Vinko Vodopivec

TAJNOST ZAPISOVANJA IN NJEGOVO RAZKRIVANJE

Abstract

SECRET OF WRITING AND ITS DECIPHERING

At all times the writings were tried to be protected by secret coding or ciphering. In the mean time the opponents were trying to desipher or decode thier meaning of the content. A similar methods of deciphering are also suitable in reading of ancient inscriptions with letters, syllables or pictures with known and unknown values of single signs. Such methods are also applicable in the transliteration and deciphering of ancient inscriptions. In particular their understanding is based on Slavic (Venetic, Slovenian) language. The secret writings and their deciphering were especially important in the war times, and particularly in the 1st and 2nd World War. Without present day secret writings and methods in banking the modern money market tarnsfers would not be possible.

Uvod

V vseh časih so ljudje odkrivali nove in uporabne stvari: orodja in orožja, načine shranjevanja živil in načine priprave hrane, raznovrstnost rastlinske in živalske hrane, obleko in obutev, posodo za jed in shranjevanje ter vodna, jezdna, vlečna in kolesna transportna sredstva. Udomačili so živali za mlečno in mesno prehrano, za volno, za obutev in obleko iz kožuhov in golega usnja, pa tudi za ježo, boj, delo itd. Vsa tako pridobljena znanja so predstavljala pomembno prednost pred drugimi skupinami, zato so znanja predstavljala varovane rodovne skrivnosti, ki pa so prej ali slej postale last tudi drugih sosednjih plemenskih in rodovnih skupin. Navedene prednosti so omogočale hitrejšo rast plemenskih skupin ali celo nadvlado sosednjih plemen. V vseh časih se je pojavljala tudi magija in s tem v zvezi tudi tajnost sporočil, ki so se ustno prenašala iz roda v rod in so pomembno vplivala na oblikovanje družbenih elit, včasih v dobrem, velikokrat pa tudi v slabem pogledu.

Ob izumih zapisovanja pa so bile skrivnosti lahko tudi zapisane in so bile zato skrbno varovane, predvsem pa so bila narisana ali napisana znamenja znana le ožji elitni skupini. Vendar so kljub skrbnemu in ustreznemu varovanju lahko prišla v roke tudi drugim, zato so v vseh časih pismenosti izumljali postopke, kako bi prikrili zapisano vsebino. Tako prikrivanje napisane vsebine imenujemo tajnopis ali šifriranje, odkrivanje njegove vsebine pa razbiranje ali dešifriranje. Z ustanovitvijo večjih skupin kot so države in kraljestva, se je zaradi dobrega poslovanja države povečalo število nujnih sporočil, in nekatera upravna in zlasti vojaška sporočila so bila zelo pomembna in niso smela s pravo vsebino

priti v sovražne roke. Zato so oblasti uvedle tajne službe, ki so šifrirala poročila za varno prenašanje njihovih pomembnih vsebin. Hkrati s tem pa so nasprotniki iskali načine, kako bi se dokopali do pravih sporočil in so iskali poti, da bi dobili šifrante ali pa so celo sami poskušali najti ustrezno pot do njihovega razumevanja. Tako sta se dopolnjevali dve povezani veji: vohunstvo in razbiranje. Vsaka šifra ima določene lastnosti, ki se opazijo pri razbiranju in po večkratnih poskusih dobijo smiselno vsebino, ki pomaga odkriti zapisano besedilo. S tem je tajna pisava odkrita in zato neuporabna. Tako se je vedno bila bitka med tajnopisjem in razkrivanjem: tajnopisje z novimi postopki zapleta odkrivanje, razkrivanje pa uporablja vedno zahtevnejše analize. Ta boj se je nadaljeval skozi vso zgodovino in je pomembno vplival na odnose med posameznimi centri moči in njihovimi bitkami in je bistveno odločal o zmagi in porazu nasprotujočih si sil. V času svetovnih vojn pa je ta boj zajel celoten svet in z množico različnih tajnopisov in množico štabov za razbiranje odločilno vplival na hitrejši in uspešnejši zaključek vojn. V sedanjem času globalizacije pa brez zanesljivega tajnopisa ni mogoče niti politično, niti gospodarsko poslovanje, saj se že večina storitev opravlja preko spletnega trgovanja.

Opozorilo

Zapis je izvleček iz knjige [1]: Simon Singh, *Knjiga šifer, Umetnost šifriranja od starega Egipta do kvantne kriptografije*, prevedel J. Plešej, Učila International, Tržič **2006**.

Tajnopisje

Najstarejši tajnopis

Najstarejši znani tajnopis opisuje Herodot, ki je bil kronist o bojih med Grčijo in Perzijo v 5. stol. pr. Kr., saj naj bi tajnopis rešil Grke pred osvojitvijo perzijskega kralja Kserksa. Ta se je pripravljal, da si podredi tudi neposlušno Grčijo in je 5 let zbiral največjo vojsko v dotedanji zgodovini. To je opazil neki Grk v izgnanstvu, ki je pisno opozoril Šparto pred invazijo, ker pa je bil na tujem ozemlju si je pomagal z zvijačo. S pisalne deščice je postrgal vosek in nanjo napisal besedilo in preko njega zopet vlil vosek in tako prekril besedilo. Deščica je prišla v prave roke, toda niso razumeli njenega pomena, dokler ni žena vodje svetovala naj odstranijo vosek, in tako so prebrali sporočilo in ga poslali še drugim Grkom. Začeli so se pripravljati na boj in zgradili 200 bojnih ladij. Tako je Kserks izgubil odločilno prednost presenečenja. Ko je leta 480 pr. Kr. napadel Grke, so perzijsko številčnejše ladjevje z begom zvabili v ozek zaliv, kjer so bile njihove manjše ladje učinkovitejše kot večje perzijske ladje, in so ponižujoče premagali Perzijce.

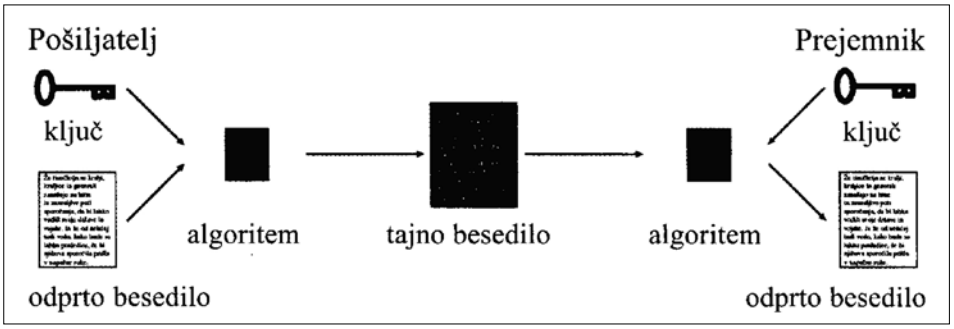
Skrito sporočilo

Najstarejši tajnopis je bil načini skritega sporočila, ki se pojavlja v raznovrstnih oblikah. Kitajci so sporočilo napisali na svilo, jo stisnili v kroglico in jo potopili v vosek. Tako pripravljeno kroglico je sel pogoltnil, in tako varno prenesel sporočilo. Če na trdo kuhano jajce pišemo z galunom, ta skozi porozno jajčno lupino prodre do beljaka in na njem pusti sporočilo, ki ga lahko preberemo le če jajcu odstranimo lupino. Že v 1. stol. pr.

Kr. so poznali nevidno črnilo, ki s sušenjem postane prozorno in se ob segrevanju obarva rumeno. Še celo v 20. stoletju so vohuni uporabljali lasten urin, če jim je zmanjkalo nevidnega črnila. V drugi svetovni vojni so nemški vohuni v Južni Ameriki uporabljati mikrotočko: sporočilo so pomanjšali v velikost pike in ga tako poslali v nedolžnem pismu. Američani so to odkrili šele po namigu, naj v pismih pregledajo bleščeče pike, ki so nastale zaradi gladkega fotografskega papirja. Ti postopki skrivanja nudijo določeno varnost, vendar so predvidljivi in dobra kontrola jih z lahkoto odkrije, potem pa je vsebina takoj znana.

Tajnopis

Naslednja stopnja je tajnopis, ki za nasprotnika nima nobene vrednosti tudi če ga prestreže, če ne pozna ključa za njegovo razbiranje. Način postopka in uporabe je viden na



Slika 1: Postopek tajnopisja in branja

naslednji sliki 1. Odprto besedilo in ključ omogočata po postopku določenem s ključem izdelavo tajnega besedila in po obratnem postopku njegovo branje. Uporabljala sta se predvsem dva postopka: prestavitev in zamenjava.

Prestavitev

Prestavitev je tajnopis, kjer črka ohrani svojo vrednost, spremeni pa svoje mesto. To je v bistvu premetanka – anagram čigar rešitev raste potenčno s številom črk zapisa, zato je daljši anagram praktično nerešljiv, vendar je nerešljiv tudi za prejemnika. Zato mora biti urejen po nekakšnem pravilu in to omogoča uporabniku hitro branje, nasprotniku pa osnovo za ugotovitev ključa za razbiranje. Uporabne so tudi enojne ali večkratne »vrtne ograje«, kar je razvidno iz naslednjega primera dvojne in trojne »ograje«:

NA VRTU SKRIT	N R S I
N V T S R T	A T K T
A R U K I	V U R
NVTRSRTARUKI	NRSIATKTVUR

Podoben sistem je uporaba rovaša (palica za označbe) iz 5. stol. pr. Kr., ko so Špartanci tanek trak ovili okoli palice in po dolgem pisali po traku na palici. Potem so trak odvili in na posameznem mestu so bili največ zlogi, ki niso nič pomenili. Šele če se je trak navil na palico enake debeline, se je pojavil pravi napis.

Zamenjava

Zamenjava je tajnopis, kjer črka ohrani svoje mesto, spremeni pa svojo vrednost. Gre za nadomestitev posamezne črke z drugo črko, številko ali simbolom. Najenostavnejše so zamenjave s črkami, ki so enako oddaljene po znani abecedi na primer za eno ali več mest: Pri premiku za eno črko namesto ABCD dobimo BCDE, CDEF, DEFG itd. Najstarejša znana zamenjava je iz 4. stol pr. Kr. v Kamasutri, kjer se poljubno določi par črk ki se zamenjuje. To je ključ, ki ga morata uporabljati tako pošiljatelj kot sprejemnik. Cezar, ki je veliko uporabljal premik za tri črke, ki se po njem imenuje Cezarjanka, je neko sporočilo napisal v grški abecedi in zato je bilo za galskega nasprotnika nerazumljivo. Sistem je torej enostaven, besedilo spremenjeno po ključu se prenese prejemniku, ki ga po znanem ključu lahko prebere.

Kodiranje

Naslednja stopnja je kodiranje, kjer določena črka ali znak predstavlja besedo. Tak sistem je možno razbrati šele z dovolj velikim številom zapisov, zato je zelo varen. Sistem pa ima vendar veliko pomanjkljivost, saj je treba sestaviti debelo knjigo izrazov, ki lahko pride nasprotniku v roke in skrivna poročila so takoj znana.

Razbiranje

Razbiranje tajnopisa je odvisno od dolžine zapisa, saj se ponavljajo podobni pojavi, ki omogočajo različne analize. Razbiranje je bistveno odvisno od zahtevnosti izbranega ključa in v nekaterih primerih brez znanega ključa ni možno.

Velik napredek so naredili Arabci, ki so v Bagdadu ustanovili Hišo modrosti, knjižnico in prevajalski center. S tajno pisavo so zaščitili mnoge dejavnosti, pomemben premik pa so naredili tudi pri razvrščanju besedil preroka Mohameda. Preverjali so zgradbo zapisov in ugotavljali ali jih je napisal sam prerok ali so jih napisali drugi. Prav tako so po starosti posameznih besed časovno razvrstili posamezne zapise. Odkrili pa so tudi različno pojavljanje posameznih črk in tako postavili temelj razbiranja tajnopisja. Pomembne pa niso le posamezne pogoste ali redke črke, ampak tudi pogosti ali redki dvojčki. V 19. stoletju je arabski »filozof« Al Kindi napisal knjigo o razbiranju tajnih pisav na osnovi frekvenčne analize najpogostejših črk in drugih jezikovnih značilnosti.

Primer pogostosti pojavljanja posameznih črk v angleščini in slovenščini je v % prikazan v naslednji tabeli 1:

Tabela 1a: Pogostost črk v angleščini v %.

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**
8,2	1,5	2,8	4,3	12,7	2,2	2,0	6,1	7,0	0,2	0,8	4,0	2,4	6,7	7,5	1,9	0,1	6,0	6,3	9,1	2,8	1,0	2,4	0,2	4,0	2,4

Tabela 1b: Pogostost črk v slovenščini v %.

A	**B**	**C**	**Č**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**R**	**S**	**Š**	**T**	**U**	**V**	**Z**	**Ž**
10,9	2,1	0,7	1,6	3,4	10,8	0,1	1,6	1,2	9,3	4,6	3,9	5,0	2,9	6,3	9,1	3,1	5,1	4,9	1,1	4,7	1,6	3,3	2,1	0,9

Poleg značilnih črk v angleščini Q, W, X in Y in v slovenščini Č, Š in Ž so značilne tudi razlike pri deležih posameznih črk, zato je taka analiza pomembna pri ugotavljanju povezanosti neznanega zapisa z znanimi jeziki. Značilne razlike v podani tabeli med angleščino in slovenščino so pri črkah: C – 4 krat, F – 22 krat, H – 2 krat, J – 23 krat, K – 6 krat in T – 2 krat.

Analiza pogostosti

Analiza pogostosti ali frekvenčna analiza se prične z ugotovitvijo jezika zapisa in z značilno pogostostjo najpogostejših in najredkejših črk. Velika pogostost predstavlja samoglasnike, majhna pa soglasnike, pri zelo majhnih deležih pa že lahko sklepamo na posamezne zelo redke črke: v angleščini J, K, Q in X, v slovenščini pa C, F, Š in Ž. Tako dobimo možen izbor črk, ki ga nadgradimo z veliko in zelo majhno pogostostjo dvojčkov in že se izluščijo najverjetnejši glasovi za posamezne črkovne znake. Na tej osnovi je možno že ugotoviti posamezne besede, zlasti če vsaj približno poznamo vsebino sporočila. Značilne so na primer vremenske napovedi za posamezna bojišča, kjer se morda celo vsakodnevno pojavljajo besede: vreme, sončno, oblačno, padavine itd.

Nadgradnja zamenjave je vstavljanje mašil, ki predstavljajo težave za razbiranje, za naročnika pa ne, saj jih pozna, vendar so tudi taki napisi hitro rešljivi.

Enako zamenljiva

Naslednja stopnja tajnopisja je »enako zamenljiva«, kjer se črke, ki se pogosteje uporabljajo označujejo z več znaki ali števili. Tako se onemogoči enostavno analizo pogostosti in so potrebni bolj zapleteni postopki. Običajno se uporabi značilne dvojčke in sicer črke ki so zelo redke in njihovih bolj ali manj stalnih spremljevalcev. V angleščini sta to črki Q in U, ki sta vedno skupaj in imata pogostost Q 0,1 in U 2,8, torej gre za dvojček, ki ima drugo črko 28 krat pogostejšo kot prvo črko. V slovenščini pa so to črke s pogostostjo F 0,1, Š 1,1 in Ž 0,9, ki jim najverjetneje slede samoglasniki torej zopet najverjetnejše kombinacije dvojčkov z bistveno pogostejšo drugo črko.

Črne komore

Črne komore so bila posebna vohunska središča, ki so jih imele vse evropske sile, najbolj znana pa je bila na Dunaju. Ob 7 uri zjutraj so prispela v urad za razbiranje pisma veleposlaništev; tajniki so omehčali pečate, prepisali sporočila in jih ponovno zapečatili ter predali pošti, kopije tajnih pisem pa so šla v razbiranje. Tranzitna pisma pa so prispela v urad ob 10 dopoldne, bila deležna enakega postopka, ob štirih popoldne pa so nadaljevala svojo pot. Skupine dunajske črne komore za razbiranje so tedaj že strle vse navadne tajnopise, in so s svojimi delom nudile usluge tudi drugim evropskim centrom, na primer neposredno francoskemu kralju Ludoviku XV.

Več-abecedna zamenjava

Črne komore so razvrednotile klasične tajnopise in pošiljatelji so bili primorani poiskati močnejše orožje in uporabiti več-abecedno zamenjavo, ki je bila znana že davno

pred tem, vendar so se je izogibali, ker je predstavljala zahtevnejši postopek tajnopisja in branja. Za to je bil primeren Vigenèrov tajnopis, ki ga je objavil že leta 1586 z razpravo *Taicté des Ciffres*. V tistem času pa so kabineti za razbiranje raje uporabljali enostavnejše načine in njegov genialni izum odložili in sicer kar za 200 let. Vigenère je abecedo ponovil v naslednjih vrstah tolikokrat kot je bilo število črk abecede, vendar premaknjeno za eno mesto naprej, kar je dalo v angleščini možnost 26 različnih zamenjav črk sporočila z drugimi črkami. Treba se je bilo le dogovoriti za ključno besedo in potem po postopku določiti ustrezne vrstice za določitev pravega znaka. Ustrezne so bile tiste vrstice, ki na prvem mestu vsebujejo ravno črke dogovorjene besede. Z enostavno analizo pogostosti črk ni možno prodreti v tak tajnopis, saj ima ista črka več znakov, ki so pomešano tako, da posamezen znak lahko predstavlja pogosto ali redko črko. Pri daljših ključnih besedah je ta pomešanost dovolj velika.

Razvozlanje Vigenèrovega tajnopisa

Charles Babbage je bil vsestranski znanstvenik z mnogimi izumi, njegov največji izum pa je bil računski stoj z več kot 25.000 deli, ki bi omogočal tudi komplicirane račune, saj je vseboval spomin, mlin in odločitve, podobno kot sodobni računalniki spomin, procesor in zanke. Žal stroj ni bil izdelan, bi se ga pa dalo ustrezno programirati. Šele sto let kasneje so prve elektronske naprave uresničile njegove zamisli. Njegovo genialno delo na področju tajnopisja pa je razbiranje Vigenèrovega tajnopisa. Tudi v tem primeru se ponovijo skupine črk, kar je odvisno od dolžine izbrane besede - ključa, ki določa vrstice za tajnopisje. Če vzamemo besedo dolgo 20 črk je ponovitev samo enkrat in če ta vmesni prostor pregledamo tudi z drugimi ponovitvami lahko ugotovimo, da se pri določenem številu pojavijo vse ponovitve. Zato je to število enako številu črk izbrane ključne besede. Na tej osnovi se že lahko vrši analiza pogostosti, ki pa obsega vse črke in iz značilnosti poteka vseh vrednosti lahko sklepamo na značilno zaporedje črk. Opazni so skupni vrhovi in daljše doline, ki so značilne za vsako abecedo, tak značilni vrh in dolina je v slovenščini EFGH. Če graf premaknemo tako, da se sklada z normalno porazdelitvijo ugotovimo vrednost do sedaj predpostavljene črke, ki je v tem primeru E. Tako lahko že verjetno določimo prvo črko ključa, drugo črko pa določimo po istem postopku z že znano prvo črko. Če izid ni smiseln je treba postopek ponoviti z drugo najverjetnejšo prvo črko. Babbage tega odkritja ni objavil in so ga odkrili šele v 20 stoletju, ko so strokovnjaki pregledovali njegovo zapuščino. Isti postopek je samostojno odkril pruski častnik Kasiski, ki ga je objavil leta 1863 pod naslovom *Die Geheimschriften und die Dechiffrierkunst*, in se po njem imenuje Kasiskijev test.

Odkritje telegrafa in radia

Obe odkritji sta vzpodbudila številne poskuse tajnopisja, vendar brez večjega uspeha. Telegrafist je znano besedilo v svojem jeziku oddal večkrat hitreje in brez napake, pri šifriranem poročilu pa je šlo bistveno počasneje, kar je bilo precej dražje in možne so bile tudi usodne napake. Radijski promet teh možnosti ni imel, zato je bilo treba najti ustrezne vrste tajnega govora, kar bi omogočilo zaupnost javno poslanega sporočila in njegovo hitro

šifriranje in razbiranje. V prvi svetovni vojni so uporabljali kombinacije starih tajnopisov, vendar je bilo vedno le vprašanje časa, kdaj bodo novo šifriranje strli.

Nemški napad na Francijo

Le 16 dni pred napadom na Francijo dne 5. marca so Nemci uporabili kombinacijski tajnopis, ki naj bi jim omogočil popolno presenečenje ob napadu, ki je bil 21. marca 1918. Francozi so imeli tedaj najboljšo službo za razbiranja tajnopisja, saj so se po bolečem porazu leta 1870, ko so Nemci priključili *Alzacijo* in *Loreno* dobro organizirali in imeli obsežno službo s številnimi strokovnjaki. Čas je bil kot vedno bistvena sestavina reševanja nove šifre in razbiranja sporočila. Novo šifro je rešil genialni Francoz G. Painvin, ki je podnevi in ponoči reševal uganko in jo je še pravočasno rešil, kar je omogočilo branje prestreženih sporočil. S postavitvijo več sprejemnih postaj so lahko določili tudi mesto oddajne postaje. Z vsebino poročil o nujnih pošiljkah orožja in z določitvijo mesta oddajanja radijskega sporočila so Francozi ugotovili mesto napada in po hudi 5 dnevni bitki zavrnili nemški napad, ki mu je manjkala bistvena sestavina presenečenja.

Neomejena podmorniška vojna

Razbiranje je tudi bistveno odločilo, da so se ZDA vključile v prvo svetovno vojno in s tem bistveno prevesile razmerje moči. Prvega dne prve svetovne vojne še ponoči je britanska ladja dvignila šop čez-atlantskih kablov in jih prerezala ter tako preprečila najvarnejšo povezavo. Novo imenovani nemški zunanji minister A. Zimmermann je zato poslal tajnopis po radijski zvezi v obliki 152 tri do pet mestnih števil. Telegram je bil poslan nemškemu veleposlaništvu v Washingtonu, ki ga je poslalo mehiškemu veleposlaništvu. Bistvo sporočila so Angleži razbrali še isti dan in ga posredovali vodji mornariške obveščevalne službe, ta pa ga je spravil v trezor, saj naj bi napovedani neomejeni podmorniški napadi v vsakem primeru potegnili ZDA v vojno. Besedilo sporočila:

Prvega februarja nameravamo začeti neomejeno podmorniško vojno. Poskušali bomo doseči, da bi Združene države kljub vsemu ostale nevtralne. V primeru, da se to ne bi posrečilo, predlagamo Mehiki zvezo na naslednji podlagi, Skupno vojskovanje. Skupna sklenitev miru. Bogata finančna podpora in strinjanje z naše strani, da dobi Mehika nazaj svoja izgubljena ozemlja v Texasu, Novi Mehiki in Arizoni. Podrobnejša določila prepuščamo vaši visokosti. Prosimo, da vse zgoraj omenjeno strogo zaupno sporočite predsedniku, takoj ko bo vse glede vojne z Združenimi državami odločeno, hkrati pa še dodate spodbudo, da bi Japonsko sam od sebe povabil k takojšnjemu pristopu ter posredoval med Japonsko in nami. Prosimo opozorite predsednika na to, da bo brezobzirna uporaba naših podmornic prinesla dobre možnosti, da bo Anglija v nekaj mesecih prisiljena k sklenitvi miru. Prosim za potrditev prejema, Zimmermann.

Ker je 1. februarja Nemčija začela neomejeno podmorniško vojno, je predsednik ZDA W. Wilson sklical 2. februarja sejo kabineta, 3. februarja pa na Kongresu razglasil, da želijo ZDA še naprej ostati nevtralne in kot posrednik miru. Angleški admiraliteti ni preostalo drugega kot seznanitev z vsebino telegrama in tako je 2. aprila 1917 predsednik W. Wilson na Kongresu razglasil: »Ugotavljam, da politika, ki jo v novejšem času vodi

nemška cesarska vlada, ni nič manj kot vojna proti vladi in ljudstvu Združenih držav. Razbrana brzojavka je uspela tam, kjer ni zadostovalo tri leta napornega diplomatskega dela. Zanimivo je, da so Angleži uporabili zvijačo, češ da je bila vsebina telegrama izdana, zato so po zvezah na mehiškem brzojavnem uradu dobili mehiško verzijo Zimmermannove brzojavke in jo objavili, tako da so Nemci skoraj dve desetletji živeli v prepričanju, da so njihove šifre nerešljive.

Šifrirne ploščice

Že v 15 stoletju je italijanski arhitekt L. Alberti vzel dve bakreni okrogli ploščici, manjšo položil na večjo in ju v sredini povezal z iglo. Na robu je napisal črke in z zasukom ploščice dobimo Cezarjev premik za eno ali več črk. Podobno ploščico so uporabljali tudi v ameriški državljanski vojni. Že njen izumitelj Alberti je predlagal več abecedno tajnopisje s ključno besedo in tako prišel do Vigenèrove metode. Ima pa ploščica to prednost, da je mehanska in omogoča hitrejše tajnopisje in branje.

Novejše šifrirna naprave

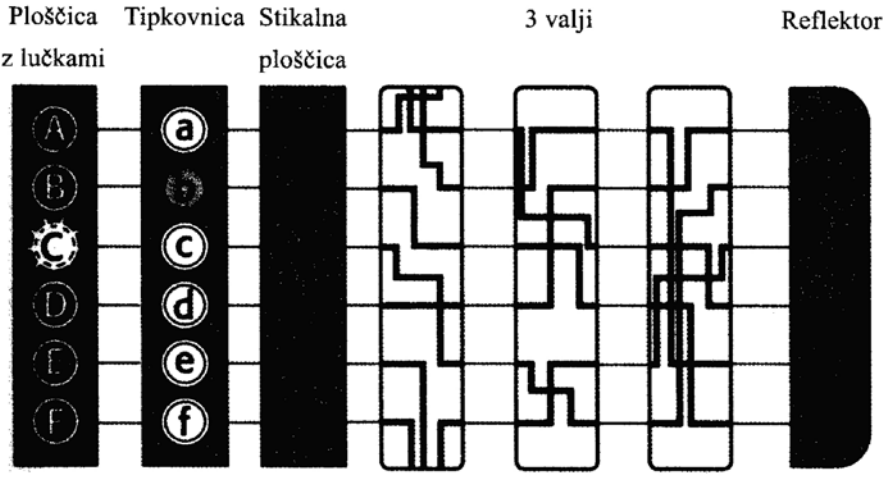
Šifrirni stroji – enigma – uganka

A. Scherbius je izumil elektromehanski šifrirni stroj, ki omogoča hitro šifriranje in hitro branje, zaradi raznovrstne kombinacije postopkov pa zagotavlja tudi izjemno veliko stopnjo zanesljivosti. Sestavljen je iz več delov, ki jih je sestavil v zelo zapleten šifrirni stroj: tipkovnica za vnos črk, šifrirna enota, ki črke spremeni v šifre in enota z lučkami, ki jih pokaže. Najpomembnejša enota je valj, ki je prepleten z žicami, vhod in izhod zanje pa je na šestih mestih, to pa je pomanjkljivost, saj se stanje ponovi po šestih prekinitvah. To so odpravili tako, da so uporabili dva valja, zato se stanje ponovi šele po 36 ponovitvah. Po vsaki črki se valj samodejno premakne za 1/26, to je za eno črko abecede, to pa je tudi pomanjkljivost, saj se stanje ponovi po 26 prekinitvah. To so odpravili tako, da so uporabili dva valja, ki so jima pozneje dodali še en valj in pri popolni abecedi je bilo že 26x26x26 = 17.576 kombinacij. Šifrer mora valje nastaviti na določen položaj, kar je v bistvu ključ, ki je veljal le tisti dan. To je pomenilo mesečno 30 ključev in razpošiljanje ključev vsem enotam, ki so imele enigmo. Šifriranje in branje sta obratna procesa, ki potekata samodejno ob enaki nastavitvi valjev. Knjiga ključev ne sme priti v nasprotnikove roke, sam šifrirni stroj pa je seveda prej ali slej dostopen tudi nasprotniku. Razbiranje bi tudi ob posedovanju enigme zahtevalo preizkus tudi do 17.576 različnih nastavitev. Valje so lahko tudi zamenjevali, kar je povečalo število možnosti še šest krat. Tudi stikalna plošča je imela šest povezav z valji, ki so jih lahko zamenjevali z vsemi črkami, kar je dalo skupno število kombinacij 10^{16}. Stroj je bil izjemen dosežek in majhen, saj je bil v kovčku velikosti 34x28x15 cm. Visoka cena 20.000 $ pa je odvrnila zainteresirane kupce. Podobne naprave so razvili tudi na Švedskem in v ZDA, vendar prav tako ni bilo zadostnega števila kupcev.

Scherbius pa je imel srečo, saj sta dve objavi iz prve svetovne vojne nedvoumno izdali, da so Angleži strli nemške tajnopise. Nemška vojska je takoj naročila obsežno raziskavo in ugotovila, da je enigma najboljša rešitev, ki so jo predelali za vojaško opremo. Zdelo se je, da

bo enigma odločilno prispevala k zmago nacionalsocializma, vendar je prispevala pomemben delež k njegovemu propadu. Po letu 1926 so angleški, ameriški in francoski oddelki za razbiranje poslušali radijska poročila, ki jih niso mogli razvozlati. Ker so jim bila poročila nerešljiva uganka so hitro odnehali, saj je bila Nemčija oslabljena in ni bilo politične volje za razbiranje teh poročil, zato je število usposobljenih ljudi za razbiranje hitro padalo. Poljska, ki je po prvi svetovni vojni postala samostojna, pa je bila med Sovjetsko zvezo, ki je širila svoj komunizem in Nemčijo, ki je hotela pridobiti nazaj ozemlja, ki jih je morala prepustiti Poljakom. Tako ukleščeni so bili Poljaki hvaležni za vsako informacijo in so na novo organizirali službo za razbiranje. Tudi oni so naleteli na tajnopis z enigmo in niso imeli nobene možnosti za njeno razkrivanje. Francozi so po izdaji dobili kopijo dokumentov: Navodila za uporabo šifrirnega stroja enigma in Navodila za uporabo ključev šifrirnega stroja enigma. Dokumenti niso vsebovali žičnih povezav, vendar dovolj podatkov, da so lahko sestavili kopijo enigme. Glede na izjemno število možnosti so bili prepričani, da je ni možno razrešiti, saj se jim je zdela nepremagljiva. Na srečo so imeli Francozi s Poljaki vojaški sporazum in so Poljakom izročili fotokopijo dokumentov in jim pustili nalogo naj strejo tudi to šifriranje. Osnovni prikaz enigme in njenega delovanja je prikazan na naslednji sliki 37:

Poljaki so se zagrizli v možnost, da mora obstajati bližnjica in pri velikem številu dnevnih poročil z istim ključem se pojavljajo ponovitve, ki pripeljejo do razvozlavanja. Zato so Nemci dodali še postopek, da so z dnevnim ključem posredovali nov sporočilni ključ za novo nastavitev valjev. Na prvi pogled je sistem neprebojen, toda Poljaki niso izgubili poguma. Na tečaj razbiranja so povabili 20 matematikov iz univerze v Poznanju,



Slika 37: Stikalna ploščica leži med tipkovnico in prvim valjem. S kabelsko povezavo je mogoče po dve črki zamenjati med seboj, v tem primeru **a** in **b**. Zdaj se **b** šifrira tako, da električni signal steče po poti, ki je bila prvotno namenjena za črko **a**. V pravi enigmi s 26 črkami ima uporabnik na voljo šest kablov, s katerimi lahko zamenja šest parov črk.

ki je prej pripadal Nemčiji, zato so vsi tekoče govorili nemško. Trije so pokazali poseben talent za razbiranje in so jih takoj zaposlili. Najbolj nadarjen je bil M. Rejewski, ki so mu predstavili enigmo.

Razbiranje enigme

Rejewski je delal popolnoma sam in je enigmo spoznal do najmanjše podrobnosti. Prav tako je vedel, da so ključ za rešitve v ponavljanjih in taka ponavljanja so bili individualni ključi, ki so bili na začetku vsakega sporočila. Te ključe sestavlja šest črk – dva enaka trojčka, ki v šifriranem besedilu dasta šest šifer. Prvi in četrti, drugi in peti ter tretji in šesti znak zanesljivo predstavljajo isto črko. Pri zadostnem številu poročil je dobil različne vzorce povezav in iz njih poiskal zaključene verige, ki so se začele in končale pri isti črki. Vzel je poljubno črko abecede in znak v spodnji vrsti, poiskal isti znak v gornji vrsti in znak pod njim in nadaljeval do zaključene verige, kot je prikazano.

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

Primer verig: A→F→W→A tri povezave

B→Q→Z→K→V→E→L→R→I→B devet povezav

Verige se vsak dan spreminjajo in črke se zamenjujejo, kar je posledica dnevnega ključa, vendar se število povezav ohrani in to je povezano z nastavitvijo valjev, ki se pri vsaki naslednji črki premaknejo za eno mesto naprej. Tu je sprejel pomembno ugotovitev: stikalna plošča in valji sicer vplivajo na natančno sestavo verig, vendar je ena lastnost odvisna izključno le od nastavitve valjev. Tako je uspel razdvojiti vpliv stikalne plošče in je njene povezave odstranil in dobil le vpliv valjev. Tako je neobvladljivo število kombinacij spustil na bistveno manjše število in sicer 105.456. Več ljudi je šele v celem letu pregledalo vse kombinacije in izdelalo katalog posameznih zaključenih dolžin verig za določeno črko. Rejewski je zdaj lahko začel razbirati enigmo. Ko je ugotovil značilnosti verig dnevnega ključa, je vedel za nastavitev valjev, vendar je bilo še bistveno preveč kombinacij glede na povezave s stikalno ploščo. Število kombinacij je bilo še vedno previsoko, vendar je bila na voljo poenostavitev. Odstranil je vse kable na stikalni plošči in prestreženi šifrant vnesel v enigmo. Večinoma je dobil nesmisle, včasih pa tudi zveze na primer: alkutlibernil – verjetno ankunft in berlin. Če je bila domneva pravilna je vedel da sta na stikalni plošči povezani črki R in L in z analizo nadaljnjih zaporedij je bilo možno odkriti še druge črke in s tem ustrezne povezave na stikalni plošči. Rejewski je imel sedaj prave povezave na stikalni plošči in nastavitev valjev in je lahko bral vsa poročila tistega dne.

Ko so Nemci nekoliko spremenili svoj postopek prenašanja sporočil, je Rejewski razvil mehanično verzijo, ki je samodejno poiskala nastavitev valjev. Zaradi šestih položajev valjev je moralo šest strojev Rejewskega delovati vzporedno, vsak v drugem možnem položaju. Skupna naprava je lahko našla dnevni ključ v približno dveh urah. Pravili so ji bomba, ker je tiktakala pri svojem delovanju. Zanimivo je, da je imel šef njihove službe ključe, ki jih je redno dobival iz istega vira kot opis enigme, vendar jih je imel v svojem

predalu, ker je vedel, da bo prišel čas, ko ključi ne bodo več na voljo in do takrat mora biti enigma odprta knjiga.

Leta 1938 so Nemci dodali še dva nova valja in za razbiranje bi rabil desetkrat toliko bomb, kar je predstavljalo 15 letnih proračunov njihovega biroja. Naslednji mesec pa so število kablov na stikalni plošči povečali iz 6 na 10, zato zdaj niso več zamenjali le 12 črk ampak 20. Poljska služba je bila leta 1938 na višku svoje moči, v letu 1939, ko so Nemci dopolnili enigmo, pa so bili brez velikih sredstev povsem brez možnosti. Zdaj bi jim njihov šef lahko prinesel ključe, ki jih je imel. Toda ključev ni bilo več, saj je bila dotedanja zveza prekinjena. Če Poljaki ne bi mogli streti tudi ojačane enigme, ne bi imeli nobenih možnosti, da bi ustavili nemški napad, ki je bil oddaljen le nekaj mesecev. Poljski major Langer je 30. junija svoje francoske in britanske kolege povabil v Varšavo, da bi se pogovorili o nujnih vprašanjih glede enigme. Longer jih je peljal v prostor, kjer je stala bomba Rejewskega in presenečeni Francozi in Britanci so ugotovili, da so bili Poljaki za desetletje pred njimi. Predal jim je tudi dva odvečna primerka enigme in načrte za bombe, ki bi strle tudi ojačano enigmo. Dne 1. septembra je nemška vojska vdrla na Poljsko in vojna se je začela.

Jeseni so Angleži že bili sposobni odkriti dnevni ključ in so potem lahko prebrali vsa ostala poročila. Iskali pa so tudi bližnjice: preobremenjeni šifrerji včasih niso izbrali treh naključnih črk, ampak kar tri sosednje, kar je dalo imenitno bližnjico. Valji niso smeli ostati na istem položaju, kar je za polovico zmanjšalo število možnosti. Podobno pravilo je bilo, da na stikalni plošči ne smejo povezati črke s črko pred njo ali za njo, kar je zopet zmanjšalo število različic. Bližal pa se je čas, ko bodo Nemci ugotovili, da s ponavljanjem dnevnega individualnega ključa bistveno zmanjšujejo njeno varnost. Problema se je lotil Turing, ki je bil odličen matematik in je pri ogledu množice poročil ugotovil določeno podobnost, če vemo za čas in kraj oddajanja. Značilno je bilo vremensko poročilo, ki so ga redno pošiljali malo po šesti uri, kjer so se pojavljale predvidljive besede na primer wetter – vreme. Torej je treba vnesti wetter v enigmo in moralo bi se pojaviti šifrirano besedilo, vendar je bilo število kombinacij mnogo preveliko. Zasnoval je kombinacijo treh strojev, ki so vedno obravnavali le en element šifriranja znotraj zanke, kljub temu pa je bilo število kombinacij nerešljivo. Tu je uporabil rešitev Rejewskega in ločil problem stikalne plošče in valjev. Z odstranitvijo stikalne plošče je bistveno zmanjšal število poskusov od $159x10^{18}$ na 17.576, to pa je bilo rešljivo že v petih urah. Vendar to še ni bilo dovolj saj pri napačnem začetnem položaju valjev žarnica ni zasvetila: teči bi moralo istočasno 60 trojnih enigem, da bi dobili ustrezen rezultat. Ko je bila znana prava nastavitev valjev, je bilo treba v enigmo vpisati besedilo in pregledati odprto besedilo. Če je bil rezultat tewwer, je bilo treba le zamenjati povezavo za w in t in iz vnosa drugega besedila so bile kmalu znane tudi druge povezave. Tudi te naprave so imenovali bombe, ki pa so bile 2 m dolge, 2 m visoke in 1 m široke, njihova zasnova pa je bila podobna zasnovi Rejewskega. Prototip so postavili 14. marca 1940, vendar je bil prepočasen, saj je naprava potrebovala en teden da je našla ključ. Minili so štirje meseci, ko je bil na voljo nov stroj. Medtem so Nemci v resnici izpustili ponavljanje in mrk razbiranja je trajal več mesecev. Čez leto in pol je delovalo že petnajst bomb in če je šlo po sreči, so ključ razbrali že v eni uri. Vendar je bila za razbiranje potrebna opora - »crib«, ki v angleščini pomeni leseno podporo v rovu,

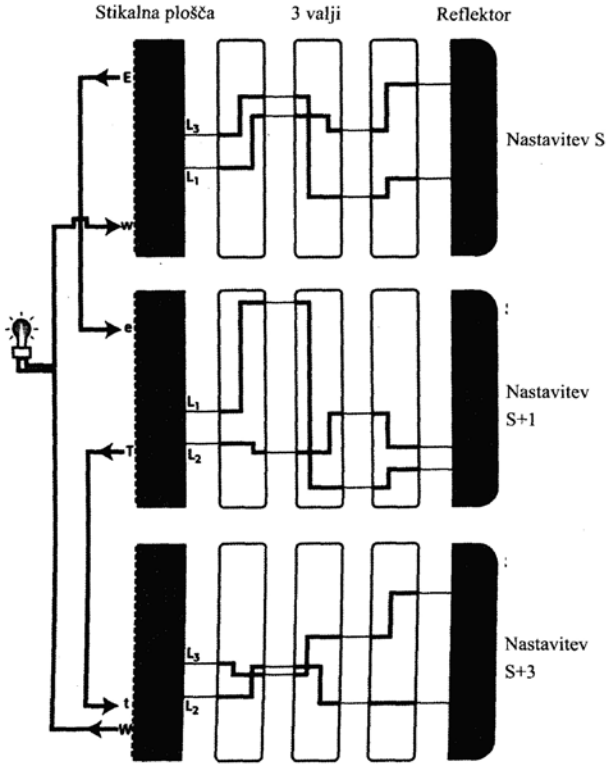
v tem primeru pa pomeni oporno točko, na kateri je mogoče graditi sistem razbiranja, ki je podobno tipanju v temnem rovu. Razbiralci so imeli več takih opornih točk, ki so ob ugodnem razpletu lahko skrajšale čas razbiranja. Predvidena delna rešitev pa je bila lahko na napačnem mestu in glede na pravilo, da ista črka ne more prestavljati sama sebe, je bilo treba to rešitev le premikati tako, da se nobena črka ni ponovila v obeh vrstah:

Domnevno besedilo			w	e	t	t	e	r	n	u	l	l	s	e	c	h	s			
Znani tajnopis	I	P	R	E	N	L	W	K	M	J	J	S	X	C	P	L	E	J	W	Q

V besedilu »crib« ni na pravem mestu saj sta črki e ena pod drugo! Če pa je »crib« na pravem mestu so ga lahko uporabili kot izhodišče za razbiranje s pomočjo bombe.

Na naslednji sliki 49 je prikaz ene trojice valjev, ki so ob ustrezni nastavitvi podali rešitev, ko je lučka zasvetila.

Šifre nemške mornarice pa so bile težavnejše, saj so imele 9 valjev, zato so si šifrante



Slika 49: Zanko *criba* lahko predstavimo z električnim integriranim vezjem. Trije stroji Enigma so nastavljeni identično, le da je pri drugem valj pomaknjen za en položaj (S+1), pri tretjem pa še za dva položaja (S+3) naprej. Izhod vsake enigme je povezan z vhodom naslednje. Tri kombinacije valjev se premikajo sinhrono, dokler ni električni krog sklenjen in lučka ne zasveti. S tem je najdena prava kombinacija. Na sliki je prehod ob pravi kombinaciji sklenjen.

preskrbeli z napadom na ladje, kjer so zaplenili ključe enigme. Pri tem pa so skrili sledi, da Nemci ne bi odkrili, da so njihovi tajnopisi brez vrednosti. Prav tako so postavili znana minska polja in potem so na radijskih sporočilih nemških ladij takoj prepoznali znane koordinate lastnih minskih polj in imeli odlično osnovo za razbiranje.

Razbiranje ostalih tajnopisov

Angleži so razrešili tudi italijanske in japonske tajnopise in s tem bistveno pripomogli k uspešnemu zaključku druge svetovne vojne tako v Sredozemlju kot po celem svetu. Vendar pa je bila ta služba v popolni tajnosti in to še desetletja po koncu vojne. Po koncu vojne so enigme delili članicam Commonwealtha in so tako lahko razbirali njihova »tajna« sporočila. Šele po treh desetletjih popolnega molka je leta 1974 lahko izšla knjiga Ultra, kar je bil znak za udeležence, da je konec zapovedane molčečnosti, in doba priznanja njihovega dela, žal za mnoge že prepozno.

Navahi

Tudi ZDA, ki so medtem že strle japonski tajnopis, so morale izdelati učinkovito napravo za prenašanje tajnih sporočil. Angleži so uporabljali TYPEX, Američani pa SIGABA. Obe sta bili zapletenejši kot enigma in tudi uporabljali so ju strokovno. Obstajale pa so tudi druge možnosti, saj je bil postopek šifriranja in branja dolgotrajen in ni bil uporaben za neposredne akcije na bojišču. Nek vojni dopisnik je težave opisal takole: »Ko so se akcije skoncentrirale na majhno območje, se je vse moralo zgoditi bliskovito hitro. Za šifriranje in dešifriranje ni bilo časa. Tedaj je pomagala dobra stara angleščina – čim bolj groba, tem bolje.« Smola pa je bila v tem, da je mnogo Japoncev obiskovalo ameriške kolidže, zato so tekoče govorili angleško. Tako so informacije prišle tudi v nasprotnikove roke, ki so prav tako vedeli za nove premike. Tu se je vključil P. Johnston. Bil je prestar za bojevanje, zato je hotel pomagati na drugačen način. Videl je, da je angleški jezik ovira in je začel razvijati sistem na izkušnjah iz otroštva. Odrasel je v arizonskih rezervatih Navahov in je dobro poznal njihov svet, poznal je njihov jezik in bil tolmač z vladnimi uradniki. Spoznal je, da bi bil jezik Navahov nerešljiva šifra, hitrost prenosa pa bi bila taka kot v angleščini. Na poskusu so dva Navaha oddaljili in radijski prenos se je povsem posrečil in takoj so ukazali rekrutiranje. Najprej so se morali odločiti za najustreznejše pleme med: Navahi, Sjuji, Čipeva in Pimapago. Odločilo je poročilo, da so Navahi edino pleme, ki jih niso obiskali nemški raziskovalci. Poleg tega je njihov jezik nerazumljiv za ostala plemena, prav tako pa je nerazumljiv tudi za ostale jezikoslovce, razen za 28 Američanov, ki so raziskovali njihov jezik.

Navahi so živeli v težkih razmerah in so bili obravnavani kot manj vredno ljudstvo, vendar so si želeli sodelovati v vojni. Njihov svet je podprl vključitev ZDA v vojno in pokazal svojo lojalnost: «Ni čistejšega izražanja patriotizma, kot je med prvimi Američani.« Tako so si želeli sodelovati, da so dali celo napačne podatke o starosti ali pa so pojedli veliko banan in popili mnogo vode, da so dosegli mejno težo 55 kg. Mnogo angleških besed ni bilo v njihovem jeziku in so jih morali nadomestiti. Tako so postali: višji oficirji - vojni poglavarji, bojni položaji - blatna bivališča, minometi - čepeče puške itd. Celoten slovar

je vseboval 274 besed. Imena pa so črkovali v angleščini, in jih poimenovali po živalih ali predmetih, ki so prevedeni v navajski jezik, kar je za celotno abecedo prikazano na naslednji tabeli 12.

Takoj so pričeli s šolanjem in na koncu šolanja so vsi odlično opravili izpit. Ameriški

Tabela 12: Navahovska kodna tabela za angleščino

A	Ant	Wol-la-chee	N	Nut	Nesh-chee
B	Bear	Shush	O	Owl	Ne-ahs-jsh
C	Cat	Moasi	P	Pig	Bi-sodih
D	Deer	Be	Q	Quiver	Ca-yeilth
E	Elk	Dzeh	R	Rabbit	Gah
F	Fox	Ma-e	S	Sheep	Dibeh
G	Goat	Klizzie	T	Turkey	Than-zie
H	Horse	Lin	U	Ute	No-da-ih
I	Ice	Tkin	V	Victor	A-keh-di-glini
J	Jackass	Tkele-cho-gi	W	Weasel	Gloe-ih
K	Kid	Klizzie-yazzi	X	Cross	Al-an-as-dzoh
L	Lamb	Dibeh-yazzi	Y	Yucca	Tsah-as-zih
M	Mouse	Na-as-tso-si	Z	Zinc	Besh-do-gliz

strokovnjaki za razbiranje niso znali njihovega govora niti zapisati, kaj šele da bi ga razumeli, očitno je šlo za izjemen uspeh. Dva sta ostala za izobraževanje naslednje skupine, ostale pa so poslali na Tihi ocean, kjer so Japonci zavzemali čedalje več ozemlja. Japonci so gradili letališče na Guadalcanalu in s tem bi postal protinapad zaveznikov skoraj nemogoč. Admiral E. King je zato priganjal k invaziji in 7. avgusta se je izkrcala I. mornariška divizija. K njim je spadala tudi prva skupina Navajcev, ki pa je prinesla zgolj zmedo, saj so radiotelegrafisti, ki tega sporazumevanja še niso poznali, v paniki oddajali poročila, da Japonci uporabljajo ameriške frekvence. Poveljnik je takoj ustavil oddaje v navajščini, dokler se ni prepričal o njihovi koristnosti. Eden od Navajev se spominja, da mu je polkovnik rekel, da jih bo obdržal, če bodo hitrejši kot njegov »beli kod«. Oba sva oddala svoja sporočila in vprašali so me koliko časa bom potreboval, ali dve uri? Bolj verjetno dve minuti sem odgovoril. Po štirih in pol minutah sem že dobil odobritev poročila in vprašal sem polkovnika, kdaj se bo odpovedal svoji napravi. Nič ni odgovoril, samo prižgal je svojo pipo in odšel proč. Med boji so Navaji dokazali svojo prednost v primeru, ko so Američani zavzeli japonski položaj in so jih obstreljevali lastni ljudje. Takoj so poslali opozorilo, vendar so ga smatrali za japonsko zavajanje in šele Navaji so dokazali resnični položaj. Pokazali pa so tudi izjemno domoljubnost, saj so kljub čedalje bolj krvavim bitkam vztrajali in dokazali svoje prednost pri hitrosti, zanesljivosti in tajnosti.

Razbiranje pozabljenih jezikov in antičnih zapisov

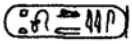
Japonci so imeli posneto mnogo navahovskega govora, pa ga kljub temu niso znali razbrati. Pri razbiranju starih napisov pa pogosto ne vedo za jezik, za glasovno vrednost posameznih znakov, niti za vsebino zapisov. Pa vendar se mnoge ženske in moški strastno lotijo te naloge. Pravila razbiranja tajnopisja in starih napisov so v mnogih pogledih podobna. Tudi tu gre za analizo, pogostost, ponavljanje in oporne točke pomešane z intuicijo in zdravim razmišljanjem.

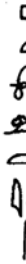
Hieroglifi

Dolga stoletja je bila to zaprta knjiga, ki se je z mojstrskim razbiranjem odprla in omogočila vpogled v davne čase starega Egipta, saj so najstarejši hieroglifi datirani okoli 3.000 let pr. Kr. Hieroglifi kot okrasne črke ali simboli so se uporabljali v templjih, stilizirani hieroglifi so predstavljali hieratsko pisavo za vsakdanje zadeve, okoli leta 600 pr. Kr. pa je hieratsko pisavo nadomestila demotska – ljudska pisava. Vse tri pisave so izumrle okoli leta 400, ko je krščanstvo te pisave nadomestilo s koptsko pisavo, ki je imela 24 grških črk in 6 demotskih črk za glasove, ki jih grščina ni vsebovala. Koptska pisava je zaradi Arabcev izumrla v 11. stoletju. S koptsko pisavo je izumrl tudi koptski jezik in tako je bila jezikovna povezava s starim Egiptom pretrgana. Koptski jezik pa še živi v liturgiji krščansko-koptske cerkve. Strokovnjaki so bili prepričani, da so hieroglifi slikovna pisava in so celo sestavili slovar pomenov predpostavljeno slikovnih znakov.

Leta 1799 so francoski učenjaki naleteli na pomemben kamen, po najdišču imenovan kamen iz Rosette, ki je imel vse tri napise: hieroglifski, demotski in grški napis, ki je bil povsem razumljiv. To je bila oporna točka za razbiranje, saj naj bi imeli vsi trije napisi enako vsebino. Kamen je bil popisan leta 196 pr. Kr. in je sedaj v britanskem muzeju. Prvi, ki je podvomil v slikovno pisavo je bil angleški matematik T. Young. Bil je vsestranski znanstvenik in je znal grško, latinsko, francosko, hebrejsko, kaldejsko, sirsko, arabsko, samaritansko, perzijsko, turško in etiopsko. Ko je zvedel za kamen iz Rosette, je zanj postal neustavljiv izziv. Pozornost so mu zbudili znaki obdani s pentljo, ki so se večkrat ponavljali v enaki ali podaljšani obliki. Predvideval je, da predstavljajo nekaj zelo pomembnega, morda ime faraona Ptolemaja in tako je dokaj dobro razbral glasovne vrednosti posameznih znakov. Žal je imel preveliko spoštovanje do predhodnikov, ki so v hieroglifih videli slikovno pisavo, zato je domneval, da so uvedli zapis imen s črkami šele, ko so po Aleksandru Velikemu Egiptu vladali faraoni, ki so bili Evropejci. Njegovo delo je nadaljeval Francoz J. F. Champollion, ki je tudi znake na obeliskih prečrkoval tako, kot je prikazano v naslednji tabeli 15.

Naslednji preboj mu je uspel, ko je razbral tudi starejšo pentljo, ki so jo sestavljali štirje znaki: znak za sonce, neznani znak in dva znaka za S. S tem je dokazal, da so tudi pri starejših hieroglifih uporabljali črkovno pisavo. Kot mladenič se je učil koptski jezik in ga tekoče obvladal. Z znanjem koptskega jezika je za znak krogec s piko, ki naj bi pomenil sonce, vstavil glasovno vrednost ra in dobil izraz RA-?-S-S in po njegovem mnenju se je to ujemalo le z enim imenim faraona. Ob običajnem izpuščanju samoglasnikov in manjkajočo črko M je prečrkoval RAMESES, torej Ramzes, ime enega največjih faraonov.

Tabela 15: Champollionovo dekriptiranje  in  , kartuš Ptolemaja in Kleopatre na obeliskih, ki jih je prinesel Bankes

Hieroglifi	Glasovna vrednost	Hieroglifi	Glasovna vrednost
	p t o l m e s		c l e o p a t r a

Ta ugotovitev ima temeljno jezikovno vrednost, saj je lahko določil jezik piscev in podrobno proučevanje drugih hieroglifov je pokazalo, da gre prav za koptski jezik. Ugotovil je, da so zapisi kombinacije slikovnih znakov kot sonce itd, lahko so kombinacija slikovnih in črkovnih znakov, ki lahko predstavljajo tudi več soglasnikov. Daljše besede so sestavljene iz slikovnih ugank ali pa so zapisane z navadnimi črkovnimi znaki.

Počasi je dopolnjeval svoje prečrkovanje tako, da je bilo možno branje hieroglifov. Svoje delo je objavil v knjigi *Précis du système hiéroglyphique* leta 1824.

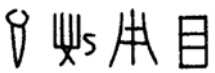
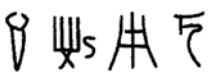
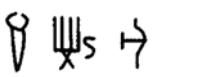
Champollion je na osnovi Youngovega dela in znanja koptskega jezika razbral hieroglife predvsem na osnovi grškega besedila na kamnu iz Rosette, ni pa razbral demotskega besedila, ki še danes čaka na ustrezno razbiranje.

Linear B

Linear B je grška pisava iz bronaste dobe. V tem pred-helenističnem času je celino obvladovala Mikenska kultura, saj so pri izkopavanjih naleteli na veliko umetnostnih izdelkov, vendar niso našli nobenih zapisov. Med trgovci s starinami v Atenah pa so našli nekaj pečatnikov, ki niso imeli pisave, ampak le simbole in ti pečatniki naj bi prihajali iz Krete. Leta 1900 so na Kreti izkopali mnogo tablic, ki so bile tako dobro ohranjene, da so se videli celo prstni odtisi zapisovalcev. Zgleda, da so se tablice ohranile, ker je palačo uničil ogenj, ki je spekel tudi tablice in jih tako ohranil. Tablice so razdelili v tri skupine: 2000 do 1650 pr. Kr. na katerih so bili slikovni znaki, 1750 do 1450 pr. Kr. na katerih so bile črke iz preprostih črt, zato so jo poimenovali linear A in tablice iz 1450 do 1375 pr. Kr. na katerih je bila pisava, ki so jo poimenovali linear B. Ob množici podobnih zapisov se je zdelo razbiranje enostavno, vendar je bilo v resnici bistveno težje. Opazili so okoli 90 različnih znakov, kar je kazalo na zlogovno pisano. Črkovne pisave imajo navadno od 20 do 40 črk za posamezne glasove, zlogovne pisave imajo 50 do 100 znakov za posamezne zloge, slikovne pisave pa obsegajo več sto, v kitajščini celo več tisoč znakov.

Nekateri raziskovalci so bili prepričani, da gre za izumrli kretski jezik, drugi pa so menili, da gre za grščino. Leta 1939 so tudi na celini našli tablice s pisavo linear B, vendar to še ni pomenilo, da gre za grško pisavo. A. Kobler je sredi štiridesetih let spoznala, da mora pustiti vnemar vse teorije o pisavi in se posvetiti le značilnostim posameznih možnih besed. Opazila je, da se besede pregibajo z različnimi končnicami, pri tem pa lahko dobijo še premostitveni zlog podobno kot v akadščini. Primera pregibanja dveh besed, najverjetneje samostalnikov, sta prikazana v naslednji tabeli 17.

Tabela 17: Dve sklanjani besedi v linearni B

	Beseda A	Beseda B
1. sklon		
2. sklon		
3. sklon		

Sestavila je pregled znakov, kjer je vsakemu znaku dodelila dvomestno število, in z dvojico številk označila nekatere besede in njihovo pregibanje. Dvojice je sestavila tudi v rešetko, vendar se ji večji preboj ni posrečil, saj je 1950 umrla za rakom na pljučih v 43 letu.

Le nekaj mesecev pred svojo smrtjo je A. Kobler dobila pismo od angleškega arhitekta M. Ventrisa, ki se je tudi zanimal za problem razbiranja pisave linear B. Ventris je izpopolnil rešetko A. Kobler tako, da je v stolpce razdelil samoglasnike, v vrste pa soglasnike in dobil 5x15=75 polj za posamezne zloge. Skoraj polovico polj je napolnil s števili, ki so pomenili ustrezne kombinacije. Nekateri samoglasniki in nekateri soglasniki so bili očitno številnejši in zato dobra osnova za razbiranje. Do sedaj se je upiral skušnjavi, da bi nekaterim skupinam dodelil glasovne vrednosti, sedaj pa je opazil, da se nekatere skupine pojavljajo pogosteje in tako je namesto šifre 08-73-30-12 vstavil a-mi-ni-so = Amnisos, pomembno pristanišče. Na tej osnovi je sklepal, da mora zlog 12 vsebovati s, ostala znaka pa o in tako je za drugo besedo dobil 70-52-12 je ?o-?o-so ali ko-no-so ali Knosos. Na tej osnovi je sestavil tretjo besedo in sicer 69-53-12 ali ??-?i-so ali tu-li-so ali Tulisos, pomembno mesto na Kreti. Postopno se je odpirala zaprta stran in posamezni zlogi so postali znani z ustrezno glasovno vrednostjo. Izkazalo se je, da so zapisi v stari grščini, ki je okoli 500 let starejša od homerjeve grščine in je bila jezik Odiseja.

Ventris je imel predavanje na BBC, ki ga je poslušal tudi J. Chadwick, ki je bil zgrožen in je tako kot večina strokovnjakov zavrnil Ventrisovo delo kot dela amaterja, kar je v jezikovem pogledu tudi bil. Priskrbel si je Ventrisove delovne zapiske in jih študiral, da jih bo lahko znanstveno raztrgal. Že v nekaj dneh pa je ta skeptični znanstvenik postal eden prvih zagovornikov Ventrisove teorije, da so zapisi v pisavi Linear B pisani v grščini. Bila

sta idealen par, Ventris kot razbiralec tajne pisave in Chadwick kot poznavalec razvoja grščine. Skupaj sta izdala več člankov in svoje delo kronala s temeljnim delom *Documents in Mycenaean Greek*, ki je izšlo 6. septembra 1956. Pregled vseh zlogovnih znakov in njihove glasovne vrednosti so podane v naslednji tabeli 23.

Tabela 23: Znaki pisave linearna B s številkami in glasovnimi vrednostmi

01		*da*	30		*ni*	59		*ta*
02		*ro*	31		*sa*	60		*ra*
03		*pa*	32		*qo*	61		*o*
04		*te*	33		*ra*$_2$	62		*pte*
05		*to*	34			63		
06		*na*	35			64		
07		*di*	36		*jo*	65		*ju*
08		*a*	37		*ti*	66		*ta*$_2$
09		*se*	38		*e*	67		*ki*
10		*u*	39		*pi*	68		*ro*$_2$
11		*po*	40		*wi*	69		*tu*
12		*so*	41		*si*	70		*ko*
13		*me*	42		*wo*	71		*dwe*
14		*do*	43		*ai*	72		*pe*
15		*mo*	44		*ke*	73		*mi*
16		*pa*$_2$	45		*de*	74		*ze*
17		*za*	46		*je*	75		*we*
18			47			76		*ra*$_2$
19			48		*nwa*	77		*ka*
20		*zo*	49			78		*qe*
21		*qi*	50		*pu*	79		*zu*
22			51		*du*	80		*ma*
23		*mu*	52		*no*	81		*ku*
24		*ne*	53		*ri*	82		
25		*a*$_2$	54		*wa*	83		
26		*ru*	55		*nu*	84		
27		*re*	56		*pa*$_3$	85		
28		*i*	57		*ja*	86		
29		*pu*$_2$	58		*su*	87		

Sodobno tajnopisje

Razvoj sodobnega tajnopisja je vezan na čedalje zmogljivejše računalnike, ki ob povezavi v super računalnik obdelajo izjemno količino podatkov in klasični načini tajnopisja niso več nerešljivi. Računalniki pa omogočajo tudi programiranje takih šifrantov, ki posnemajo klasične šifrirne stroje, vendar s skoraj neomejenimi spremenljivkami, zato jih ni mogoče dešifrirati. Ostane pa problem prenosa šifrirnega sistema, ki ga morata imeti tako pošiljatelj kot naslovnik. Težava se je pojavila z rabo v poslovnem svetu, zato so iskali standardizirani sistem. Uveljavil se je sistem IBM z imenom Lucifer, ki je sporočilo premešal skladno s ključem, ki sta ga morala imeti pošiljatelj in naslovnik. Dovolj veliko število ključev je zagotavljalo tajnost sporočil. Ostal pa je problem in sicer razdeljevanje ključev. Problem je rešljiv z osebnim prevzemom ali z dostavo z zanesljivim kurirjem, kar pa je v sodobnem svetu in globalnem poslovanju predrago in prepočasno.

Razrešitev razdeljevanja ključev

Razrešitev razdeljevanja ključev je največji tajnopisni dosežek vseh časov. Različne skupine zanesenjakov pa so strle tudi ta problem. Američana Diffie in Hellman sta ugotovila, da je možno poslovanje tako, da A pošlje B sporočilo v zaboju z obešenko. B doda svojo obešenko in jo pošlje A, ki odstrani svojo obešenko in jo pošlje B, ki sedaj lahko prebere sporočilo. V elektronski obliki namesto zaboja uporabimo tajnopis, vendar je pomemben vrstni red, saj mora biti zadnje prvo, tako kot si obujemo nogavice in čevlje moramo sezuvanje ponoviti v celoti v obratmem vrstnem redu, saj ne moremo sezuti nogavic prej kot čevljev. Elektronska inačica obešenke daje nesmisel, saj B razbira tajnopis šifriran s ključem A, ki ga je A že odstranil. Tak sistem v elektronskem poslovanju sicer ne deluje, je pa odprl možnost uporabe enosmerne matematične funkcije, ki ima lastnost obešenke. Take lastnosti imajo neponovljivi procesi kot so mešanje barv, razbitje jajca itd, v matematiki pa je mnogo takih funkcij, predvsem so to modularne funkcije. To pokažemo na primeru eksponentne funkcije, kjer je modul 7 in je rezultat le presežek preko mnogokratnika števila 7.

x	1	2	3	4	5	6
3^x	3	9	27	81	243	729
3x(mod7)	3	2	6	4	5	1

Diffie – Hellman – Merklov postopek za izmenjavo ključev (odkril ga je Hellman, vendar so delovali skupaj) uporabi funkcijo Y^x (mod P). Celoten postopek zahteva več javnih sporočil in je zato nekoliko neprijeten: »A« in »B« se javno dogovorita za vrednosti Y in P, s tem, da mora biti Y manjši od P. »A« izbere vrednost za x in ga obdrži v tajnosti, z njim pa izračuna vrednost funkcije in vrednost pošlje »B«; »B« stori enako, vendar s svojo vrednostjo za x; ko ponovita račun s sprejetim številom dobita isti rezultat, ki je ključ!

Odprti ključ

Nesimetrični ključ

Diffie je odkril nov šifrirni postopek tajnopisja z nesimetričnim ključem. Do sedaj je bilo tajnopisje in razbiranje preprosto obrnjen postopek, pri nesimetričnem ključu pa je le enosmeren postopek. Primer: »A« pošlje javni ključ za šifriranje (število) po spletu, zasebni ključ za razbiranje pa obdrži v tajnosti; katerikoli »B, C itd« lahko pošlje šifrirano sporočilo A, ki je dostopno tudi vsem drugim uporabnikom spleta; sporočilo pa lahko prebere le »A« z zasebnim ključem. Ko je poleti 1975 Diffie objavil svoje odkritje so se mu pridružili še drugi znanstveniki in pričeli iskati enosmerne funkcije, ki bi ustrezale pogojem za nesimetrično tajnopisje. Odkritje pa se jim ni posrečilo, saj jih je prehitela druga skupina.

Praštevila

Praštevila so ustrezna nesimetrična funkcija. Skupina Andelman, Rivest in Shamir so sestavljali odlično ekipo, kjer sta Rivest in Shamir podajala predloge, Andelman pa jih je zavračal in ju držal v pravi smeri. Rivest je odkril pravo funkcijo v obliki praštevil, postopek pa so poimenovali ARS po začetnicah avtorjev. Postopek: »A« objavi javni ključ, ki ju tvori zmnožek dveh praštevil p in q, ki jih je obdržal v tajnosti. Če hoče »B, C, itd« poslati »A« tajno sporočilo, ga šifrira z njegovim javnim ključem in »A« ga lahko prebere, saj lahko funkcijo obrne, ker pozna svoji izbrani praštevili. Drugim pa razbiranje ni dostopno, razen če po dolgotrajnem postopku ugotovijo oba faktorja p in q. Pri majhnih praštevilih je rešitev hitra, pri zelo velikih praštevilih pa je čas razbiranja prevelik. Za bančne posle se uporabljajo zmnožki večji od 10^{300} in čas razbiranja z super računalnikom je večji od 1000 let. Pri dovolj velikih številih p in q pa je šifra ARS nerešljiva.

Prijazna zasebnost

Pretty Good Privacy s kratico PGP. Phil Zimmermann je bil prepričan, da ima vsak človek pravico do zasebnosti v javnem sporazumevanju in to na enostaven način. Sistem ARS je nadgradil s programom, ki samodejno opravlja delo tajnopisja in razbiranja in ga poimenoval Pretty Good Privacy s kratico PGP. Obrnjen postopek ARS pa omogoča tudi elektronski podpis, ki je javno dostopen, vendar potrjuje, da je sporočilo prišlo prav od osebe z določenim javnim ključem. Združena postopka omogočata tako zasebnost kot lastnoročni podpis pošiljatelja. Zimmermann je hotel najprej svoj izum prodajati, zaradi zahtev, da bi bila elektronska sporočila dostopna tajnim služba zaradi preprečevanje terorističnih dejanj, pa je ponudil svoj izdelek kot del programske opreme zastonj in se tako izognil mnogim upravnim oviram. Kljub temu je ameriški FBI tri leta iskal temelje za obtožbo, da je Zimmermann izvozil nevarno orožje, saj je sovražne države in teroriste oskrbel z orožjem s katerim so se lahko izmaknili obrambnim ukrepom ameriške vlade. Tu so nastopili borci za človekove pravice, predvsem pa podjetja, ki jim je elektronsko poslovanje prineslo pocenitev, razvoj in široko dostopnost do kupcev in surovin. Končno

so pri FBI uvideli, da je stvar zamujena in so s procesom naredili le reklamo za široko uporabno in prijazno tajnopisje. Tako je bil Zimmerman rehabilitiran, njegov program pa so s spleta lahko dobili vsi.

Problem terorizma

Ob nedvoumni zaščiti tajnopisja se je pojavilo vprašanje tajnosti dopisovanja terorističnih skupin in to vprašanje je odprto še danes. Sodobno gospodarstvo čedalje močneje zahteva tajno poslovanje tako za zaščito proizvodnje kot zlasti za spletno prodajo. Nekatere oblasti pa se kljub temu zavzemajo za obvezno deponiranje ključev, kar pa ne rešuje problema zadovoljivo, saj so prav tako možne zlorabe, ob izgubi ključa pa je potreben ustrezen postopek za izbris starega in za dodelitev novega ključa. Poleg tega pa so lahko kadarkoli objavljeni tudi drugi ne deponirani javni ključi, ki omogočajo tajnopisje. Res je, da se jih lahko takoj ugotovi in zato lažje preverja njihovo tajnopisno delovanje, ki pa je še vedno nerešljivo. Poleg tega pa se lahko javni ključi tudi hitro spreminjajo in tako sproti puščajo svoje nove sledi, kar je za teroristično delovanje značilno. Tako jih je težje odkriti, saj stare sledi niso več uporabne, nove pa še niso odkrite.

Zaključek

V vseh časih so ljudje odkrivali novosti, ki so predstavljale varovane prednosti različnih, plemenskih, elitnih, narodnih in državih skupin. Ob izumih zapisovanja so zato izumljali postopke, kako bi prikrili zapisano vsebino, nasprotniki pa so jo poskušali odkriti. Prikrivanje napisane vsebine je tajnopis, odkrivanje vsebine pa razbiranje. Enostavno tajnopisje je hitreje rešljivo, zato so tajnopisci čedalje bolj zapletali postopek, razbiralci pa uporabljali čedalje uspešnejše načine analiz. Sodobno tajnopisje uporablja šifriranje z zmožkom dveh velikih praštevil, ki zagotavlja ustrezno varnost pred razkrivanjem. Žal je varnost zagotovljena tudi mafijskim in terorističnim skupinam.

Očitno ne moremo zaradi peščice teroristov prepovedati tajnega poslovanja, ki obsega večji del svetovne proizvodnje in trgovine. Velikemu bratu tudi ne moremo dopustiti, da bo v našem imenu obvladoval naše življenje in nas kontroliral v vseh porah našega življenja. Očitno bo treba poiskati druge preizkušene načine urejanja sveta, verjetno prav tako kot nam ga že od nekdaj ponujajo velika verstva sveta. Ponovno se bo treba vrniti k materi naravi in novim generacijam privzgojiti ne le tekmovalnost, ampak predvsem sodelovanje v mirnem sožitju med različnimi svetovnimi, narodnimi in osebnimi interesi.

Tajnopisje in razbiranje sta na kratko prikazana prav zaradi tega, ker so mnoge osnove in postopki uporabni tudi pri razbiranju pred-antičnih napisov razumljivih na slovanskih osnovah. Razbiranje etruščanskih, venetskih, retijskih in frigijskih napisov je enostavnejše, saj so glasovne vrednosti večine črkovnih znakov dobro znane in le izjemoma naletimo na znake, ki jim je treba glasovno vrednost dodeliti šele na osnovi razumevanja obdelovanega besedila. Gre preprosto za to, da neznano zvezno pisano besedilo v glasovno znanem zapisu, delimo na različne sklope črk, ki predstavljajo znane besede. Tako dobljene besede preverjamo z različnimi znanimi, sodobnimi ali izumrlimi jeziki in njihovimi narečji ter

statistično ugotovimo najboljše ujemanje. Tako primerjanje nam podaja tudi najustreznejši jezik razumevanja tako obravnavanih napisov in primerna narečja, saj navedeni napisi niso pisani v normiranih jezikih.

Literatura

1 Simon Singh, *Knjiga šifer, Umetnost šifriranja od starega Egipta do kvantne kriptografije*, prevedel J. Plešej, Učila International, Tržič **2006**.

Povzetek

V vseh časih pismenosti so obstajale skrivnosti, ki so jih varovali s tajnopisjem, medtem ko so nasprotniki poskušali odkriti njihovo vsebino z razbiranjem. Postopki razbiranja so uporabni tudi pri preučevanju starodavnih črkovnih, zlogovnih in slikovnih zapisov z znanimi in neznanimi glasovnimi vrednostmi posameznih znakov. Uporabni pa so tudi pri prečrkovanju in razumevanju napisov, ki jih predstavljajo pred-antični zapisi v jezikih razumljivih na slovanskih osnovah. Tajnopisje in razbiranje je bilo posebno pomembno v vojnih časih, zlasti v obeh svetovnih vojnah. Brez sodobnega tajnopisja ni možna sodobna organiziranost svetovnega denarnega in dobrinskega trga.