FIATAL MŰSZAKIAK TUDOMÁNYOS ÜLÉSSZAKA

Kolozsvár, 2004. március 26-27.

REJTJELEZÉS

Tomka Ildikó

Abstract

Nowadays the most important thing is not who you know or what you know but what you know about the people you know.

Kivonat

Ma már nem az számít, hogy mit tudunk vagy kit ismerünk, hanem hogy mit tudunk azokról, akiket ismerünk.

1. Bevezetés

A titkok megőrzésének vágya gyakorlatilag egyidős az írásbeliséggel - amint volt mit titkosítani, ki is találták rá a kor rejtjelezésének megfelelő titkosító módszert. A rejtjelfejtők pedig igyekeztek megfejteni az egyes módszereket, minek következtében a titkosítás egyre fejlettebb lett, és fejlődik napjainkig. Már a legelső titkosítási módszerek is, hol kriptográfiai („rejtett írás”), hol szteganográfiai („fedett írás”) technikákat alkalmaztak.

Utóbbi lényege a küldött üzenet létezésének elrejtése. Míg az i.e. V. században az is elég volt, hogy egy leborotvált hajú ember bőrére írták az üzenetet, megvárták, míg kinő a haja, majd elküldték a címzetthez, a II. világháborúban egyes német ügynököknek már a modern technikára kellett támaszkodniuk: a mikropont néven ismert módszerrel egy gépelt oldalnyi szöveget egy milliméternél is kisebb ponttá zsugorítottak, majd egy ártalmatlan levélben elhelyezték, mint mondatvégi pontot.

A szteganográfia nagy hátránya viszont, hogy ha az üzenet létére fény derül (mint az többször meg is történt a mikropont-módszer esetében), fény derül az üzenet tartalmára is. Így a kriptográfia, az üzenet tartalmának elrejtése is fejlődésnek indult. A két módszer ugyan teljesen eltérő, együttes alkalmazásuk az üzenet biztonságát megnöveli. (Még ha rossz kezekbe kerül is az elrejtett üzenet, elolvasni már nem tudják.)

2. A Kriptográfia

2.1. A kriptográfia is két részre oszlik: átrendezésre és behelyettesítésre.

Az átrendezés nem más, mint az üzenetet alkotó írásjelek más sorrendbe helyezése. Egy viszonylag rövid, tízbetűs mondatot három és félmillióképpen lehet leírni - egy harmincbetűs mondatnál viszont

már körülbelül $5 \cdot 10^{24}$ lehetőség van, így az eredeti mondat kitalálása egy kevés időt - pár milliárd évet - venne igénybe.

A teljesen véletlenszerű átrendezés, bár igen nagy biztonságot ad, titkosításkor és visszafejtéskor is sok időt vesz igénybe. Ezért a feladó és a címzett előre megállapodik egy bizonyos átrendezési módszer használatában. Ilyen például a „fésűs” módszer: az üzenet betűit felváltva a felső vagy az alsó sorba írják, majd az alsó sort a felső végéhez illesztik - így egy zagyva betűsor alakul ki. A módszer továbbfejlesztett változatában több sorba is lehet írni a betűket, és természetesen ott van a katonai rejtjelezés egyik legelső eszköze, a szkütalé is, a spártai vezérek parancsnoki botja. Szabályos, sokszög alapú hasáb, mely köré bőrszalagot tekertek, az üzenetet ráírták, a bőrszalagot letekerték, majd akár övnek álcázva elszállították a címzethez, aki szintén szabványméretű szkütaléval rendelkezett.

2.2. A behelyettesítés

Az átrendezés alternatívája a behelyettesítés, melyet már a Káma-szutra is melegen ajánlott a nők figyelmébe, szerelmi viszonyaik eltitkolására. Lényege az ábécé betűinek tetszőleges párosítása, majd az üzenet módosított betűkészlettel történő leírása. Egyik leghíresebb alkalmazása a gall háborúk idején volt - Julius Caesar bajban levő vezérének szánt üzenetét görög betűkkel írta latin helyett. Bízást számíthatott rá, hogy az ellenség nem tud ógörögül.

Caesar másik kedvence a később Caesar-kódként elhíresült módszer volt: az egyes betűk helyett a hárommal utánuk következőt írta le. Ez a módszer viszonylag egyszerűnek és könnyen megfejthetőnek tűnik - amíg eszünkbe nem jut, hogy (az angol, 26 betűs ábécét alapul véve) összesen 25 féle eltolás lehetséges, és hogy nem kell feltétlenül eltolni - át is lehet rendezni az egészet. Így máris $4 \cdot 10^{26}$ darab kódábécénk van, melynek megfejtése bizony időbe telik.

3. Kerckhoff-elv

A Kerckhoffs-elv szerint „a kódolási rendszer megbízhatósága nem függhet a titkosítás algoritmusától, azt csak a kulcs titkának megőrzése garantálja.”

A kriptográfia alapköve tehát a kulcs, a titkosító algoritmus megfejtéséhez többnyire ugyanis a kulcs ismerete szükséges (lehetséges az anélküli visszafejtés is az úgynevezett „brute force” módszerrel, ez azonban aránytalanul sok időbe telik). Azon kívül, hogy a kulcsnak titokban kell maradnia, szükséges az is, hogy kellő számú lehetséges kulcs legyen (a Caesar-kódnál ez a feltétel nem teljesül, hiszen mindössze 25 lehetséges kódábécé van), illetve hogy a kulcs ismerete nélkül az algoritmus kellőképp megfejthetetlen legyen (az ábécé véletlenszerű átrendezése nem ilyen; egyszerű betűeloszlás-elemzéssel viszonylag könnyen megfejthető). Mivel a rejtjelezők és rejtjelfejtők közti küzdelem a

kódolás korai időszakában leggyakrabban az utóbbiak javára dőlt el¹, a rejtjelek készítőinek valami nehezebbet kellett kitalálniuk - az egyszerű monoalfabetikus rejtjelek túl könnyen feltörhetőek voltak.

4. Vigenere-kód

Az úgynevezett Vigenere-kód alapjai a XV. századba nyúlnak vissza, de végleges formáját a XVI. században nyerte el Blaise de Vigenere francia diplomata munkássága révén. Nagy előnye, mely évszázadokig feltörhetetlenné tette, a polialfabetikusság (több kódábécé használata) volt. A kód 26 különféle kódábécét használ a nyílt szöveg rejtjelezésére. A titkosítás első lépése a Vigenere-tábla elkészítése, melyben a nyílt ábécét 26 kódábécé követ, melyek mindegyikét egy hellyel eltolják az előzőhöz képest. Így az első kódábécé a nyíltábécé egybetűs eltolásával létrehozott Caesar-kód, a második kétbetűs, stb.

A Vigenere-sifre alkalmazásakor az eredeti üzenet betűit a Vigenere-tábla más-más sora szerint sifrírozzák. Az üzenet elolvasásához a címzettnek tudnia kell, melyik betűhöz melyik kódábécét használták, ezért tudnia kell a kulcsot is, ami egy szó. A kulcsszót a rejtjelezendő szöveg fölé írták, annyiszor ismételve, hogy minden betű fölé jusson, majd az üzenet első betűje fölötti kulcsbetűhöz tartozó kódábécé-sor szerint rejtjelezték az üzenetet.

A Vigenere-kód nagy előnye, hogy egy betűt több betűvel lehet helyettesíteni, így a gyakoriságelemzők tehetetlenül álltak előtte². Nagy hátránya volt viszont, hogy a használata nehézkes volt, mind kódolás, mind dekódolás szempontjából, így igen kevesen használták.

Megfejteti is csak jó háromszáz év múlva sikerült. Charles Babbage egy kihívásra válaszolva nekilátott a gyenge pontok keresésének, és talált is. A Vigenere-kódban ugyanis találhatók ugyanolyan betűcsoportok, melyek elárulhatják, milyen hosszú is a kulcsszó. Ezután pedig a megfejtés már viszonylag egyszerűen visszavezethető a gyakoriságelemzésre. Természetesen, ha a kulcsszó épp olyan hosszú, mint maga az üzenet, a feltörés némiképp megnehezedik, de nem válik lehetetlenné.

5. Enigma kódológép

Miután a Vigenere-kód is feltörhetőnek bizonyult, a rejtjelezőknek valami újat kellett felmutatniuk. Ez meg is történt 1918-ban, mikor Arthur Scherbius német feltaláló bemutatta az Enigma nevű kódoló gépet, mely görcsös fejfájást okozott sok kódtörőnek. A szerkezet három fő egységből állt, amelyeket vezetékek kötöttek össze: egy billentyűzet a nyílt szöveg betűinek bevitelére; egy keverőegység amely a nyílt szöveg betűit a kódszöveg megfelelő betűivé alakítja; és egy kijelző panel, amelyen kis

¹ A monoalfabetikus (egy kódábécét használó) titkosírás megfejtése először az araboknak, a kriptóanalízis megalapozóinak sikerült. A különböző nyelvek tanulmányozása során rájöttek ugyanis, hogy egyes betűk gyakrabban fordulnak elő más betűknél - így leegyszerűsítve a dolgot, a rejtjelfejtőknek nem volt más dolguk, mint megszámolni a megfejtendő szövegben a jelek számát, majd a leggyakoribb jel helyére behelyettesíteni a leggyakoribb betűt, és így tovább.

² Az ún. homoalfabetikus kód is kivédi a gyakoriságelemzést: minden betűhöz az előfordulása szerinti számú jelet rendelnek (a magyar nyelvben az e betű átlag 12%-a egy szövegnek, így az e betűhöz 12 jel szükséges). Ezzel a módszerrel minden jel pontosan 1%-os gyakoriságú.

lámpácskák felvillanása jelzi a kódszöveg betűit. A nagy ötlet pedig az volt, hogy a keverőtárcsa minden betű leütése után $1/26$ -nyit elfordul, így ha egymás után 26-szor kódolják ugyanazt a betűt, 26 különböző jelet kapnak vissza. A lehetséges kulcsok száma $26 \cdot 26 \cdot 26 \cdot 6 \cdot 100\,391\,791\,500$ (három keverőtárcsa az ábécé betűivel * tárcsák elrendezése * a 26 betűs ábécé 6 betűjének lehetséges elrendezése), mintegy 10^{15} darab.

Az Enigma 1926-ban mutatkozott be először, és bár a franciák 1931-ben jó pénzért szereztek egyet, a vele rejtjelezett üzenetek továbbra is megfejthetetlennek bizonyultak, hiszen a németek a kód biztonságának tesztelésekor feltételezték, hogy a gép az ellenség kezében van. Ráadásul 1938-ban az Enigmákat két újabb keverőtárcsával látták el, alaposan megnehezítve a feltörésüket. Ezzel szemben a II. világháború alatt az angliai Bletchley Parkban többnyire sikerült megfejteni az üzeneteket - esetenként nem csak matematikai módszerekre támaszkodva.

Összefoglalás

A nyilvános kulcsú rejtjelezési módszerek a legmodernebb rejtjelezési módszerek, amelyek a korábbi, titkos kulcsú módszerek legtöbb hátrányát kiküszöbölik. Alapötlete, hogy a kódolás, titkosítás folyamatát elválasztja a dekódolástól, és olyan algoritmust használ, ahol a kódoláshoz használt kulcs nem azonos a dekódoláshoz használt kulccsal. Feltörésük hagyományos módszerekkel igen nehéz vagy lehetetlen, így a mai üzleti életben is biztonsággal használhatóak. Legismertebb változata, az RSA algoritmus (kitalálói, Rivest, Shamir és Adleman nevéből) aszimmetrikus, nyílt kulcsú rejtjelezés, mely a nagyon nagy prímszámokon alapul. A feladónak és a címzettnek is van privát és publikus kulcsa is - előbbit csak a tulajdonosa ismerheti. Az üzenetet a feladó a címzett nyilvános kulcsával kódolja, így az csak a címzett titkos kulcsával kódolható vissza. Az RSA-algoritmust digitális aláírásként is lehet használni, mivel a címzett a feladó publikus kulcsával ellenőrizheti az üzenet hitelességét. Az algoritmus nagy hátránya viszont a lassúsága, így gyakran a gyorsabb szimmetrikus (egykulcsú) titkos kulcsú algoritmusokkal (például DES, Data Encryption Standard) együtt használják.

Irodalom

- [1] Simon Singh: Kódkönyv (Park Könyvkiadó, 2001)
- [2] Virasztó Tamás: Titkosítás és adatrejtés (NetAcademia Oktatóközpont, 2003)
- [3] RSA Laboratories (www.rsasecurity.com)

Tomka Ildikó, hallgató
BMF, Bánki Donát Gépészmérnöki Kar
Budapest 1081 Népszínház u. 8
Tel: (+36-1) 314-1438
E-mail: vissai@turul.banki.hu