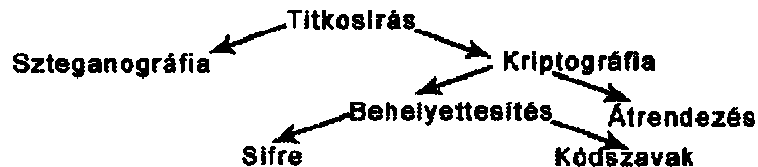


Kriptográfia az Újkorban

Reflektorfényben a TITKOSÍRÁS



Poligrafikus helyettesítő rejtjelek

A poligrafikus rejtjel során a rejtjelezést betűcsoportokon hajtják végre. Az első megjelenése ugyan 1563-as, de azt nem használták a nehéz megjegyezhetősége miatt. A kód első igazán használt megjelenése az 1854-es Playfair-rejtjel. Az ilyen kódok biztonságosabbak a sima monografikus behelyettesítésnél.

Megfejtése

A kódban jellegzetes, hogy a betűpárok fele csak ritkán vagy nem jelenik meg a szövegben. A megfejtése során a leggyakoribb betűtömböket azonosítják, majd kísérleteznek a cseréjükkel, végül kifejezéseket próbálnak megtalálni benne.

Playfair-kód

A Playfair-rejtjtjelet Sir Charles Wheatstone találta ki, Lyon Playfair báró propagálta. A kulcs a betűpárokat helyettesíti a következőképp: venni kell egy kulcsszót és ennek alapján egy 5-ször ötös mátrixba helyezni a betűket. Ezt követően az üzenetet betűpárookra tördelik, ha két betű egyezne (pl. merre), akkor közéjük x-et helyeznek, ha magányos betű marad a szöveg végén, oda is. A betűket ekkor a következőképp kategorizálják: a két betű ugyanabban a sorban van, ugyanabban az oszlopban vagy egyik sem. Ha az első eset, az ugyanolyan sor fordul elő, akkor a betűpár tagjaitól jobbra levőt veszik (a sor végén levőknél a sor elejét), ha a második, akkor

az alattuk levő, hasonló "átfordulással", ha a harmadik, akkor az első betű sorának és a második oszlopának metszéspontjában levő lesz a betűpár 1., a második betű sorának és az első oszlopának metszéspontjában levő a második.

Gyengesége

A kód gyengesége, hogy a leggyakoribb betűpárok alapján megfejthető. Ezek az angolban th, he, an, in, er, re, es.

Könyvkódok

A könyvkódokat még az első és a második világháború alatt is használták, gyakori kódok voltak. A lényegük az, hogy a könyvek alapján számozott betűkkel kódolnak. Polúbiosz például egy mátrixba rendezte a betűket és sor-oszlop számot írt le.

Beale-papírok

A Beale-papírokkal kapcsolatos összes eddig ismert információt egy 1885-ben kiadott füzet tartalmazza. 1820-ban Lynchburg városába érkezett egy Thomas J. Beale nevezetű személy, aki egy Robert Morriss nevű szállodatulajdonosnak adta át a papírokat, egy későbbi, 1822-es visszatérésekor. Azt mondta, hogy a papírokért jön később, de Beale eltűnt. Azt is állította, hogy 1832. júliusa előtt nem, de azután megkaphatja a kulcsot, ám ez nem történt meg. Morriss 1845-től próbálkozott megfejteni a talált három lapot. 1862-ben adta át egy máig ismeretlen barátjának, ő lett a közreadó. Ő arra következtetett, hogy

a számok nagy száma miatt ez egy úgynevezett könyvkód, ami azon alapul, hogy egy könyv betűit (esetleg oldalanként) megszámozzák és ezeket helyettesíti be. A második papírt rengeteg könyv kipróbálása után a Függetlenségi nyilatkozat segítségével oldotta meg. Ez a lap a kincsek mennyiségét és helyét (Bedford megye, Bufordtól mintegy négy mérföldnyire) jelölte. A szövegben tévedések is vannak, például a *four miles* (négy mérföldnyire) szóban a 95-ös számú u valójában inalienable, ám lehetséges, hogy a gyakori unalienable állt a szó helyén. A füzetek közreadását követően több hivatásos kriptográfus és kincskereső kereste a kincset, mindmáig sikertelenül.

A másik két lap megfejthetősége

Sem az első, sem a harmadik lapot nem fejtették még meg. A probléma az, hogy olyan magas szám, hogy 2906 nem szerepel az 1322 szavas Függetlenségi nyilatkozatban. Nehézség továbbá, hogy csak egyszer használták a kódot, így, ha Beale saját maga készített egy kulcsszöveget, amit nem nyomtattak ki és esetleg az, akinél biztonságba helyezte, elvesztette azt, akkor megfejthetetlen a kód.

Elméletek a kóddal kapcsolatban

Egy elmélet a kódok megfejthetlenségére, hogy meghamisította a kódokat a közreadó. Egy másik szerint azért nem találták meg a kincset, mert az NSA elvitte. Más elméletek szerint azért megtalálhatatlan a kincs, mert a történet hamis. Erre magyarázatnak vélik azt, hogy a levél tartalmazza a *stampede* szót, amit először csak 1834-ben írtak le. Emellett öt virginiai szövegmintát megvizsgálva a közreadó és Beale stílusa egyezik meg a legjobban. Amennyiben viszont hamisítvány volna a szöveg -állítják a kétkezdők- nem lenne annyira gondosan megírva (például a Függetlenségi nyilatkozat kulcsszövegnek vétele esetén előáll a majdnem ábécérendben levő abdefghijklmmnohpp betűfüzér). Egyesek szerint ez a betűfüzér egy bátorító utalás, miszerint a következő rész fejlődő meg, vagyis szupersifírozással titkosították a lapokat.

Pontokkal történő kódolás

A módszert, hogy egy szöveg betűi alá tűszúrásokat helyezve szöveget lehet küldeni, egy ógörög történész vetette fel. Mégis ez a fajta könyvkód legelterjedtebb nem titkosírásként volt, hanem költségkímélési okokból. Ugyanis Nagy-

Britanniában a posta reformjáig leveleket pénzért, újságokat viszont ingyen lehetett küldeni, így az emberek az újságok betűi alá pontokat szúrtak, ami ha nem nézik meg gondosan, nem volt feltűnő. A betűkből kijött a levél.

Egyszeri kulcsos titkosítás

A Vigenère-sifre hátulütője az ismétlődő kulcs. Ennek javítására van az egyszeri kulcsos titkosítás, ahol a kulcs ugyanolyan hosszú mint a szöveg. Amennyiben értelmes szavakból áll, akkor megfejtése a következőképp történik: elhelyezik a *the* szót (angol nyelven) különböző helyekre. Ahol értelmes szó lehet, akkor kipróbálják a többi lehetőséget (csak kevés lehetőség esetén, pl. YPT-nél). Ha értelmes résznek tűnő szöveg jön ki (például atthe), akkor a szavak alapján próbálnak következtetni a kulcsra. Például, ha EGYPT szerepel, akkor a CAN lehet CANADA. A szótöredékeket próbálják rekonstruálni a többi szó alapján, így ha például themee?????? atthe????, akkor valószínűleg meeting áll a szövegben. Ezt a szöveg megfejtéséig folytatják. Az első világháború alatt is kísérleteztek vele, de nem volt sikeres.

Morzekód

Nemzetközi morzekód

1. Egy pont és két vonal jelölés az A betűre.
2. A két vonal jelölés a B betűre.
3. Egy pont és két vonal jelölés az X betűre.
4. Két vonal jelölés az O betűre.

A	• — —	U	• — —
B	— — • • •	V	• — — •
C	• — — • •	W	• — — • —
D	• — — • • •	X	• — — • — •
E	• — —	Y	• — — • — • —
F	• — — • • •	Z	• — — • — • — •
G	• — — •		
H	• — — • •		
I	• — —		
J	• — — • — • —		
K	• — — • • —	1	• — — • — • — • — • —
L	• — — • • •	2	• — — • — • — • — • — • —
M	• — — • —	3	• — — • — • — • — • — • — • —
N	• — — • • —	4	• — — • — • — • — • — • — • — • —
O	• — — • — • —	5	• — — • — • — • — • — • — • — • — • —
P	• — — • — • — •	6	• — — • — • — • — • — • — • — • — • — • —
Q	• — — • — • — • —	7	• — — • — • — • — • — • — • — • — • — • — • —
R	• — — • — • —	8	• — — • — • — • — • — • — • — • — • — • — • — • —
S	• — — • — • — • —	9	• — — • — • — • — • — • — • — • — • — • — • — • — • —
T	• — — • —	0	• — — • — • — • — • — • — • — • — • — • — • — • — • — • —

A nemzetközi morzekódok

A morzekód is felfogható titkosításnak, hiszen a betűket pontok és vonalak helyettesítik. Itt az adott eszköz (például távíró ki- vagy bekapcsolt állapota jelzi a betűt. Több titkosírási üzenetet így közvetítettek. Ilyen morzézással továbbított kód például az ADFGVX. A

morzekód segítségével (s betűvel) tesztelték a rádió működőképességét is, ami a kriptográfusoknak felváltva riadalmat és örömet okozott, hiszen a gyorsabban továbbított üzeneteket bárki lehallgathatja és nem megfelelő kódolás esetén meg is fejtheti. A kódnak többféle változata is létezik, Európában a nyelvtől függően is változhat.

A karám

A 18. században szabadkőművesek alkalmazták az egyszerű monoalfabétikus karám nevű kódot, aminél különböző ábrákat helyettesítettek be, attól függően, hogy mi határolta körül a betűt.

Kriptográfia az I. világháború alatt

Az első világháború kitörésével még előrehaladottabbá vált a kriptográfia. A háború alatt számos új eljárást is kidolgoztak, de ezek 19. századi már feltört kódok változatai, kombinációi voltak. Némelyik rövid időre bevált, de sokáig nem állt egyik sem ellen. A rejtjelfejtést megnehezítő legerősebb körülmény a sok üzenet volt.

ADFGVX

Az ADFGVX kód, a háború egyik legsikeresebb kódja egyszerre behelyettesítéses és keveréses. Az első lépésben egy 6*6-os táblázatba beírják az angol ábécé huszonhat betűjét és a tíz számjegyet. A kód megfejtéséhez ezt is ismerni kell. Ezután minden karakterre megkeresik a sort és oszlopot, majd ezt sor-oszlop sorrendben leírják (azaz például ha az a az F sor G oszlopában van, FG fogja helyettesíteni). Aztán egy kulcsszóval táblázatba írják a betűket, majd úgy rendezik a táblázatot, hogy a kulcsszó ábécérendbe kerüljön, azaz például ha KRIPTOGRAFIA volt, AAFGIKOPRRT lesz. Erre azért van szükség, hogy egy egyszerű gyakorlati elemzéssel ne legyen a kód megfejthető. Ezt morzekóddal továbbítják. Ezért is ADFGVX, hogy a félreütéseket elkerüljék.

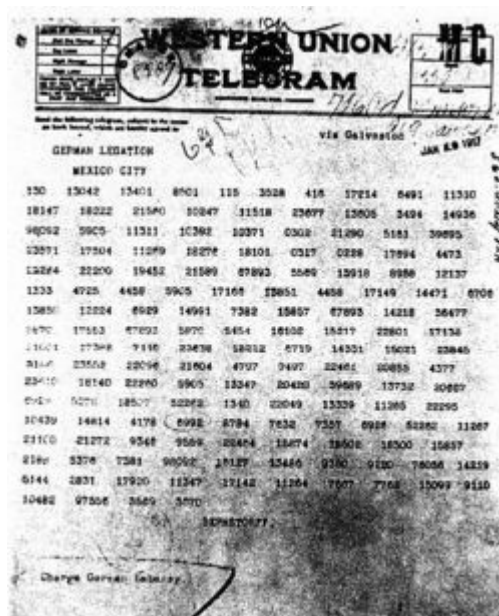
Feltörése

1918. június 1-én a Párizst támadó német tüzérség alig száz km-re volt a településtől. Ekkor már csak a kód feltörése volt a remény. A franciák között ott volt Georges Painvin is, aki május 2. éjjelén fejtett meg egy ADFGVX kódot, ami a következőt tartalmazta: *"Municiót haladéktalanul. Akár nappal is, ha nem látják."*

Az USA hadbalépése

Arthur Zimmermann a korlátlan tenger-

alattjáró háborút fontolgató Németországban azon munkálkodott, hogy Mexikó délről, Japán pedig keletről támadja az USA-t, ezáltal ellehetetlenítve annak hadbalépését. Emiatt január 16-án táviratot küldött Németország washingtoni nagykövetének. A Svédországon át küldött táviratot elfogták és a 40-es irodába, az Admirális rejtjelfejtő irodájába küldték. A kódot Montgomery tiszteletes és Nigel de Grey kezdte el megfejteni. Néhány óra alatt pár szövegtöredéket meg is találtak, amiről látszott, hogy fontos anyag, így folytatták a megfejtést. Csak részben sikerült. Az amerikaiaknak nem akarták átadni a nem teljesen megfejtett táviratot, hiszen ekkor az amerikaiak nyilvánosan kritizálják a németeket, így új, erősebb kódot készítenek. Február 1-jén elkezdődött a korlátlan tengeralattjáró-hadjárat, de két nap múlva Woodrow Wilson bejelentette, hogy semleges marad. Eközben a kódot megfejtették, de hogy ne sejtsek meg a németek kódjuk gyengeségét, kapcsolatba léptek a mexikói brit ügynök Mr. H.-val. Elloptak egy kódolatlan változatot és ezt adták át. Emellett az angol hírszerzőket nyilvánosan kritikusan illették. A kódot több amerikai így is koholmányának hitte, de Zimmermann kijelentette: *"Nem tagadhatom. Igaz."*



Zimmermann távirata

A Vigenère-kód újabb javítása

A Vigenère-kódot a háború alatti, 1918-as újabb javításaival próbálkoztak a rejtjelezők komoly előnybe kerülni a rejtjelfejtőkkel szemben. A véletlenszerű kulcs fogalmát Joseph Mauborgne amerikai őrnagy vezette be. A kulcs így nem a meg-

fejthető értelmes szavakból, hanem értelmetlen betűfüzérekből (például MQWBZTXSAUAA) állnak. Vélekedése az volt, hogy a hírközlés biztonságát soha nem látott szintre emelik. A kódban jelentős szerepet játszik, hogy minden kulcs megegyezik a kódszöveg hosszával és csak egyszer használnak egy-egy kulcsot, a felhasználása után pedig megsemmisítik, ezáltal sehol nem lesz támpontot adó ismétlődés. Emiatt is nevezik *egyszeri kulcsos módszereknek*.

Még ha végig is lehetne próbálni az összes esetet - bár ez mind az ember, mind a gép képességét jelen pillanatban meghaladja, az összes adott hosszúságú karakterlánc is kijönne, így a „véddindiát” és a „támadjmost” is kijöhetne. A kódolásról matematikailag bebizonyítható, hogy megfejthetetlen. A kódban hátrány az, hogy a véletlen kulcsok előállítása napi akár több milliós mennyiségű betűnél szinte lehetetlen. A kriptográfusok úgy gondolták, hogy az írógép billentyűinek véletlenszerű lenyomásával előállítható kód jó, de rászoktak arra, hogy felváltva a bal, majd jobb oldalon üssenek le billentyűt. Ezeknek van struktúrájuk, így nem véletlenek. A "legjobb" kódokat olyan fizikai folyamatok segítségével hozzák létre, mint a radioaktivitás. Ekkor a Geigerszámlálót az asztalra teszik egy radioaktív anyaggal és ez alapján készül a kulcs. A kóddal akadt még egy probléma: a szétosztás. Hiszen a nagy mennyiségű kódokat nem lehet egyesével szétosztani, ehhez nagyobb adagok kellenek kódkönyvekben. Ekkor viszont, ha az ellenség megszerzi ezt, könnyen megfejtheti az összes üzenetet. Az újrafelhasználása a kódoknak hasonlóan veszélyes. Emiatt a módszer nem leegyszerűsíthető, így a gyakorlatban ritkán alkalmazzák.

Kódfejtést elősegítő stratégiák a háború alatt

Mivel rögtön egy-egy új eljárás nem volt megfejthető, egyéb stratégiákat dolgoztak ki, például a franciák hat iránykereső állomást telepítettek, ami ha az üzenetről nem is adott információt, de egy-egy csapat helyéről igen.

Kriptográfia a II. világháború alatt

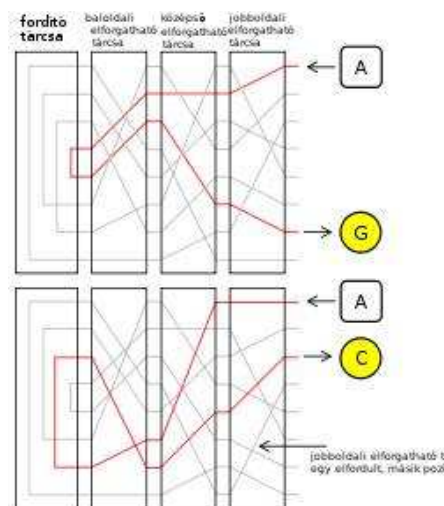
A villámháború a gyorsaságon alapult. A csapatok irányítása, kapcsolattartás csak rádióval volt lehetséges. Ezeket természetesen lehallgatták az ellenséges csapatok is. Követelmény volt az üzenetek megbízható kódolása. Megkezdődött a titkosító gépek tömeges alkalmazása. Ezek leghíresebb példája II. világháborúban a németek által alkalmazott *Enigma*, az e géppel előállított kódot a németek megfejthet-

lennek tartották. Ez a vélekedés tévesnek bizonyult, noha a kódot az angolok valóban nem csak matematikai, hanem a kezelési hibákat kihasználva, illetve titkoszolgálati módszereket is alkalmazva törték fel (az ellenségtől zsákmányolt készülék, kódkönyvek ismeretében). A világháború és hidegháború valósággal gondolat-háborút jelentett a harcoló felek titkosítás-foglalkozó szakemberei között is, és óriási lendületet adott a matematika és az informatika fejlődésének.

Enigma

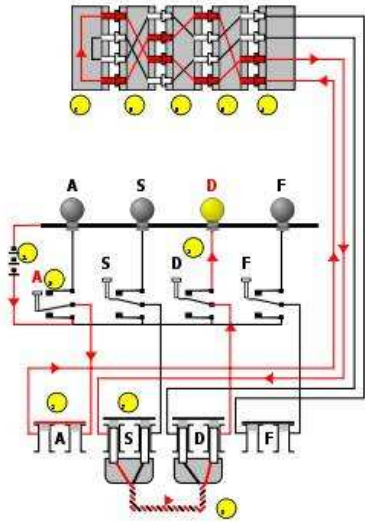


Az Enigma katonai, háromtárcsás változata



Az Enigma tárcsák kódolása két egymást követő betűnél. Az áram átfolyik az egymás után kapcsolt tárcsákon, megfordul a fordítóban, és újra átfolyik a tárcsákon. Szürke vonalak jelzik a tárcsákon belüli egyéb útvonalakat. Az A betű két egymást követő leütésnél más és más betűt ad – itt a példában először G-t, utána pedig C-t. Ez azért van, mert a két leütés között a jobb oldali tárcsa egyet elfordult, és az áram már teljesen más utat jár be. Több

leütés után a többi tárcsa is előbb-utóbb elfordul.



Az Enigmában folyó áram útját mutató ábrán az látszik, hogy az A gomb lenyomásával kigyullad a D lámpa. A D-ből ugyanígy lesz A, de az A-ból soha sem lesz megint A. Ez volt az Enigma-kód egyik nagy nehézsége, ám ugyanezt lehetett kihasználni a kód feltöréséhez is.



A Bletchley Park, ahol az üzeneteket megfejtették

Az Enigma elődjének az olyan kódtárcsás gépek tekinthetők, mint amiket Leon Alberti itáliai építész hozott létre a 15. században. Az Alberti által készített kódtárcsa még csak Caesar eltolásos módszerét használta. Az Enigmát Albert Scherbius alkotta meg az első világháború végén. A gép fő egységei a beviteli célokat szolgáló billentyűzet, a nyílt szöveg betűit sifírozó keverőegység és a kódszöveget lámpák felvillanásával jelölő kijelző volt. A keverőben a sok vezetékkel rendelkező vas-tag gumitárcsa az egyik fontos rész.

Az angol ábécében 27. alkalommal ismétlődni kezd a kulcs. Két keverőnél a második csak akkor fordul el, ha az első megtett egy teljes kört, ez már 676-féle kulcsot jelent az angol ábécé esetében. Az Enigmán három ilyen kódtárcsa volt, 17 576-féle kódtáblázatot biztosítva. Emellett volt egy visszairányító, ami a kódábécék számát nem növeli, így fölöslegesnek tűnik, de a használati mód miatt nem az. A keverőtár-

csák elfordulása miatt elég naponta egy kulcs. Az elküldött kódolt üzenetet a címzett begépel, a megfelelő tárcsabeállítások ismerete esetén megkapja a megfejtést. A találmány biztonságát növelve cserélhető és felcserélhető keverőtárcsákat alkalmazott Scherbius - hiszen a 17 576 lehetséges üzenet megfejtésére akár csak tíztizenkét embert "ráállítva" alig egy nap elég. A három tárcsának hatféle elrendezése van, azaz a biztonság hatszorosára nő. Emellett kapcsolótáblát is elhelyezett, ami felcserél bizonyos betűket. Ráadásul található benne egy kódolást csak némiképp befolyásoló gyűrű. A gép ára igen magas volt, mai áron körülbelül harmincöt-ezer dollár. Három másik feltaláló, Alexander Koch Hollandiában, Arvid Damm Svédországban és Edward Hebern az Amerikai Egyesült Államokban nyújtott be szabadalmat hasonló eszközökre. A németek első világháborús kriptográfiai hibáikból tanultva úgy érezték, hogy az Enigma a legbiztonságosabb megoldás.

Megfejtése

Az első jelentős lépéseket az Enigmával kódolt üzenetek megfejtésére a lengyelek tették, amikor az amerikaiak és a franciák már lemondtak róla. Az itteni munkát Maksymilian Cieccki irányította. A megfejtéshez vezető úton egy a hazájától elfordult német Hans-Thilo Schmidt tette az első lépést, aki az Enigma huzalozásának kikövetkeztetésére alkalmas fotokópiákat adott át a francia kriptográfusoknak, akik a lengyeleknek átadták ezek másolatát. A német rendszerben volt még egy nehéztés: egy fő kulcsot használtak a napi kulcs kódolására. Ekkor a rendszer tudományos alapja miatt a Biuro Szyfrów matematikusokat kezdett alkalmazni. A megfejtésben közülük a legnagyobb szerepet Marian Rejewski tette. A németek a kulcsot a rádiointerferencia kiküszöbölésére egymás után kétszer is leírták. A kulcsból így Rejewski megfelelő számú üzenet esetén egy első betű-negyedik betű (a kettő ugyanolyan) táblázatot készített. Ezek után a betűkből létrejövő láncokat vizsgálta. A hossz csak a keverőtárcsák sorrendjétől és beállításától függ. Ebből 105 456 kulcs állítható elő. Az egyes beállításoknál a kulcs-hosszt egy év alatt megvizsgálta és katalogizálta. A kapcsolótábla meghatározásához a következő műveletet végezte el: az Enigma-másolatán a kapcsolótáblát kiiktatta és a többi szöveget nézte csak. Az üzeneteket begépelve értelmeshez hasonlító szókapcsolatok jöttek ki, például alliveinbelrin, azaz vélhetően arrive in Berlin. Ez alapján megállapította, hogy mik lehetnek ezek a felcserélések. Innen készített egy gépesített katalógust, "bombát", ami meggyorsít

totta a folyamatot. 1938-ban a németek biztonsági intézkedései miatt öt keverőtárcsából lehetett hármát, négyet vagy ötöt választani. A nehezebb kódra már nem volt elég pénzük a lengyeleknek, a britekhez szállították a bombákat és az Enigma-másolatokat.

Angliában a Bletchley Parkban megalapított Government Code and Cypher Schoolba (Állami Rejtjelező és Rejtjelfejtő Iskola, GC&CS) vitték az Enigmát. A lengyel módszerek segítségével előre tudtak hírt adni az angliai bombatámadásokról. Ezek után egyre több módszert találtak a gyorsításra. Például sietség miatt gyakran használtak olyan kulcsot, mint QWE vagy BNM. Egy másik használati gyengeség, hogy nem hagytak egy keverőtárcsát sem két napig a helyén, ami jelentősen csökkentette az esetek számát. Emellett tilos volt a kapcsolótáblán két szomszédos betűt felcserélni. Az Enigmát folyamatosan továbbfejlesztették, de a britek lépést tudtak tartani. Az egyik jelentős személy Alan Turing volt. Az üzenetek elején kódolt kulcs hibája volt a duplázás, az ő feladata volt az egyéb hibák keresése. Ilyenek voltak például a megszozott időpontok, például egy este hat után nem sokkal küldött üzenet nagy valószínűséggel tartalmazta az időjárás szót. A Rejewski-féle betűláncokat is támpontnak tekintette. Az egymás utáni lépéseknél három összekötött gépet képzelt el. A kapcsolótáblákat kiiktatta. Ilyen módszerekkel száznál is több Enigmával és egyenként 17 576 beállítással desifriroztak. 1940-ben azonban a németek megváltoztatták a kulcsforgatási eljárásukat. Augusztus 8-ig nem tudtak a problémával szembeszállni, de később sikerült. Egy másik megoldási segítség az volt, hogy az Enigma nem tudott önmagával kódolni egy betűt. A Kriegsmarine Enigmája viszont nyolcféle keverőtárcsával rendelkezett, és a visszairányító huszonhatféleképp volt rögzíthető. Rajtaütések révén kódkönyvek megszerzése is segített az angolokon. A Bletchley Park emellett az olasz és japán üzeneteket is desifrirozta. A munkásságukról viszont a titoktartás miatt csak az 1970-es évek végén értesülhetett mindenki.

Egyéb eszközök

Az Enigmán kívül egyéb eszközök is voltak, például a japán Purple, amit az amerikaiak megfejtettek és ezzel jelentős előnyre tettek szert. Mindkettőnél a használatának módjából fakadó sebezhetőségeket használták ki. A britek egy Typex (más néven Type X) nevű eszközt használtak a rejtjelezésre, az amerikai katonasága a SIGABA (M-143-C) nevű eszközzel kódolt. A Lorenz-kóddal, a Lorenz SZ40 típusú gépek segítségével kódolták Adolf Hitler üzeneteit. A "bombák"

csak egyféle műveletre voltak alkalmasak, ez a kód pedig bonyolultabb volt, így emberi elmére és hetekre volt szükség a megfejtéséhez. Ekkor az egyik bletchley-i, Max Newman egy több különböző művelet végrehajtására képes gépet tervezett, amit ma *programozható számítógépnek* neveznek. A tervet lehetetlennek tartották, de az egyik ottani mérnök, Tommy Flowers tíz hónap alatt megépítette és kivitelezte azt, Colossus néven. Mint minden ottani eszközt, a Colossust is megsemmisítették a háború után.

A navahók

*„Nemhogyan megfejteni nem tudtuk,
de még leírni sem.” - tengerészeti
hírszerzés*

A SIGABA-nak volt egy jelentős hátránya, mégpedig az, hogy az olyan heves csatákban, mint amik a Csendes-óceánon zajlottak, nincs idő kétszer gépelni és kódolni, dekódolni. Egy haditudósító erről mondta a következőt: *"Ilyen esetekben az angol nyelv az utolsó mentsvár. Minél nyersebb, annál jobb."* Ezzel volt egy probléma, mégpedig, hogy sok japán tanult az Egyesült Államokban, folyékonyan beszéltek az angolt, a káromkodást is. Erre találta ki egy Philip Johnston nevű mérnök azt, hogy a navahó indiánok nyelvével kommunikáljanak. A négy legnagyobb törzs jött szóba, mert ott beszélnek a legtöbben angolul: a navahó mellett a sziú, a csipeva és a pimapago. A navahóknál volt a legkevesebb írástudó, őket választották.

A nyelv nem volt felkészülve a repülőgépek, hajók, hadászati kifejezések használatára, így lett például a csatahajó szóból bálna. Az ábécé betűit a szó angol kezdőbetűje alapján fordították navahóra (például az O-nál az owl (bagoly) szó navahó változatát készítették el). Egy probléma volt, hogy a navahókat és a nyelveket japánnak nézték azok a nem navahó katonák, akik nem tudtak az új "kódról". Az ábécét később bővíteni kellett, hogy ne legyen feltűnő, a leggyakoribb hat betűhöz két-két, a második leggyakoribb hathoz egy-egy új szó került. A szavak is 234 szóval bővültek.

Következik a

MODERN KRIPTOGRÁFIA