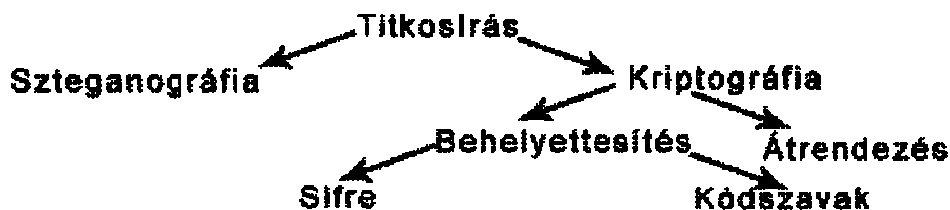


A SecINFO következő számaiban a titkosírás fejlődését követjük nyomon.

Reflektorfényben a
TITKOSÍRÁS



Szteganográfia

A *szteganográfia* az üzenetek titkos továbbításának legősibb módja az üzenet elrejtése. A szó jelentése rejtett írás.

Egy esetben egy Demaratosz nevű görög, aki, bár elkergették hazájából, hű maradt Görögországhoz, a perzsa had készülődését látva viasszal fedett egy palatáblát, amire korábban már írt. Mivel sürgősen át kellett a táblát csempészni, nem maradt idő ezt a módszert egyeztetni, így a megérkező üzenet nyitjára Kleomenész lánya, Gorgo (egyben Leónidasz felesége) jött rá. A meglepetés erejének hiányában a perzsák megsemmisítő vereséget szenvedtek.

Hérodotosz számol be arról, hogy a perzsa király ellen szövetkezni akaró Hisztiaieusz leborotváltatta a küldöncének haját, ráírta az üzenetet, majd megvárta, amíg a küldöncének haja újból kinő, így átkelhet a határon. Bár ez nagyon ráérő módszer, akkor még volt rá idő. A küldönc célba ért, leborotváltatta fejét és megmutatta a címzett Arisztagorasznak.

A kínaiak selyemlabdacskokra írták az üzenetet, melyet viasszal fedtek, majd a küldönc lenyelte.

Giambattista della Porta, egy olasz tudós leírta, hogy timsó és ecet elegyéből készített tintával a tojás héjára írva az írás csak a héj eltávolításával válik láthatóvá.

Már az első évszázadban leírta idősebb Plinius azt, hogy pitypang tejével is lehet írni, hiszen az száradás után láthatatlan, de melegítésre barna lesz. Ez a tulajdonság sok szerves vegyületben megvan, így előfordult, hogy a kémek saját vizeletükkel írtak. Használható hagymalé vagy tej is.

A Dél-Amerikában tevékenykedő német ügynökök a szöveget egy milliméter nagyságúra zsugorították és ezt egy lényegtelennek tűnő szövegre helyezték. Ezt az FBI 1941-ben vette észre egy kapott üzenet segítségével. Ezt a módszert néha vejtették kriptográfiával is.

A kriptográfia

A kriptográfia a *szteganográfiával* egyidőben alakult ki, és célja nem magának az üzenetnek, csupán csak a tartalmának, jelentésének elrejtése, kódolása, hiszen a határőrök előbb-utóbb az üres lapot felmelegítik, leborotváltatják a haját, azaz rájönnek a módszerre.

A *kriptográfia* két ágra oszlik: átrendezésre (keverésre) és behelyettesítésre.

Szkütalé

Átrendezésnek nevezzük azt a titkosítási módszert, amikor az üzenet szövegének betűit véletlenszerűen, vagy valamilyen szabályrendszer alapján átrendezik – a betűk megtartják eredeti hangértéküket, de megváltoztatják a pozíciójukat. A módszer előnye, hogy a betűk számának növekedésével rohamosan csökken az esély. Egy 35 betűs mondat, ha másodpercenként egy lehetőséget tudna az ember ellenőrizni, a világmindenség élettartamának ezerszerese lenne. Az egyik gyakori módszer a *fésűs*, ahol a betűket soronként változtatva jön ki az eredmény. Ennek a megfejtése a betűk soronkénti hasonló felírása (a felénél elválasztva). Létezik módszer, ahol a betűpárokat felcserélve jön ki az eredmény, például: megkeverve→gkmervvee.

A spártai szkütaléra az ábrán láthatóhoz hasonlóan feltekertek egy papírt, erre vízszintesen írták a szöveget és így értelmetlen lett. I. e. 404-ben a perzsiai támadást így kapott üzenetből tudta meg Lüszaandrosz spártai hadvezér.

Behelyettesítés

A behelyettesítési módszer esetén a nyílt szöveg minden betűjét egy másikkal helyettesítik – a betűk megtartják pozíciójukat, de megváltozik a hangértékük.

E titkosításról szóló első leírás érdekes módon a Káma szútrában található, amelyet a 4. században vetett papírra egy brahmin tudós, Vátszjájana, egy kétszáz évvel régebbi kézirat alapján.

Időszámításunk első évezredének titkosírását – egyszerűsége és megbízhatósága révén – a behelyettesítési kód uralta.

Monoalfabetikus kódok

Azokat a behelyettesítési kódábécéket nevezzük monoalfabetikusnak, amelyek egy betűt egy másik betűvel vagy szimbólummal helyettesítenek. A módszer katonai célokra használatát először Julius

Caesar *A gall háborúk* című műve írja le. Itt a latin betűket görögökkel helyettesítette és ezt hajította be a megadás küszöbén álló Cicerónak.

A Káma-szútrában található módszer

A Káma-szútrában található leírás az ábécé betűinek véletlenszerű párosítását és egymásnak kölcsönös megfeleltetését ajánlja. Ez a nőknek ajánlott 64-művészet közül a 45., a mlekhitavikalpa. Például a 26 betűből álló angol ábécé esetén:

Betűk megfeleltetése

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | D | H | I | K | M | O | R | S | U | W | Y | Z |
| X | V | G | B | Q | J | C | T | L | N | F | E | P |

Kódolás

| | |
|-----------------|------------------------------|
| Az üzenet | kriptográfia (→kriptografia) |
| A kódolt szöveg | QTBZRCHTXWBX |

Atbas

Az atbas egy egyszerű helyettesítő rejtjel a héber ábécéből kiindulva, ám később más ábécékre is elterjedt. A működése során az első és utolsó, második és utolsó előtti, stb. betűk felcserélésén alapul. A neve is innen ered: alef (1. betű), táv (utolsó), bét, sin betűk nevéből. Például a Jeremiás 25:26 és 51:41-ben a Bábelt a Sesah helyettesíti a Bibliában. Az ilyen és hasonló bibliai kódok valószínűleg csak rejtélyességet akartak kelteni, nem a jelentés palástolása volt a céljuk. Ennek egy változata az albam, ahol a módszert két fél ábécén hajtották végre.

Polübiosz-négyzet

A A Polübiosz-rejtjelegy egyszerű titkosítási eljárás, melynél az ABC 25 betűjét egy táblázatba foglalták. Itt a rejtjelezett betűk a mátrix elemeinek feleltek meg, a sorok és az oszlopok azonosítójából olvasták le a kétjegyű kódot. A rejtjelezett kódot fáklyákkal adták tovább, a jobb- és balkézben egytől ötig terjedő égő fáklyákkal. A módszer hátránya az volt, hogy csak sötétben, jól látható magaslatról volt használható, illetve a szöveget betűnként küldte el.

| Kódtábla | | | | | | Kódolás | |
|----------|---|---|---|---|---|---------|---|
| | 1 | 2 | 3 | 4 | 5 | | |
| 1 | A | B | C | D | E | | |
| 2 | F | G | H | I | K | A | w |
| 3 | L | M | N | O | P | A | 5 |
| 4 | Q | R | S | T | U | | |
| 5 | V | W | X | Y | Z | | |

Polübiosz-tábla

A

Caesar-rejtjel

A Caesar-rejtjel, melyet Julius Caesar írt le, mint általa használt eljárást. Itt Caesar az ábécét egy bizonyos számmal eltolta, azaz ha az n . betűből az m . lett, akkor az $n+1$ -edikből $m+1$ k-s maradéka, ahol k az ábécé hossza (például az angol ábécénél 26 betű).

A napjainkban is gyakran használják az 1980-as években elterjedt **ROT13** (rotate by 13 places, 13 hellyel forgatás) nevű speciális Caesar-kódot fórumokban. Ez tizenhárommal van eltolva, így a dekódolás is pontosan ugyanaz a művelet.

Egy másik változata a ROT47, amit az ASCII 33-as (!) és 126-os (~) jelű karaktere között hajtanak végre. Ez 47 hellyel van eltolva, ami hasonló tulajdonságokat eredményez, mint a ROT13.

Általános behelyettesítési algoritmus

Ez az algoritmus kiküszöböli a Caesar eltolásos ábécéjének gyengeségét, ugyanis a kódábécé a nyílt ábécé bármelyik tetszőleges átrendezése lehet. Hátránya, hogy a véletlenszerű párosítás miatt a kódot nehezen lehet fejben tartani.

Általános behelyettesítési algoritmus kulcsszó vagy kulcsmondattal alkalmazásával

Az előző módszeren alapuló algoritmus, ám a kulcsmondattal alkalmazásának következtében a kódábécé megjegyzése egyszerűbbé válik. A kódábécé a kulcsmondattal különböző betűivel fog kezdődni, majd annak utolsó betűjétől a normál ábécé szerint folytatódik (természetesen a már felhasznált betűk kihagyásával). Igaz ugyan, hogy e megszorítások miatt a lehetséges kulcsok számának csökken, de a feltörés szempontjából nem számottevő mértékben. (Bár észrevéve az értelmes szavakat vagy legalábbis a részeit a megfejtés egy része után könnyebb lesz a megfejtés.)

Monoalfabetikus kódok

A 15. századra már Európában a kriptográfia virágzott. itáliában különösképpen

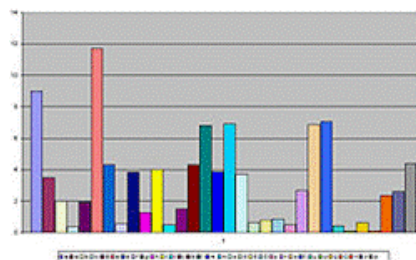
gyakori volt, hiszen a különböző városállamokban elhelyezett követeknek leveleznie kellett. Ekkor hozták létre a *titoknoki* állást. Az első ilyen személy a feltételezések szerint az olasz Giovanni Soro volt, 1506-ban nevezték ki. A Vatikán is küldött neki kódokat. 20 évvel kinevezése után küldött a pápa egy levelet, amit a firenzeiek elfogtak, hogy fejtsse meg. Soro megfejthetetlennek nevezte, de vélhetően azért, hogy a Vatikán ne fejlesszen ki egy nehezebb kódot. A földrész más területein, például Franciaországban is elkezdtek kriptográfusokat alkalmazni. Ide tartozott Philibert Babou is. A 16. század végén tűnt fel François Viète, aki elsősorban a spanyol kódok megfejtésén dolgozott. A naiv spanyolországi kriptográfusok, látván, hogy megfejti a kódjukat, kijelentették, hogy az ördöggel cimborál és pápai bíróság elé akarták állíttatni. A vatikániak, tudván, hogy ők is olvassák a kódot a kriptográfusai segítségével, megtagadták ezt.

Az arabok is a monoalfabetikus behelyettesítési kódot használták a közigazgatásban is.

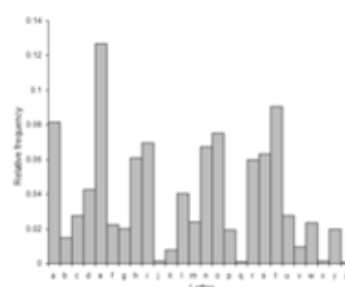
Az alkimisták

Az alkimisták gyakran szimbólumokat használtak szavakra, betűkre. Például a főleg irodalmi téren ismert Geoffrey Chaucer a Traktátus az asztrolábiumról című művéhez szimbólumokkal írt egy kiegészítést. Noha ez a módszer biztonságosabbnak tűnik, ugyanannyira megfejthető, mintha betűket helyettesített volna be.

A monoalfabetikus kód feltörése



A magyar karakterek gyakorisága:



Az

angol

karakterek gyakorisága.

Az arab rejtjelfejtők találták fel a **kriptoanalízist**, ami a kódolt szövegek kulcs nélküli megfejtését jelentette. Ehhez a statisztika, matematika és nyelvészet különösen magas fokú ismerete kellett. A módszerről először Jákúb ibn Iszhák al-Kindi írt a 9. században.

„...veszünk egy ugyanolyan hosszú szöveget, ami elég hosszú ahhoz, hogy legalább egy lapot megtöltsön és megszámláljuk, melyik betű hányszor fordul elő benne. „

Al-Kindi azt írja, hogy az elsőként szereplő az első, ám ez nem mindig igaz, viszont hosszabb szövegeknél feltételezhető, hogy a 10% fölötti az angolban az **e** lesz. Ez nem mindig igaz, például rövid szövegekre (*Zanzibárt támadjuk*). Emellett a francia Georges Perec 1969-ben megjelentetett egy könyvet *La Disparition* címmel, aminek 200 oldalán nem található egyetlen **e** betű sem. Ezt Gilbert Adair angolra lefordította angolra *A Void* címmel. Európa ezt a módszert vélhetőleg átvette, bár lehet, hogy újból kialakította.

Egyéb módszerek

A megfejtési lehetőségek, egyszerűsítések közé tartozik a kettőzött betűk vizsgálata (az angolban ezek főleg **ss**, **ee**, **tt**, **ff**, **ll**, **mm**, **oo**). Aszóközök megléte esetén az **egy**, a kétbetűs szavak és a hárombetűs leggyakoribb szavak (az angolban **the** és **and**) is a gyakori fogások közé tartoznak. Emellett sokszor igazítani kell a környezethez a gyakorisági táblázat szövegét. Például a katonai üzenetekben kevés **I**, **the** található az angolban. Amennyiben a leggyakoribb az **e**, aztán **t** jön, és hasonlóan folytatódik a gyakorisága a betűknek, akkor betűkeverés kód van a szövegben.

A gyakoriság eltorzítása

A megfejtés megnehezítésére használható módszer a gyakoriság eltorzítása, például *ltorzitot gja korisság*.

Behelyettesítési algoritmus nullításokkal

A nyugati reneszánsz idején azokban az országokban, ahol már felismerték a monoalfabetikus kód gyenge pontjait, egyéb elemekkel próbálták javítani a kód hatékonyságát. Az egyik ilyen volt a nullítások bevezetése, ami a semmit nem jelentő karaktereket jelenti. Ez a gyakoriságelemzést nehezíti meg.

Kódok a Bibliában

Michael Drosnin 1997-ben írt egy könyvet *A Biblia kódja* címmel, amelyben azt írta le,

hogy a Bibliában egy tetszőleges betűtől kezdve egy bizonyos hellyel előreugorva nagyszámú EETLB található a Bibliában, vagyis nullítások vannak benne. Drosnin úgy vélte, hogy az EETLB-k egész mondatokat tartalmaztak, ezáltal látta bennük John F. és Robert Kennedy vagy épp Anvar Szadat meggyilkolását, de találmányokat is felfedezett benne. A könyvet rengetegen kritizálták. Brendan McKay hasonló módon a Moby Dick-ben tizenhárom híres ember meggyilkolására talált állítást, ezzel demonstrálva a "felfedezés" hibásságát. Emellett a héber szövegek kevés magánhangzót tartalmaznak, így sok EETLB található bennük.

Behelyettesítési algoritmus és nomenklátor

A monoalfabetikus kód javítását célozta a szórajstromok (nomenklátorok) bevezetése is, ami azt jelentette, hogy a titkosítandó szöveg egyes szavait külön szimbólummal jelölték, a fennmaradó részt pedig a szokásos módon titkosították. Előfordult az is, hogy minden szót külön jelöltek, ám ehhez fáradságosan szétosztható kódkönyv kellett, aminek elvesztése beláthatatlan következményekkel járhat.

Ilyen típusú titkosítást használt Mária skót királynő a Babington-összeesküvésben résztvevőkkel egyetemben. Ám Thomas Phelippes (I. Erzsébet miniszterének, Sir Francis Walsinghnek a titoknok) megfejtette a levelezést és az összeesküvőket elítélték. Ebben az ügyben rengeteg múlt a titkosírás megfejthetőségén, hiszen Erzsébet vonakodott a levelek tartalmának ismerete nélkül halálra ítélni Máriát. Az elítélésben szerepet játszott a katolikus Gilbert Gifford, aki a leveleket csempészte be, de eközben az angol udvart segítette. Az összeesküvés tagja volt Anthony Babington, aki viszont Máriát segítette. A kódábécé négy nullításból, az ábécé 23 betűjéből (a j, v, w nem volt benne) és harmincöt szavakat vagy kifejezéseket helyettesítő karakterből állt. Miután Phelippes megfejtette a titkosírást, utóiratot hamisított rá, ezáltal az összeesküvőket is elítélték, mert Mária nem vette észre a hamisítást. Példa: az „öljétek meg a királyt ma” szövegből „X□i” lesz.

| | | |
|----------------|---------------|----------------|
| megölni = X | herceg = § | holnapután = μ |
| megtámadni = ~ | miniszter = # | ma = i |
| megvédeni = √ | király = □ | azonnal = □ |

Homofonikus behelyettesítés

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 6 | 6 | 2 | 4 | 5 | 7 | 2 | 4 | 5 | 9 | 9 | 2 | 4 | 5 | 2 | 4 | 5 | 2 | 4 | 6 | 0 | 1 | 1 | 3 | 5 | 7 |
| 4 | 5 | 0 | 2 | 6 | 4 | 1 | 3 | 7 | 0 | 1 | 2 | 4 | 8 | 3 | 5 | 9 | 4 | 6 | 0 | 2 | 1 | 6 | 8 | 2 | 0 |
| 1 | 1 | 2 | 4 | 6 | 8 | 9 | 1 | 3 | | | 5 | 7 | 3 | 3 | 2 | | 6 | 8 | 8 | 4 | | 4 | | 3 | |
| 4 | 5 | 5 | 7 | 1 | 7 | 9 | 7 | 9 | | | 3 | 1 | 6 | 7 | 6 | | 2 | 8 | 9 | 8 | | 9 | | 1 | |
| 5 | | 5 | 5 | 2 | | | 6 | 0 | | | 7 | | 3 | 5 | | | 7 | 0 | 1 | 3 | | | | | |
| 4 | | 0 | 1 | 7 | | | 3 | 6 | | | 2 | | 2 | 5 | | | 9 | 0 | 2 | 4 | | | | | |
| 7 | | | 3 | 1 | | | 6 | 0 | | | 6 | | 0 | 0 | | | 1 | 3 | 1 | | | | | | |
| 3 | | | 3 | 0 | | | 6 | 7 | | | 8 | | 3 | 1 | | | 3 | 5 | 8 | | | | | | |
| 6 | | | | 1 | | | 7 | 8 | | | | | 9 | 2 | | | 2 | 3 | 4 | | | | | | |
| 7 | | | | 9 | | | 6 | 1 | | | | | 3 | 8 | | | 9 | 0 | 0 | | | | | | |
| 7 | | | | 0 | | | 4 | 0 | | | | | 8 | 9 | | | 8 | 7 | 9 | | | | | | |
| 5 | | | | 8 | | | 1 | 9 | | | | | 2 | 4 | | | 0 | 7 | 6 | | | | | | |
| 9 | | | | 8 | | | | | | | | | | 8 | | | | | 8 | | | | | | |
| 7 | | | | 4 | | | | | | | | | | 6 | | | | | 5 | | | | | | |
| 0 | | | | 9 | | | | | | | | | | | | | | | 7 | | | | | | |
| 5 | | | | 2 | | | | | | | | | | | | | | | 8 | | | | | | |
| | | | | 8 | | | | | | | | | | | | | | | 9 | | | | | | |
| | | | | 3 | | | | | | | | | | | | | | | 5 | | | | | | |
| | | | | 0 | | | | | | | | | | | | | | | | | | | | | |
| | | | | 4 | | | | | | | | | | | | | | | | | | | | | |
| | | | | 6 | | | | | | | | | | | | | | | | | | | | | |
| | | | | 9 | | | | | | | | | | | | | | | | | | | | | |
| | | | | 8 | | | | | | | | | | | | | | | | | | | | | |

A rejtjelezőkkel szemben a rejtjelfejtők kerültek lépéselőnybe. Kerestek egy közbülső megoldást, hogy ne a monoalfabetikus (időnként még mindig megbízhatónak hitt) kódot kelljen használniuk és ne is a veszélyes nomenklátorokat. Erre találták ki a homofonikus behelyettesítést, aminél a betűk gyakorisága alapján ugyanannyi lehetőség felelt meg egy betűnek, mint ahány százalék volt az elterjedtsége. A név eredete is innen jön: a görög homosz (ugyanaz) és fonosz (hang) szóból. Ez sem nyújt azonban tökéletes biztonságot, hiszen különböző módokon megfejthető. Például az angolban a legfeltűnőbb jelekkel a Q rendelkezik, ami után csak U állhat. A többi betűnek is vannak hasonló tulajdonságai, minden nyelvben.

Grand chiffre

A grand chiffre (nagy kód) eljárással kódolták XIV. Lajos legtitkosabb üzeneteit. A rendszert Antoine és Bonaventure Rossignol (apa és fia) dolgozta ki 1650 körül. 587-féle számot tartalmazott (betűket, szótagokat jelöltek), sőt voltak olyanok is, amik csapdába ejtették a kódfejtőt. Használtak például olyan kódszámot, ami csak az előtte lévő szám törlését volt hivatva jelölni.

1890-ben talált rá Victor Gendron a kódra, aki továbbadta Étien Bazeriesnek. Végül 1893-ban a francia hadsereg rejtjelfejtési osztályán dolgozva ő törte fel három év munkával.

| | |
|------------------|--|
| Az üzenet: | egyedem begyedem |
| A kódolt szöveg: | 56-21-52-61-42- 27-44 65-10-99- 31-19-47-08-71 |

A grand chiffre feltörése

Bazeries első elképzelése a homofonikus kód volt. Több hónapig próbálkozott ezen a tévúton, ám sikertelensége miatt feladta. A következő feltételezése a betűpárok jelzése volt. 26 betűből 676 különféle pár lehetséges, a szövegben 587-féle volt. Innen a leggyakoribb számokról (22, 42, 124, 125, 341) feltételezte, hogy a leggyakoribb es, en, ou, de, nt betűpárokat jelölik. Ez az út sem volt jó.

Innen következtetett a szótagokra. Ezekből statisztikát készített és ezekkel próbálkozott, ám ez sem adott jó eredményt. Ezek után sikerült egy számcsoporthoz azonosítania, amely viszonylag gyakran fordult elő a szövegben, és amiről Bazeries feltételezte, hogy az *ellenség* karaktorsorozatot jelenti (124-22-125-46-345 *les-en-ne-mi-s*). Innen a szavak jó részét ki tudta következtetni egymás után a meglévő szótagokból, ám a kódban "csapdák" is voltak, néha egy szám csak egy betűt jelentett, és volt, hogy olyan jelek szerepeltek a szövegben, ami törölte az előző két szótagot.

Miután megfejtette a szöveget, egy levélből kiderült, hogy a Vasálarcos, akiről régóta találgattak, kiderült, hogy Bulonde tábornok volt, akit a pignerole-i várba zártak. Egyesek szerint ezt pont a valós személy (akit XIV. Lajos ikertestvérének gondolnak) kilétének elrejtésére szánták.

Polialfabetikus kódok

Polialfabetikusnak nevezünk minden olyan helyettesítő rejtjelezést, amely többféle kód-ábécét használ az üzenet sifírozásakor. Leonardo Battista Alberti találta ki az 1460-as években egy pápai titkárral való beszélgetés során, két vagy három sifrét javasolt, de az elképzeléseit nem dolgozta ki egészen. Ezt Johannes Trithemius, majd Giambattista della Porta folytatta, ám végső kidolgozást Blaise de Vignère által nyert. Ez lett a Vignère-sifre, amit az 1800-as évekig nem tudtak feltörni. Az ilyen kódok több rejtjelezőnek is lassú módszer volt, kevésbé használták.

Vigenère-kód

A Vigenère-kód a polialfabetikus rejtjelek egy egyszerű fajtája, amely a rejtjelezés során egy adott kulcsszó betűitől függően, különböző Caesar-kódokat használ. A kód a következőképp működik: a táblázatban az összes Caesar-kód fel van tüntetve, minden betűvel, és a megfelelő kóddal kezdődő ábécé a kódolás alapja. A sifre a gyakorisági elemzéssel megfejthetetlen, hiszen például a *ketté* szóban a két t-t a legtöbb esetben más betű jelöli. A kód annyira biztonságos volt, hogy *le chiffre indéchiffrable* (feltörhetetlen kód) néven emlegették.

A kód megfejtése

A kódot Charles Babbage fejtette meg. A legtöbb kriptográfus már lemondott arról, hogy valaha is kitalálják a módszert, ám egy John Hall Brock Twaites nevű bristoli fogorvossal történő beszélgetés adott Babbage-nak lökést. Thwaites 1854-ben ugyanis feltalált egy "új" kódot, ami pont a Vigenère kód volt. Babbage mutatott rá, hogy a kód régi, erre Thwaites úgy reagált, hogy fejtse meg a kódot, ha régi. Babbage először megvizsgálta az ismétlődéseket egyes karaktereknél és ezek távolságát. Ez alapján táblázatba foglalta azokat. Például, ha 5-ös távközzel ismétlődik a PSDLP, akkor a táblázatba a PSDLP-hez az ötöt bejelölte. Innen megvizsgálta a leggyakoribb lehetséges távközöket, majd leírta a legvalószínűbb kulcsot $K_1-K_2-\dots-K_n$ formában. Minden ilyen K-ról gyakorisági analízist készített és összevetette a jellemzőkkel és a csony statisztikájú helyeket és megkereste, hogyan lehet eltolni, hogy ezek jelentős

százalékban egybeessenek. Bár a kódot vélhetően 1854-ben fejtette meg, kilenc évig, 1863-ig senki nem tudott erről, így Friedrich Wilhelm Kasiski nem találta meg, majd publikálta. Erre két magyarázatot találtak: az egyik szerint a publikálás nem volt Babbage erős oldala, a másik azt állítja, hogy a krími háború miatt nem engedték az angolok publikálni.

Következik:

KRIPTOGRÁFIA AZ ÚJ KORBAN