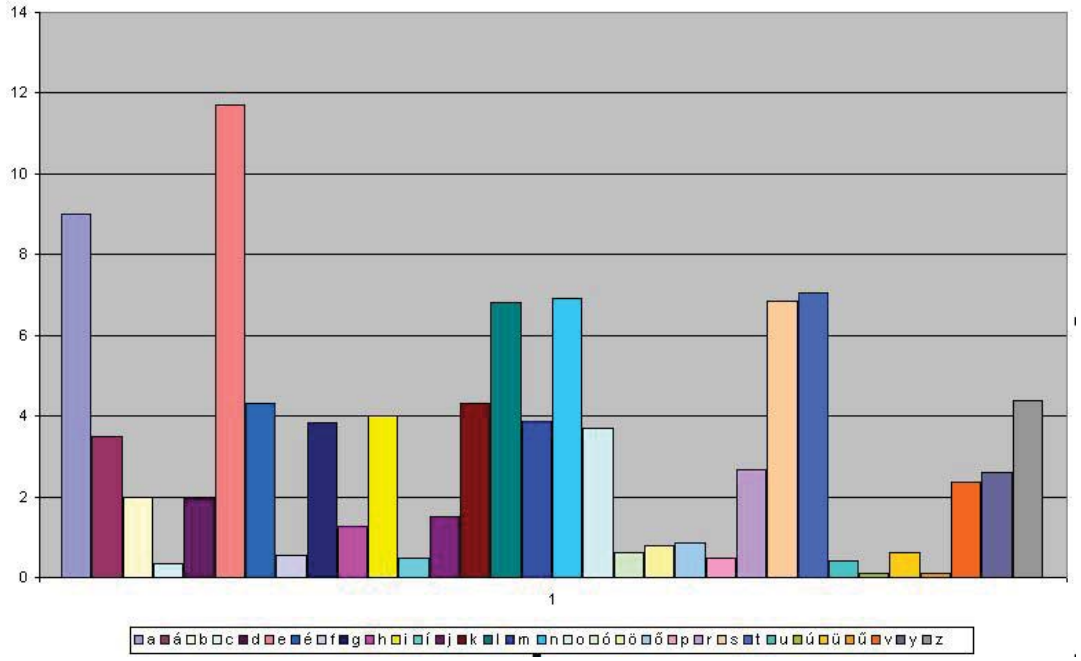
abból, hogy a szöveg párbeszédekkel tagolt. Egy-egy sor nem lehet egy-egy szó, mert a sorok ahhoz túl hosszúak.

Betűszámlálással folytatjuk, ennek eredménye a következőt adja (3. ábra).



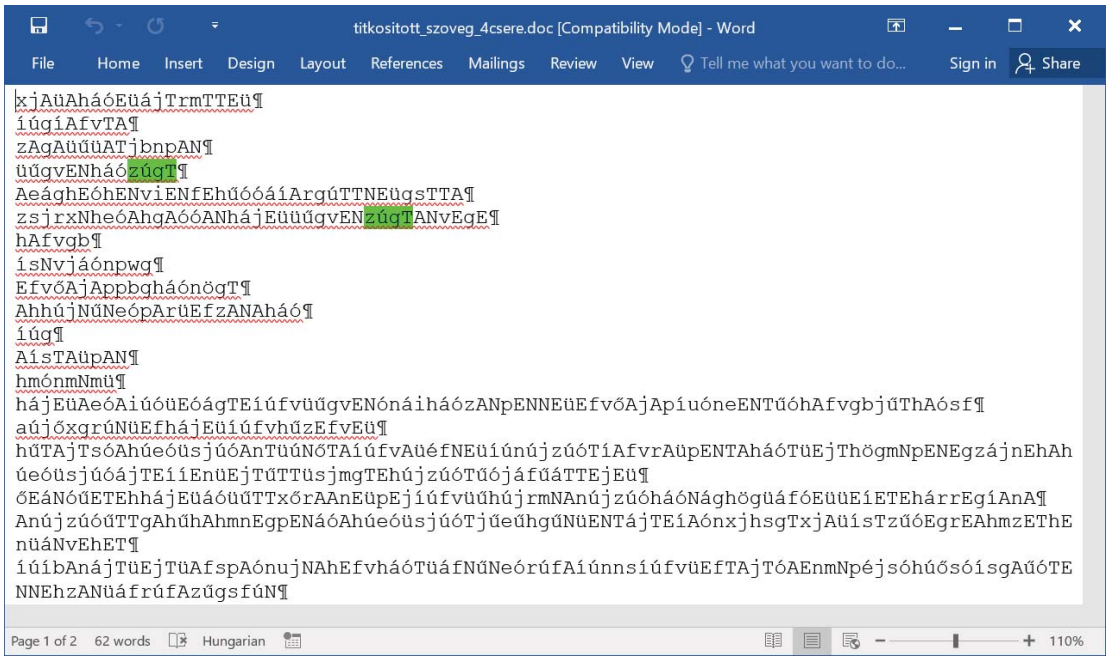
3. ábra: Betűszámolás Excellel
Forrás: saját szerkesztés (2020)

Látható, hogy a kódolt szövegben a leggyakoribb szimbólum a **k** betű, utána következik az **o**, majd a **c**, és negyedjére a **q**. A Caesar-féle eltolás (leggyakoribb betűkre) semmilyen módon nem feleltethető meg a magyar betűgyakoriságoknak, ezért kizárható. Feltehető tehát, hogy betűcserés titkosírást alkalmaztak. Magyar szövegre ezek a gyakoriságok rendre az **e**, **a**, **t** és az **n** vagy **l** betűknek felelnek meg.



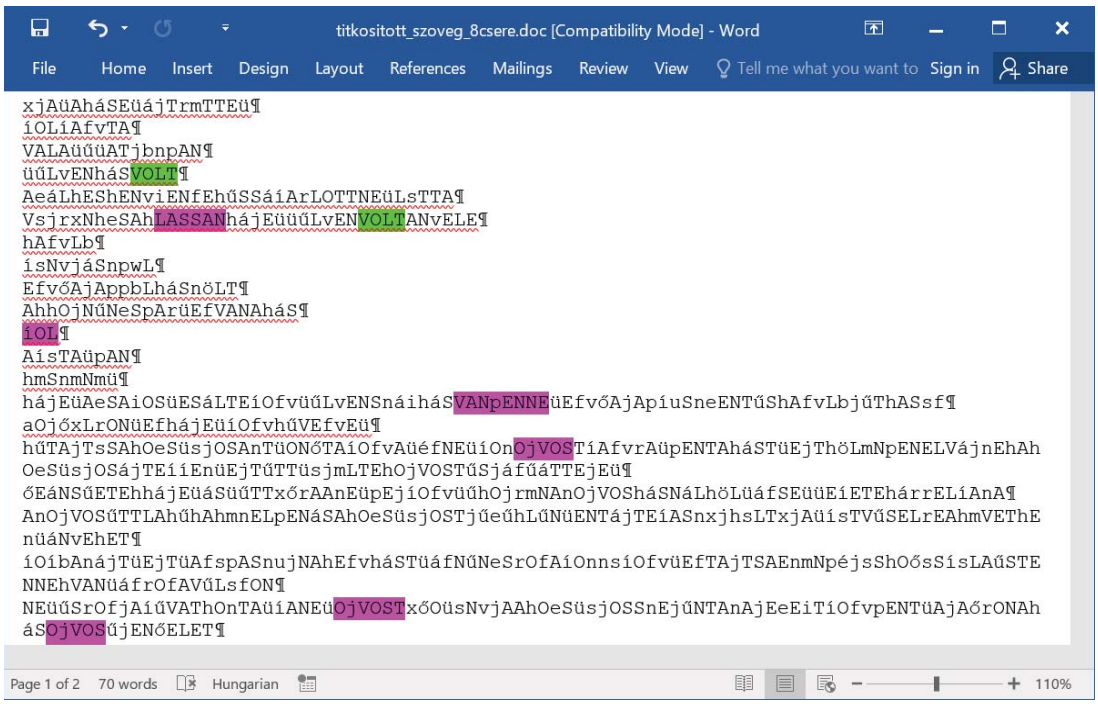
4. ábra: Tipikus betűgyakoriságok magyar szövegre (százalék)
Forrás: saját szerkesztés (2020)

Cseréljük ki ezeket a betűket a jó párjukra! (Nagy betűkkel jelöljük a már helyes karaktereket.)



5. ábra: A szöveg 4 csere után
Forrás: saját szerkesztés (2020)

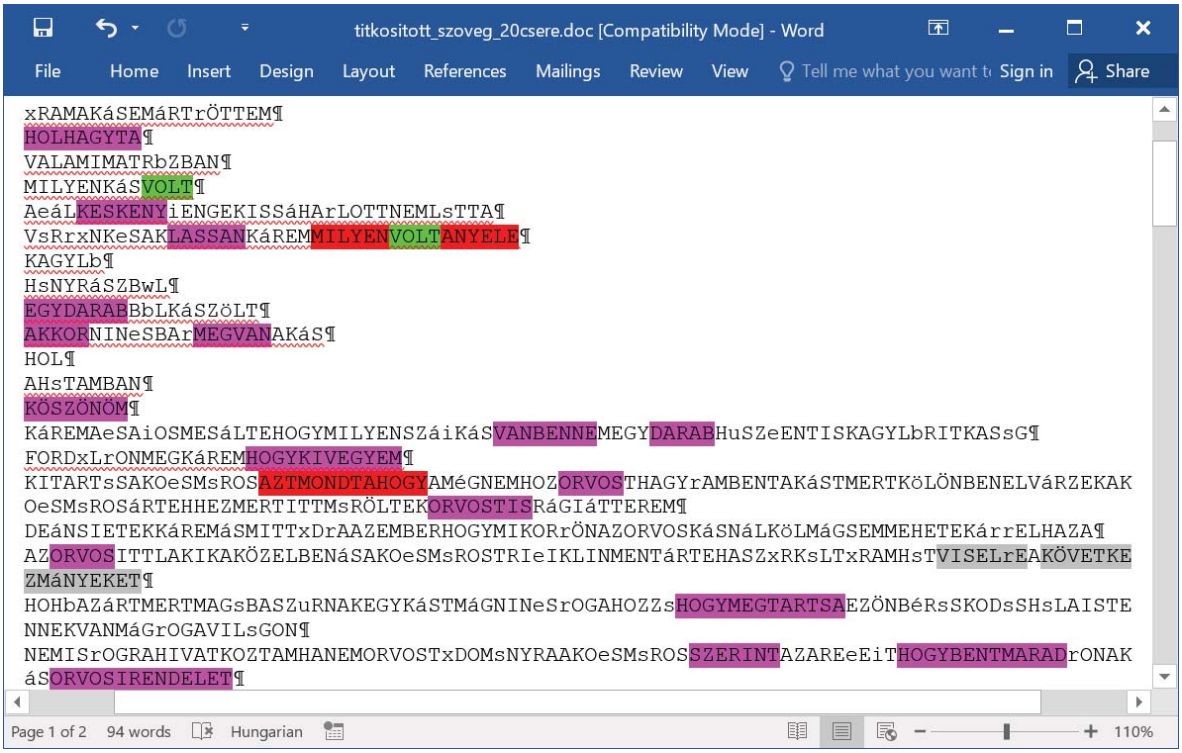
Ismerve a leggyakoribb – legalább négybetűs – magyar szavak listáját (volt, hogy, vagy, mert, mint, kell stb.) feltehetjük, hogy az ábrán kiemelt minta, a „zúgT” valójában a „volt” szócska. (Azt is gondolhatjuk hasonlóan, hogy az „üEjT” a „mert”.) Az előbbi feltételezéssel megyünk tovább, újabb 3 cserével, és még becseréljük a következő leggyakoribb betűt is (**S**).



6. ábra: A szöveg 8 csere után
Forrás: saját szerkesztés (2020)

Láthatjuk, hogy 8 csere után már egyre több értelmes szó és szórészlet jelenik meg, egyre könnyebben adódnak az újabb helyettesítések. A magánhangzók megtalálása fontos, sokat segíthet, ezért érdemes azokra kiemelten fókuszálni. A nyelvi redundanciát is használjuk,

sokszor már úgy is teljesen el tudunk olvasni egy-egy részletet, hogy még akár a betűk 20-25%-a hiányzik a megfejtésből.



7. ábra: A szöveg 20 csere után
Forrás: saját szerkesztés (2020)

20 csere után már szinte majdnem folyékonyan olvasható a szöveg (amely, mint láthatjuk, egy Rejtő-regény ismert részlete). A hasonló példák szépirodalmi szerzők figyelmét is felkeltették, érdekes, krimiszerű kódfejtési történeteket olvashatunk pl. Edgar Allan Poe vagy Sir Arthur Conan Doyle írásaiban (Pig-pen, táncoló emberkék stb.).

4. Többábécés helyettesítés (polialfabetikus rejtjel)

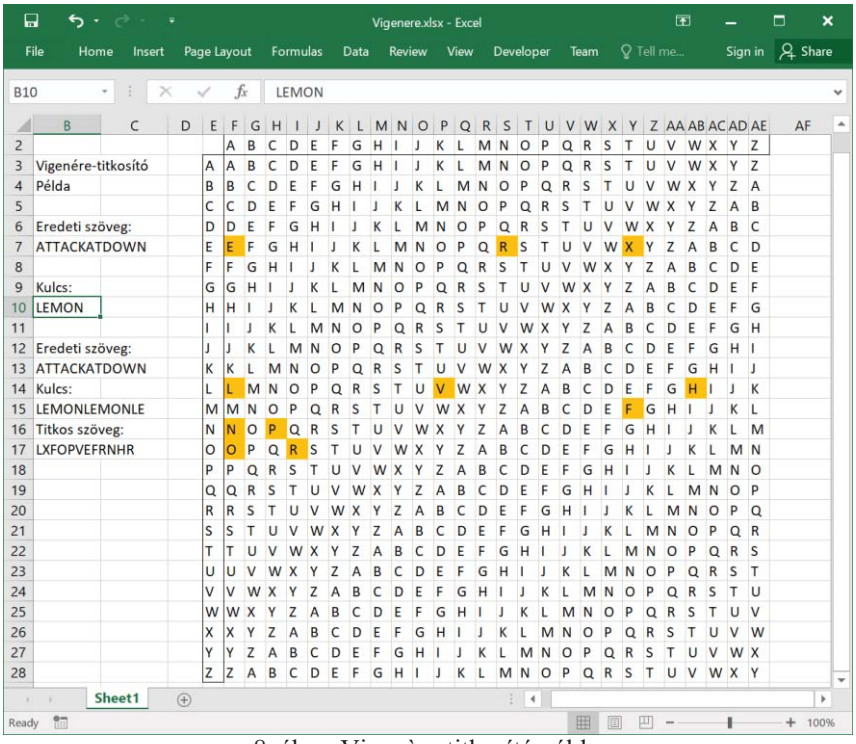
Miután a klasszikus monoalfebetikus rejtjel „lebukott”, a titkosítók fejlettebb eljárásokkal próbálkoztak. A cél a statisztikai elemzés megzavarása volt. Ez elérhető például úgy, hogy a leggyakoribb betűkhöz többféle kód is tartozhat (pl. az E kódja lehet 12 és 23 is; homofónok használata). Ezt az ötletet először Leon B. Alberti jegyezte le, majd ugyanő később már két kódábécé egyidejű használatát javasolta.[1]

Alberti ötletével megszületett a **polialfabetikus** rejtjel. Ennek lényege tehát az, hogy nem egy kódábécét használunk, hanem többet, valamilyen rendszer szerint váltogatva. Ez a módszer általános formájában Blaise de Vigenère francia tudós nevéhez kötődik (1585-ben írta le). A legerősebb titkosításban annyi kódábécét használunk, mint az eredeti ábécénk elemszáma (Vigenère-négyzet). Az üzenet soron következő betűinek a kódját valamilyen szabály szerint (egy kulcs alapján) választjuk a lenti sorokból (Rothe 2004). (Azt is megtehetjük akár, hogy minden lépésben eggyel lejjebb mozdulunk el.)

A következő példában a „lemon” kulcsszót használjuk az üzenet kódolásához. Látható, hogy az első **A** betű kódját az **L** sorából választjuk, az első **T** betű kódját az **E** sorából, a

[1] Más jó megoldás lehet, hogy nem betűket, hanem betűcsoportokat helyettesítsünk, így ha egy gyakori betű más-más párral szerepel, akkor a kódbetűk is mások lehetnek, pl. Playfare titkosító.

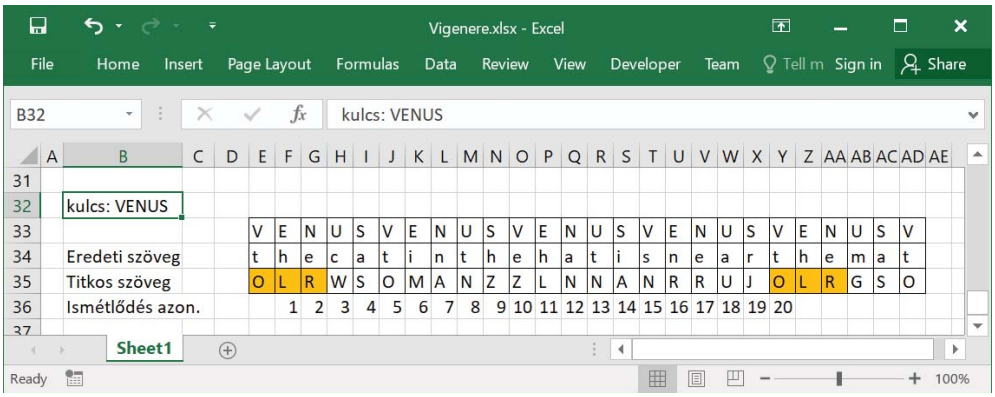
második **T** betű kódját az **M** sorából, a második **A** betűét az **O** sorából stb. Jól megfigyelhető, hogy a polialfabetikus rejtjelnél az azonos betűk kódja általában eltérő.



8. ábra: Vigenère-titkosító példa
Forrás: saját szerkesztés (2020)

Az ilyen elven működő titkosítókat az 1870-es évekig széles körben használták, pl. még az amerikai polgárháborúban is (Alberti-tárcsák). A titkos szöveg megfejtése a fentiek miatt szinte lehetetlennek tűnik. A feltörés majdnem 300 évig megoldatlan probléma maradt. Csak 1863-ban tette közzé a német Friedrich Kasiski, hogy sikerült módszert találnia az általános polialfabetikus rejtjel feltörésére. (Valamivel korábban Charles Babbage is sikerrel járt, de a feljegyzéseit erről csak a XX. században találták meg).

A feltörés ötletét mutatja be a következő egyszerű példa (9. ábra).



9. ábra: Vigenère-titkosító, feltörési példa
Forrás: saját szerkesztés (2020)

Az eredeti szöveg egy tréfás angol mondat („the cat in the hat …”) a kulcs pedig „Venus”. A szöveg elején az első „the” a „Ven” kulcsszórész alatt szerepel. Vegyük észre, hogy ugyanez később is előfordul, a harmadik „the” esetén. Ez azt eredményezi, hogy a titkos szövegben

ismétlődő mintázat jelenik meg („olr”). A minta ismétlődése 20 betű távolságra fordul elő újra, a kódszó hossza pedig 5, és 5 osztója a 20-nak. Ha tehát valaki türelmesen összegyűjti az ismétlődő mintákat, és méri azok távolságát, akkor az osztók vizsgálatával előbb-utóbb megtalálhatja a kulcs hosszát (jelöljük azt $|k|$-val). Ekkor pedig a polialfabetikus rejtjel elemzése visszavezethető $|k|$ darab különálló monoalfabetikus rejtjellé, és így a gyakoriságelemzés segít már a feltörésben. A valóságban ez azért persze nem olyan egyszerű, mint a kis példánkban, a kulcs jóval hosszabb lehet, és az osztóknál is becsapódhatunk. Rövidebb szöveg esetén ráadásul a gyakoriságelemzés is megbukhat a több külön kódábécé miatt. Ennek ellenére megfelelő idő ráfordítása esetén a feltörés lehetséges.[2]

5. Keverés

A fejlődés másik útját képviselik a betűk keverésén alapuló titkosítások. Ilyenkor az eredeti szöveg betűinek a sorrendjét valamilyen információ (kulcs) alapján összekeveréssel változtatják meg. Mivel a szöveg eredeti jelei nem változnak meg, a módszer alkalmazása könnyen felismerhető (a gyakoriságok megmaradnak). Ez azonban nem jelenti azt, hogy a megfejtés is könnyű.

Az első dokumentált keveréses titkosítást Spártában alkalmazták, ennek neve: szkütálé. Egy rögzített átmérőjű botra rátekertek egy szalagot, és erre soronként ráírták a titkosítandó üzenetet. Ezután a szalagot letekerték, és csak azt továbbították a bot nélkül. Ha valaki elfogta a küldöncöt, a kulcs ismerete nélkül a szalagon csak összekevert betűket láthatott. A címzettnél azonban volt egy ugyanolyan átmérőjű bot, és ő a szalagot erre feltekerve el tudta olvasni az üzenetet.

10. ábra: Szkütálé
Forrás: https://educalingo.com (letöltési idő: 2020. november 12.)

A keveréses titkosítás egyik fejlett megvalósítása a **titkos rács** vagy rostély, amely a Verne-regényben (lásd lent) bemutatott ismertetés szerint mai formájában Fleissner Wostrowitz osztrák ezredes nevéhez kötődik. Valójában azonban már korábban is ismert volt (Katzenbeisser–Petitcolas 2000).[3]

Gyermekkorunk egyik kedvenc romantikus könyve Verne Gyula: Sándor Mátyás című regénye, ahol a magyar szabadságért küzdő főurak postagalamb segítségével ily módon titkosított üzenetekkel kommunikálnak. (A történet ezután következő, szomorúbb részét is ismerjük: Sárkány, a pénzéhes félalvilági kalandor a gyenge tartású Torontál Simonnal megszerzi az egyik titkos üzenet mellett a rostélyt is, és együtt elárulják, feljelentik a szabadságharcosokat.)

A regényben szereplő rostély 6×6-os, 36 négyzetet tartalmaz, amelyek közül 27 teli és 9 üres. Így 4 teljes fordulattal mind a 36 betű megjelenik; összesen 3 ilyen csoport van, tehát a

[2] Egy ilyen kódolású szövegre vonatkozó, érdekes feltörési példát olvashatunk Verne Gyula: „800 mérföld az Amazonason” című regényében.
[3] Már az ókori Kínában is használták, Cardano és Lord Walsinghamne is bemutattak egyszerűbb változatokat, és Carl Hindenburg matematikus az 1700-as évek végén részletesen is leírta.

teljes üzenet 108 betűből áll. Bár minden betű az eredeti jelentését hordozza, mégis, az elméleti lehetőségek óriási száma miatt a rács ismerete nélkül a feltörés szinte lehetetlen. Azonban a módszer sérülékenységét pont a rács fizikai megléte okozza: ez esetleg megszerezhető! Ennek ellenére még az első világháborúban is használták.

6. Enigma

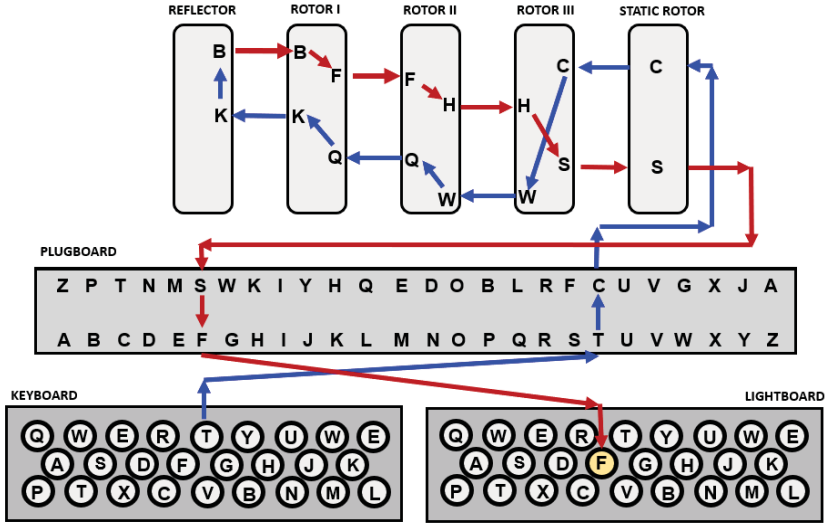
Az első világháború (és közben a mechanikai eszközök fejlődése is) nagy lendületet adott a titkosító eljárások fejlődésének. Nyilvánvalóvá vált, hogy a biztonságos, igen nehezen megfejthető, de akár harctéri körülmények között is jól alkalmazható módszerek jelentősen, akár döntő módon is befolyásolhatják a harctéri helyzetet. Ezen tapasztalatok alapján nyújtotta be 1919-ben egy német mérnök, Arthur Scherbius egy gép szabadalmát (Enigma), amelyet a tökéletesen biztos kommunikációhoz tervezett. Akkor még kevesen gondolták volna, hogy ez a gép lesz talán a leghíresebb eszköz a titkosítások több évezredes történelme 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. Többek között a tengeralattjárók irányítására is használták, amelyek az Angliába irányuló szövetséges szállítóhajókat gyakran elsüllyesztették, ezért vált a szövetségesek számára elsőrendűen fontossá az Enigma-kódolás feltörése.

Az Enigma elektromechanikus berendezés, amely külsőleg egy vaskos, régivágású írógépre emlékeztet. A gép fő részei a következők: billentyűzet (keyboard), közös tengelyen forgó tárcsák (rotors), fordító (reflector), kapocstábla (plugboard), lámpatömb (lightboard). A kódolás és a dekódolás technikailag egyaránt úgy történt, hogy a megfelelő tárcsa- és kapocstábla beállítás mellett a kezelő lenyomott egy gombot a billentyűzeten, és erre kigyulladt egy lámpa a lámpatömbön. Ez volt a bekódolt betű. (A kikódolás technikája is ugyanez.)

Fontos, hogy a tárcsák a betűk leütésének hatására elfordulhatnak. Nevezetesen, a jobb szélső tárcsa minden karakter leütésekor egyet fordul, a középső a jobb szélső egy teljes körbefordulásakor fordul egyet, a bal szélső pedig ugyanígy a középső egy teljes körbeérésekor. (A szárazföldi haderőnél három tárcsát használtak, később négyet; a haditengerészetnél négyet, később ötöt.)

Az egyes tárcsák más-más helyzetben maguk is másként keverik (permutálják) a betűket (tehát a szövegben ismétlődő betűk kódja eltérő lesz).



11. ábra: Az Enigma működési vázlata
Forrás: https://www.une.edu.au/info-for/visitors/museums/museum-of-antiquities/codebreaker-challenge (letöltési idő: 2020. november 10.)

Ennek megértéséhez tekintsük az Enigma egy nagyon leegyszerűsített modelljét (Gómez 2016). Ebben a modellben egy konkrét jobb szélső keverőtárcsa csak 3 betűt tartalmaz (az eredeti 26 helyett). Alaphelyzetben az **A** betű képe az **A** betű, a **B** betűé a **C**, a **C** betűé a **B**. Az első betű rejtjelezése után a tárcsa 1/3 fordulatot tesz, ezáltal most a **B** betű képe lesz önmaga, az **A**-é a **C**, a **C**-é az **A**. A második betű kódolása szintén 1/3 fordulatot eredményez, így most a **C** betű képe lesz önmaga, az **A**-é a **B**, és a **B**-é az **A**. A tárcsánál tehát adott/rögzített a betűk keverésének a logikája, viszont háromféle helyzetbe állítható, és eszerint háromféle működésre képes.

Képzeljük el most azt, hogy – a valós helyzetnek megfelelően – sok 26 betűs tárcsát használunk (mondjuk 30-at), amelyek mind különbözően permutálják a betűket, ezeknek mind-mind 26 különböző helyzetük lehetséges (4 tárcsára kb. 450 ezer lehetőség), és a napi alkalmazandó 4 tárcsát ebből a 30-ból válogatjuk (kb. 100 ezer lehetőség), és ráadásul bármely lehetséges sorrendbe rakhatjuk őket (24 lehetőség). Ez így mindösszesen kb. 1 billió lehetőség.

A kezelők a titkosításnál ráadásul még a kapocstáblát is használták direkt betűcserékhez. Ezeket napi kódkönyvek szabályozták, hasonlóan a tárcsák alapbeállításához. A kapocstábla alkalmazása (pl. 6 tetszőleges betűpár cseréjével) elvileg szintén nagyjából újabb 1 billiószorosára növeli az elméleti lehetőségek számát. A német hadvezetés ezeket a csillagászati számokat elemezve úgy értékelte, hogy ez a kód feltörhetetlen. Ebben azonban tévedtek! Az Enigma – igen nagy bonyolultsága ellenére is – „csak” egy felerősített polialfabetikus titkosító.

Lengyel matematikusoknak sikerült az 1930-as évek elején az akkor még egyszerűbb Enigmát feltörniük (csak 3 tárcsa kevesebből válogatva és csak kevés betűpárcsere). Később Angliába menekültek és ötleteiket, eredményeiket a szövetségesek rendelkezésére bocsátották. Az angolok 1939-ben létrehoztak egy titkos kódfejtő központot London szélén (Bletchley Park), és Alan Turing matematikus vezetésével célul tűzték ki az Enigma-kód feltörését, amely végül valóban sikerült is (általában). Az eljárás lényege az volt, hogy a megszerzett információkat felhasználva (kódkönyvek, napi kódszavak, tipikus üzenetek) különböző elemzésekkel sokszor sikerült a lehetőségek számát több trillióról néhány millióra

vagy tízmillióra csökkenteni, ez pedig már az akkori elektromechanikus számítógépekkel (Turing-bomba, Colossus) kielemezhető mennyiség volt.

A részleteket ezen írás keretei között nem tudjuk bemutatni, de a feltörésnél a legfontosabb felhasznált ötletek a következők voltak (Kahn 1996):

- Az Enigma-kód szimmetrikus (ha pl. az A betű kódja Q, akkor a Q betű kódja is A lesz).
- Az Enigma-kódolásnál egy betű kódja sosem lehet önmaga (tehát pl. az A betű kódja nem lehet A).
- A németek tipikusan rendkívül precíz, konzervatív módon írták meg az üzeneteket. Sokszor sejthető volt, hogy az üzenet kezdete tisztelgő megszólítás, pl. „An General X.Y.”. Rutinszerűen továbbították a „Keine besonderen Ereignisse” (Nincs mit jelenteni) üzenetet, ill. az adott hely időjárási jellemzőit is. Ezek lehetőséget adtak az **ismert nyílt szövegű támadásra** (known-plaintext attack).

Akkoriban nem volt ez ismert, de ma már elfogadott tény, hogy Turing és csapata akár 1-2 évvel is lerövidíthette a második világháborút (és így közvetve sok ember életét is megmentették). Sir Winston Churchill a háború végén maga is azt jelentette VI. György királynak, hogy a Bletchley Park kódfejtő csapata nagy mértékben hozzájárult a szövetségesek győzelméhez.

12. ábra: Bélyegek az Enigma kód megfejtéséről
Forrás: mathematicalstamps.eu (letöltési idő: 2020. november 13.)

Az első és második világháborúban alkalmazott további titkosításokról, híres gépekről – az Enigma mellett – jó összefoglalást olvashatunk Kahn (1996) könyvében.

7. Számítógépes korszak

Az elektronikus számítógépek megjelenésével lezárult a titkosítás „hőskora”. A feltörésnél (és a kódolásnál) használt egyedi emberi ötletek fokozatosan egyre jobban kiegészültek a gépek monoton műveletvégző képességével. A továbbiakban már a titkosító (vagy kódfejtő) gép fizikai megépítése sem szükséges, hiszen a számítógépen ez is szimulálható.

A régebbi korok tapasztalatai úgy összegezhetők, hogy önmagukban sem a helyettesítő, sem a keverő titkosítók nem elég biztonságosak a nyelv jellegzetességei miatt. Ha azonban

számítógéppel keverések és helyettesítések egy hosszabb sorozatát hajtjuk végre (ezek az ún. produkciós titkosítók; lényegében sok-sok tárcsa a keverésre és alacsony szintű, akár bitenkénti keverések), akkor elő tudunk állítani biztonságos titkosító eljárást. Az első ilyen szabványként elfogadott titkosító a 64 bites DES volt.

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).

8. Új ötletek

Az eddigiekben bemutatott összes eljárás ún. szimmetrikus kulcsú titkosítás, azaz esetükben a visszafejtő („kikódoló”) kulcs nagyon hasonlít a titkosító („bekódoló”) kulcshoz. 1976-ban azonban Bailey W. Diffie amerikai kutató kieszelt egy olyan rendszert, amelyben a bekódoló kulcs és a kikódoló kulcs lényegesen eltér egymástól, és az előző nyilvánossá is tehető, mégsem fejthető meg a titkos üzenet (**aszimmetrikus titkosítás**). A módszert gyakorlatba átültetve született meg az RSA algoritmus 1977-ben. Az RSA mozaikszó az alkotók nevének a rövidítése (Ron Rivest, Adi Shamir és Len Adelman).

Az RSA-t bemutató eredeti feladványt Martin Gardner tette közzé a *Scientific American* szakújságban, „Egy új fajta rejtjel, amelynek megfejtéséhez évmilliókra lenne szükség” – kicsit túlzó – címmel (Gardner 1977). Gardner itt leírta az algoritmust, majd megadta, hogy a következő, 129 jegyű N összetett számot kellene két prím szorzataként ($p \cdot q$ alakban) felírni a megfejtéshez: N = 114 381 625 757 888 867 669 235 779 976 146 612 … (az első 36 jegyet közöljük). A feladat (és maga az eljárás is) igen nagy érdeklődést keltett. Végül 17 év múlva, több mint 600 ember közös munkájával fel lett törve az RSA-129.[4]

A következőkben bemutatunk egy egyszerű RSA példát (Fekete 2014; Rothe 2004). Ehhez a következő fontos matematikai fogalmakra lesz szükségünk:

- Prímszámok (osztóik csak 1 és önmaguk);
- Relatív prímek (legnagyobb közös osztójuk 1; pl. 4 és 9, 8 és 15 stb.);
- Egészosztási maradék (pl. 10 (mod 4) = 2, jelölhető: $10 \equiv 2 \pmod 4$ stb.);
- Euler-féle φ függvény, $\varphi(n)$: 1, 2, …, n közül az n-hez relatív prímszámok darabszáma; és prímekre speciálisan: $\varphi(p) = p - 1$.

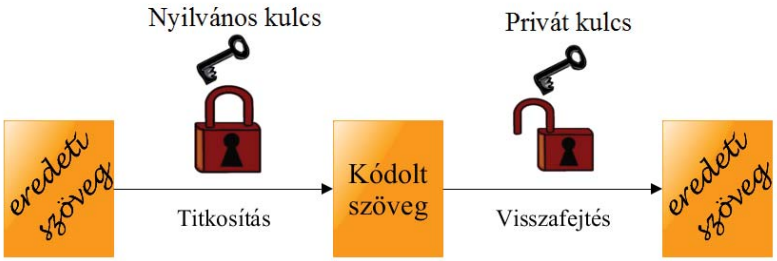
Konkrét példánkban válasszunk két prímet, ezek legyenek p = 59 és q = 97. Így $n = 59 \cdot 97 = 5723$, és $\varphi(n) = (p - 1) \cdot (q - 1) = 58 \cdot 96 = 5568$. Választunk egy e számot, ami relatív prím $(p - 1)$-hez és $(q - 1)$-hez, ez lesz a bekódoló kulcs. Sok ilyen szám választható, pl. lehet e = 73. Ezután kiszámolunk egy f számot, amire $e \cdot f \pmod{(p - 1) \cdot (q - 1)} = 1$ (azaz $e \cdot f \equiv 1 \pmod{\varphi(n)}$). Ilyen f egyértelműen létezik (az euklideszi algoritmus megfordításával kapható meg), nálunk most f = 4729. Ezzel elkészült a titkosítónk, az n és e számok nyilvánosak, f titkos.

Tegyük fel, hogy Bob barátunk a következő üzenetet szeretné küldeni nekünk: „secret message”. Ekkor Bob részéről először az üzenet számmá alakítása szükséges, választható pl. a = 01, b = 02, …, z = 26, szóköz = 00. Így az üzenet: „19 05 03 18 05 20 00 13 05 19 19 01 07 05 00” lesz. Ezután Bob kódolja (titkosítja) az üzenetet a következők szerint. Mivel az n szám 4 hosszú, ezért 3 hosszú részekre darabolja az üzenetet, és minden darabot felemel az e-edik hatványra, majd veszi a maradékot n-nel osztva. Pl. 190^73 mod 5723 = 1160, 503^73 mod

[4] A szükséges feltörési idő eredeti becslésénél nem vették kellő mértékben figyelembe a számítógépek műveletvégző képességének rendkívül gyors fejlődését, és a feltörő algoritmusok dinamikus fejlődését.

5723 = 1631 stb. Így megkapja a kódolt üzenetet, amit elküld nekünk: „1160 1631 2054 1490 0001 2117 5629 5078 0221 4210”.

A visszafejtésnél mi a (4 hosszú) darabokat felemeljük az *f*-edik hatványra, és vesszük a maradékukat *n*-nel osztva. Pl. 1160^4729 mod 5723 = 190, 1631^4729 mod 5723 = 503 stb. Végül visszakapjuk az eredeti szöveges üzenetet.



13. ábra: Az RSA titkosító működésének elvi vázlata
Forrás: tanszéki szerkesztés (Kallós–Pukler–Szörényi 2011)

Az RSA működésének matematikai igazolása Euler-tételével végezhető el, miszerint: ha *b* és *n* relatív prímek, akkor igaz, hogy $b^{\varphi(n)} \equiv 1 \pmod{n}$. Jelöljük *M*-mel az eredeti üzenetet, és *E*-vel a titkos üzenetet. Ekkor: $E^f \equiv (M^e)^f \equiv M^{e \cdot f} \equiv M^{\text{„}\varphi(n) \text{ többszöröse”} + 1} \equiv 1 \cdot M \equiv M \pmod{n}$, tehát a visszafejtésnél valóban az eredeti üzenetet kapjuk vissza (Bressoud 1989).

Természetesen a fenti példa a kis *n* szám miatt csak szemléltetésre alkalmas, valódi titkosításra nem. Ha ugyanis egy rosszindulatú külső személy meg akarja fejteni (fel akarja törni) a titkosításunkat, akkor neki a titkos kulcsot kell előállítani, amihez viszont φ(*n*) ismerete szükséges, tehát végeredményben az *n* szám felbontása $p \cdot q$ alakba. Ez kis *n*-ekre könnyen megy, nagyobb *n*-ekre viszont igen nehezen megvalósítható, lényegében lehetetlen (ha nem követünk el néhány hibát, pl. hogy *p* és *q* túl közel van egymáshoz vagy egyéb módon túl speciálisak). Az RSA biztonsága azon alapul, hogy nagyjából 400 jegyű (jó) *n* esetén a feltörés még a mai legjobb szuperszámítógépekkel is reménytelen vállalkozás. Érdemes kipróbálni ezt a Maple vagy a Wolfram Alpha rendszerrel! (Generálunk két nagy prímet, összeszorozzuk őket, és utána megpróbáljuk az így kapott *n*-et felbontani.)

Az RSA forradalmi újdonsága az, hogy hiába ismerjük pontosan a titkosítási módszert, mégsem tudjuk visszafelé alkalmazni a titkosítási lépéseket (az összes hagyományos titkosítással ellentétben), tehát nem juthatunk el a megfejtéshez. A magyarázat pedig a háttérben „elbújt” matematika: a prímfelbontás a mai ismereteink szerint nagy *n*-ekre „nagyon nehéz” feladat.

Befejezés

Még rengeteg érdekes témáról folytathatnánk az elemzést (akár a jövőre vonatkozóan is, pl. kvantumszámítógép), de a terjedelmi korlátok miatt most a bemutatás végére értünk. A tanulmány elején felvetett kérdésre (hipotézis) a válaszunk határozott igen, a titkosítások és visszafejtések ötleteiben (és sikerességében) visszatükröződik az adott korszak technológiai fejlettsége, erős a korreláció.

Az érdeklődő olvasó folytathatja a „kirándulást” a kriptográfia területén, mert a cikkben bemutatott szakirodalmakat úgy válogattuk, hogy a témában való további önálló elmélyedéshez is megfelelő alapot nyújtsanak. Természetesen további hasznos hivatkozásokat is találunk bennük. Külön érdemes kiemelni a Gómez (2016) munkáját, amely 2019-ben magyarul is megjelent.

Irodalom

Bressoud, D. 1989. *Factorization and Primality Testing*. New York: Springer-Verlag.
Fekete I. 2014. *Dan Brown digitális erődje és a nyilvános kulcsú titkosítás.* Budapest: ELTE TTK (szakdolgozat).
Gardner, M. 1977. Mathematical Games. A New Kind of Cipher that Would Take Millions of Years to Break. *Scientific American* Aug., 120–124.
Gómez, J. 2016. *Mathematicians, Spies and Hackers; Coding and Cryptography*. London: RBA Coleccionables, S. A.
Kallós G.–Pukler A.–Szörényi M. 2011. A számolás története és a kódolás. In: Pukler A. (szerk.): *Informatikai rendszerek alapjai*. Győr: SZE.
Kahn, D. 1996. *The Codebreakers: The Story Of Secret Writing*. New York: Scribner.
Katzenbeisser, S.–Petitcolas F. 2000. *Information Hiding Techniques for Steganography and Digital Watermarking*. Boston: Artech House.
Papp P.–Szabó T. 2006. A kriptográfiai biztonság megközelítési módjai. *Alk. Mat. Lapok* 23: 207–294.
Rothe, J. 2004. Kriptográfia. In: Iványi A. (alkotó szerk.) *Informatikai algoritmusok I.* Budapest: ELTE Eötvös Kiadó, 94–124.
Verne, Gy. 1980. *Sándor Mátyás*. Budapest: Móra Kiadó.

Internetes hivatkozások

https://shopretroworks.com/products (letöltési idő: 2020. november 12.)
https://educalingo.com (letöltési idő: 2020. november 12.)
https://www.une.edu.au/info-for/visitors/museums/museum-of-antiquities/codebreaker-challenge (letöltési idő: 2020. november 10.)
mathematicalstamps.eu (letöltési idő: 2020. november 13.)