

Turinys

Įvadas	9
Škotijos karalienės Marijos Stiuart šifras	14
Le Chiffre Indéchiffrable	56
Paslapties mechanizavimas	107
Kaip buvo įveikta „Enigma“	146
Kalbos barjeras	190
Aldona su Broniumi išeina į viešumą	239
PGP	285
Kvantinis šuolis į ateitį	307
Iššūkis iššifruotojams	337
A priedas	352
B priedas	354
C priedas	356
D priedas	357
E priedas	358
F priedas	360
G priedas	362
H priedas	363
I priedas	364
J priedas	365
Žodynėlis	368
Padėka	372
Papildoma literatūra	375
Rodyklė	380

Kalbos barjeras

Kai britų dekoduočiai galynėjosi su vokiečių „Enigmos“ šifru ir keitė karo eigą Europoje, amerikiečių dekoduočių vaidmuo Ramiojo vandenyno regiono įvykiuose buvo lygiai toks pat svarbus nulaužinėjant japonų šifravimo mašinos šifrą, Amerikoje vadinamą „Purple“. Pavyzdžiui, 1942 m. amerikiečiai iššifravo pranešimą, kuriame bendrais bruožais buvo išdėstytas japonų planas suvaidinti puolimą ir patraukti JAV karių jūrų laivyno pajėgas prie Aleutų salų, kad japonų karinės jūrų pajėgos pasiektų savo tikrąją tikslą – užimtų Midvėjaus salą. Nors amerikiečių laivai žaisdami pagal planą išplaukė iš Midvėjaus, labai toli nenuplaukė. Kai amerikiečių kriptanalitikai perėmė ir iššifravo japonų įsakymą pulti Midvėjų, laivai greitai parplaukė atgal ir išsaugojo salą viename svarbiausių mūšių per visą karą Ramiajame vandenyne. Pasak admirolo Česterio Nimico (*Chester Nimitz*), amerikiečių pergalė prie Midvėjaus „iš esmės buvo žvalgybos pergalė. Bandydami užpulti netikėtai, japonai patys buvo užklupti“.

Maždaug po metų amerikiečių kriptanalitikai perėmė pranešimą, kuriame buvo išdėstytas admirolo vyriausiojo Japonijos laivyno vado Isoroku Jamamoto (*Isoroku Yamamoto*) apsilankymo šiaurinėse Saliamono salose maršrutas. Nimitas nusprendė pasiųsti naikintuvą Jamamoto lėktuvui perimti ir jį numušti. Tiksliai 8.00 val., kaip tik tada, kaip buvo nurodyta perimtame tvarkaraštyje, pagarsėjęs maniakišku punktualumu Jamamotas priartėjo prie savo kelionės tikslo. Ten jį pasitiko aštuoniolika amerikiečių naikintuvų „P-38“. Jiems pavyko sunaikinti vieną įtakingiausių vyriausiosios Japonijos vadovybės figūrų.

Nors galiausiai „Purple“ ir „Enigma“ – japonų ir vokiečių šifrai buvo įveikti, iš pradžių jie tikrai apsaugodavo informaciją, o amerikiečių ir britų analitikams reikėjo labai smarkiai pasistengti juos įveikti. Iš tikrųjų jei šifravimo mašinos būtų buvusios naudojamos tinkamai, be pasikartojančių pranešimo raktų, be silių, neribojant komutatoriaus nustatymų

ir šifratoriaus kombinacijų ir be stereotipinių pranešimų, kurie ir buvo ruošinių šaltinis, greičiausiai jos taip niekada ir nebūtų įveiktos.

Tikrąją mašininę šifrų pranašumą ir galimybes pademonstravo šifravimo mašina „Typex“ (arba „Type X“), kuri buvo naudojama britų sausumos ir oro pajėgose, o amerikiečių kariškiai naudojo šifravimo mašiną „SIGABA“ (arba „M-143-C“). Abi šios mašinos buvo sudėtingesnės už „Enigmą“ ir abi naudojamos taip, kaip reikia, todėl per karą jų niekas neįveikė. Sąjungininkų kriptografai buvo įsitikinę, kad elektromechaniniai mašininiai šifrai gali užtikrinti ryšių saugumą. Tačiau sudėtingi mašininiai šifrai – ne vienintelis būdas siųsti saugius pranešimus. Iš tiesų viena saugiausių užšifravimo formų, naudotų per Antrąją pasaulinę karą, buvo pati paprasčiausia.

Per Ramiojo vandenyno karinę kampaniją amerikiečių vadai suprato, jog šifravimo mašinos, kaip antai „SIGABA“, turi esminį trūkumą. Nors elektromechaninis šifravimo saugumo lygis buvo palyginti aukštas, jis buvo skausmingai lėtas. Pranešimus reikėdavo spausdinant įvesti paraidžiui, išvedinį – užrašyti paraidžiui, o tada radistas perduodavo užbaigtą kriptogramą. Tada užšifruotą pranešimą priėmęs radistas turėjo jį perduoti šifravimo specialistui, kuris atidžiai parinkdavo teisingą raktą, spausdindamas įvesdavo kriptogramą į šifravimo mašiną ir iššifruodavo vieną raidę po kitos. Tokiai kebliai operacijai reikalingas laikas ir vieta buvo tik vadavietėje ar laive, tačiau nepalankiomis ir įtemptomis sąlygomis, pavyzdžiui, Ramiojo vandenyno salose, mašininis užšifravimas ne labai tiko. Vienas karo korespondentas aprašė ryšio sunkumus per mūšio džiunglėse įkarštį: „Kai mūšis vykdavo mažoje teritorijoje, viskas turėdavo vykti žaibiškai. Laiko užšifruoti ir iššifruoti nebuvo. Tokiu metu kuo nešvankesnė kalba, tuo geriau; literatūrinė anglų kalba būdavo paskutinė išeitis.“ Amerikiečių nelaimei, daugelis japonų kareivių mokėsi amerikiečių koledžuose ir laisvai kalbėjo angliškai, laisvai ir keikdavosi angliškai. Vertinga informacija apie amerikiečių strategiją ir taktiką patekavo priešui į rankas.

Vienas pirmųjų sureagavęs į šią problemą buvo inžinierius iš Los Anželos Filipas Džonstonas (*Philip Johnston*), kuris buvo per senas eiti į frontą, bet norėjo prisidėti prie šalies gynybos. 1942 m. pradžioje, įkvėptas vaikystės prisiminimų, jis ėmė kurti užšifravimo sistemą. Džonstonas, protestantų misionierių sūnus, užaugo Arizonos navachų rezervatuose, todėl navachų kultūra jam buvo kaip gimtoji. Jis buvo vienas iš nedaugelio pašaliečių, laisvai kalbėjusių navachų kalba, todėl galėdavo dirbti

vertėju per navachų ir valdžios atstovų susitikimus. Vertėjo darbas nuvedė jį į Baltuosius rūmus, kur devynmetis Džonstonas vertė dviem navachams, kurie kreipėsi į prezidentą Teodorą Ruzveltą (*Theodore Roosevelt*), kad jų bendruomenei būtų užtikrintos vienodesnės sąlygos. Džonstonas gerai žinojo, kad pašaliečiai šios kalbos visai nesupranta, ir tai davė jam mintį, kad navachų ar bet kuri kita Amerikos čiabuvių kalba tikrai gali būti neįveikiamas kodas. Jei kiekviename Ramiojo vandenyno batalione būtų pora radistų navachų, būtų užtikrintas saugus ryšys.

Jis pasidalijo šia mintimi su pulkininku leitenantu Džeimsu E. Džonsu (*James E. Jones*), teritorijos ryšių karininku Elioto kariniame miestelyje prie pat San Diego. Vien metęs kelias navachų frazes suglumusiam kariškiui, Džonstonas įtikino jį, kad šią mintį verta rimtai apsvarstyti. Po dviejų savaitių Džonstonas sugrįžo su dviem navachais pasirengęs atlikti parodomąjį bandymą vyriausiųjų laivyno karininkų akivaizdoje. Navachus atskyrė vienas nuo kito ir vienam buvo duoti šeši tipiniai pranešimai anglų kalba, kuriuos jis išvertė į navachų kalbą ir per radiją perdavė savo kolegai. Gavėjas navachas išvertė pranešimus į anglų kalbą, užrašė ir įteikė karininkams, kurie palygino su pirminiais pranešimais. Navachų radistų žaidimas pasirodė tobulas, taigi karinio laivyno karininkai pavedė vykdyti bandomąjį projektą ir įsakė nedelsiant pradėti navachų šaukimą.

Tačiau prieš ką nors priimdami pulkininkas leitenantas Džonsas ir Filipas Džonstonas turėjo nuspręsti, su kuo atlikti bandomąjį tyrimą – navachais ar pasirinkti kokią kitą gentį. Pirmą kartą demonstruodamas Džonstonas atsivedė navachus, nes buvo asmeniškai susijęs su gentimi, tačiau nebūtinai dėl to juos reikėjo rinktis. Pats svarbiausias atrankos kriterijus buvo žmonių skaičiaus klausimas: jūrų pėstininkams reikėjo rasti gentį, galinčią atsiųsti daug žmonių, kurie būtų raštingi ir laisvai kalbėtų angliškai. Dėl menkos finansinės vyriausybės paramos daugelyje rezervatų raštingumo lygis buvo labai žemas, todėl dėmesys buvo skirtas keturioms didžiausioms gentims – navachams, sijams, čipevams ir pimams.

Navachai buvo didžiausia, bet neraštingiausia gentis, o pimai buvo raštingiausia, bet gerokai mažesnė gentis. Rinktis nelabai buvo iš ko – tik keturios gentys, ir galutinį sprendimą lėmė kitas nepaprastai svarbus veiksnys. Oficialioje ataskaitoje dėl Džonstono projekto buvo teigiama:

„Jungtinėse Valstijose navachai yra vienintelė gentis, kurios per pastaruosius dvidešimt metų nebūtų užpuolę vokiečių studentai.

Tie vokiečiai, apsimetę menininkais, antropologais ir panašiai, studijuoja įvairius genčių dialektus ir neabejotinai gerai praktiškai susipažino su visų genčių, išskyrus navachų, dialektais. Todėl navachai – vienintelė gentis, kuri gali užtikrinti visišką svars-tomo darbo saugumą. Derėtų pažymėti ir tai, kad kitos gentys ir tautos, galima išimtis – tie 28 amerikiečiai, kurie studijavo dialektą, visai nesupranta navachų genties dialekto. Šis dialektas – tas pat, kaip slaptas kodas priešui, ir puikiai tinka sparčiam bei saugiam susisiekimui.“

Tuo metu, kai Amerika įsitraukė į Antrąjį pasaulinį karą, navachai gyveno baisiomis sąlygomis ir buvo laikomi antrarūšiais žmonėmis. Vis dėlto genties taryba pritarė mobilizacijai ir prisiekė ištikimybę: „Niekur nerasite grynesnio amerikiečio, kaip tarp pirmųjų amerikiečių.“ Navachai taip veržėsi į mūšį, kad kai kurie meluodavo dėl amžiaus arba prisirydavo bananų ir prisiplepdavo tiek vandens, kad pasiektų reikalaujamą minimalų 55 kg svorį. Lygiai taip pat nesunku buvo rasti tinkamų kandidatų į navachų radistus šifruotojus arba kodakalbius, kaip jie buvo praminti. Per keturis mėnesius nuo Perl Harboro bombardavimo 29 navachai, kai kurie vos 15 metų, pradėjo dviejų mėnesių ryšių kursą pas jūrų pėstininkus.

Dar prieš mokymus jūrų pėstininkams reikėjo išspręsti vieną klausimą, kuris apsunkindavo vienintelį kitą Amerikos čiabuvių kalba grįstą kodą. Per Pirmąjį pasaulinį karą Šiaurės Prancūzijoje 141-ojo pėstininkų pulko D kuopos kapitonas E. V. Horneris (*E. W. Horner*) įsakė aštuonis čoktavų genties vyrus pasamdyti radistais. Aišku, kad nė vienas priešas nesuprato jų kalbos, todėl čoktavai garantavo saugų ryšį. Tačiau tokia šifravimo sistema turėjo esminį trūkumą, nes čoktavų kalboje nebuvo šiuolaikinės dalykinės karinės kalbos atitikmenų. Todėl specialus techninis terminas pranešime galėdavo būti išverstas kaip neaiški čoktavų kalbos frazė ir kildavo pavojus, kad gavėjas ją neteisingai supras.

Ta pati bėda būtų kilusi ir dėl navachų kalbos, tačiau jūrų pėstininkai sumanė sudaryti navachų terminų žodynėlį kitaip neišverčiamais anglų kalbos žodžiams pakeisti ir taip išvengti galimų dviprasmybių. Stažuotojai padėjo sukaupti žodynėlį, kuriame žodžiai, susiję su gamta, buvo parinkti konkrečioms kariniams terminams apibrėžti. Taip paukščių pavadinimai buvo panaudoti lėktuvams, o žuvų – laivams pavadinti (11 lentelė). Vyresnieji karininkai tapo „karo vadais“, būriai – „pirminiais

klanais“, įtvirtinimai pavirto „urvais“, o minosvaidžiai buvo vadinami „tupinčiais ginklais“.

Nors užbaigtame žodynėlyje buvo 274 žodžiai, ne tokius nuspėjamus žodžius, asmenvardžius ir vietovardžius vis tiek buvo keblu išversti. Buvo nuspręsta sukurti užkoduotą fonetinį raidyną sudėtingiems žodžiams paraidžiui rašyti. Pavyzdžiui, žodis *Pacific* („Ramusis“) buvo surašomas pirmosiomis žodžių raidėmis *pig, ant, cat, ice, fox, ice, cat* („kiaulė, skruzdė, katė, ledas, lapė, ledas, katė“), kuris į navachų kalbą buvo verčiamas kaip *bi-sodih, wol-la-chee, moasi, tkin, ma-e, tkin, moasi*. 12 lentelėje pateikiamas visas navachų raidynas. Per du mėnesius radistai stažuotojai išmoko visą žodynėlį ir raidyną, todėl kodų žurnalai, galėję patekti į prieš rankas, pasidarė nebereikalingi. Navachai buvo įpratę viską mokytiis mintinai, nes navachų kalba neturėjo rašto, todėl jie įsimindavo jiems pasakojamas liaudies pasakas ir šeimos istorijas. Pasak vieno iš stažuotojų Viljamo Makabės (*William McCabe*), „pas navachus viskas yra galvoje – dainos, maldos – viskas. Mes taip išauklėti“.

Naikintuvas	Kolibris	Da-he-tih-hi
Žvalgybinis lėktuvas	Pelėda	Ne-as-jah
Torpednešis	Kregždė	Tas-chizzie
Bombonešis	Suopis	Jay-sho
Pikiruojamasis bombonešis	Vištvanagis	Gini
Bombos	Kiaušiniai	A-ye-shi
Mašina amfibija	Varlė	Chal
Kreiseris	Banginis	Lo-tso
Eskadrinis minininkas	Ryklis	Ca-lo
Povandeninis laivas	Geležinė žuvis	Besh-lo

11 lentelė. Kodiniai navachų kalbos žodžiai, vartoti lėktuvams ir laivams koduoti.

Baigę stažuotę navachai laikė egzaminą. Siuntėjai išversdavo eilę pranešimų iš anglų į navachų kalbą, juos perduodavo, o gavėjai vėl išversdavo pranešimus į anglų, prireikus pavartodami įsimintus žodžius ir raidyną. Vertimai atitikdavo žodis į žodį. Sistemos patikimumui patikrinti įrašas buvo perduotas karinių jūrų pajėgų žvalgybai – padaliniui, kuris buvo nulaužęs „Purple“ – sunkiausią japonų šifrą. Po trijų savaičių intensyvios kriptoanalizės karinių jūrų pajėgų dekodotojai vis dar suko galvą dėl pranešimų. Anot jų, navachų kalba – tai „keista gomurinių, nosinių,

neištariamų garsų seka, kurios net transkribuoti negalime, o juo labiau nulaužti“. Buvo nuspręsta, kad navachų kodas tinka. Dviejų navachų karių, Džono Benalio (*John Benally*) ir Džonio Manuelito (*Johnny Manuelito*), buvo paprašyta pasilikti ir apmokyti kitą šauktinių partiją, o likusieji 27 navachų radistai šifruotojai buvo priskirti prie keturių pulkų ir išsiųsti į Ramiojo vandenyno regioną.

A	Ant (skruzdė)	Wol-la-chee	N	Nut (riešutas)	Nesh-chee
B	Bear (lokys)	Shush	O	Owl (pelėda)	Ne-as-jah
C	Cat (katė)	Moasi	P	Pig (kiaulė)	Bi-sodih
D	Deer (elnias)	Be	Q	Quiver (strėlinė)	Ca-yeilth
E	Elk (taurusis elnias)	Dzeh	R	Rabbit (kiškis)	Gah
F	Fox (lapė)	Ma-e	S	Sheep (avis)	Dibeh
G	Goat (ožys)	Klizzie	T	Turkey (kalakutas)	Than-zie
H	Horse (arklys)	Lin	U	Ute (jutas)	No-da-ih
I	Ice (ledas)	Tkin	V	Victor (nugalėtojas)	A-keh-di-glini
J	Jackass (asilas)	Tkele-cho-gi	W	Weasel (žebenkštis)	Gloe-ih
K	Kid (vaikas)	Klizzie-yazzi	X	Cross (kryžius)	Al-an-as-dzoh
L	Lamb (ėriukas)	Dibeh-yazzi	Y	Yucca (juka)	Tsah-as-zih
M	Mouse (pelė)	Na-as-tso-si	Z	Zinc (cinkas)	Besh-do-gliz

12 lentelė. Navachų raidyno kodas.



52 pav. Pirmieji 29 navachų radistai šifruotojai pozuoja tradicinei išleistuvių nuotraukai.

1941 m. gruodžio 7 d. japonų karinės pajėgos užpuolė Perl Harborą ir netrukus viešpatavo vakarinėse Ramiojo vandenyno regiono dalyse. Gruodžio 10 d. japonų kariai užėmė amerikiečių įgulą Guame, gruodžio 13 d. – Gvadalkanalį, vieną iš Saliamono salyno salų, gruodžio 25 d. kapituliavo Honkongas, o 1942 m. sausio 2 d. Filipinuose pasidavė JAV kariai. Japonai planavo Gvadalkanalijoje pastatyti aerodromą, įrengti bombonešių bazę, kuri suteiktų jiems galimybę sunaikinti Sąjungininkų tiekimo linijas, taip atimti iš Sąjungininkų kontratakos galimybę ir kitą vasarą įsivertinti Ramiojo vandenyno regione. Amerikos karinių jūrų pajėgų operacijų vadas admiras Ernestas Kingas (*Ernest King*) paragino pulti salą, kol aerodromas dar neužbaigtas, ir rugpjūčio 7 d. 1-oji jūrų pėstininkų divizija įsiveržė į Gvadalkanalį. Su pirmais išsilaipinimo būriais išsilaipino ir pirma radistų šifruotojų grupė, kurie savo akimis matė karo veiksmus.

Navachai buvo įsitikinę, kad jų gebėjimai bus didelė paspartis jūrų pėstininkams, tačiau pirmosios jų pastangos sukėlė tikrą sumaištį. Daugelis profesionalių ryšininkų nežinojo šio naujo kodo ir per visą salą siuntinėjo panikos kupinus pranešimus, kad japonai naudojami amerikiečių

dažniais. Operacijai vadovavęs pulkininkas tučiuojau sustabdė navachų pranešimus, kol pats įsitikino, kad sistema verta dėmesio. Vienas iš radistų šifruotojų prisiminė, kaip vis dėlto grąžino navachų kodą:

„Pulkininkui gimė mintis. Jis pasakė, kad mus laikys tik su viena sąlyga – jei aš aplenksiu jo „baltąjį kodą“ – mechaninį stuksestantį cilindrą. Mes abu išsiuntėme pranešimus – per baltąjį cilindrą ir aš balsu. Abu gavome atsakymus, bet lenktyniavome tam, kad pažiūrėtume, kas pirmas dekoduos gautą atsakymą. Manęs paklausė: „Kiek užtruksi? Dvi valandas?“ „Apie dvi minutes“, – atsakiau. Kitas vaikinai dar dekodavo, kai maždaug po keturių su puse minutės gavau patvirtinimą, kad pranešimas priimtas. Aš paklausiau: „Pulkininke, kada gi pagaliau atsisakysite to savo cilindro?“ Jis nieko neatsakė. Tiesiog užsidegė pypkę ir nuėjo.“

Netrukus radistai šifruotojai įrodė, ko verti mūšio lauke. Per vieną epizodą Saipano saloje jūrų pėstininkų batalionas užėmė pozicijas, kurias prieš tai laikė atsitraukią japonų kareiviai. Staiga šalia pratrūko kulkosvaidis. Jie papuolė į draugiškų amerikiečių pajėgų, kurie nieko nežinojo apie puolimą, ugnį. Jūrų pėstininkai nusiuntė radiogramą anglų kalba, kurioje nurodė savo pozicijų koordinatas, tačiau papliūpos nesiliovė, nes puolančios amerikiečių pajėgos manė, kad tuos pranešimus pamėgdžioja japonai, mėginantys juos apgauti. Tik nusiuntus navachų pranešimą puolantieji suprato klydę ir nutraukė ugnį. Navachų pranešimų buvo neįmanoma suklastoti, jais visada buvo galima pasitikėti.

Kalbos apie radistus šifruotojus pasklido greitai ir jau 1942 m. pabaigoje buvo užsakyti dar 83 vyrukai. Navachai tarnavo visose šešiose jūrų pėstininkų divizijose, ir kartais juos pasiskolindavo kitos amerikiečių karinės pajėgos. Neilgai truko ir navachai per žodžių karą tapo didvyriais. Kareiviai siūlydavosi panešti jų radijus ir šautuvus, jiems netgi skirdavo asmens sargybinius kartais nuo jų pačių kovos draugų apsaugoti. Mažiausiai tris kartus amerikiečiai palaikė radistus šifruotojus japonų kareiviais ir paėmė juos į nelaisvę. Navachų kodakalbius paleido tik tada, kai už juos laidavo to paties bataliono kariai.

Navachų kodas buvo neįveikiamas tik todėl, kad navachų kalba priklausė na-dene kalbų grupei, kuri visai nesusijusi su jokia azijiečių ar europiečių kalba. Pavyzdžiui, navachų kalbos veiksmažodis kaitomas ne vien asmenimis. Veiksmažodžių galūnes lemia papildinio kategorija:

ilgumas (pvz., pypkė, pieštukas), plonumas ir lankstumas (pvz., gyvatė, diržas), grūdėtumas (pvz., cukrus, druska), pluoštiškumas (pvz., šienas), klampumas (pvz., purvas, išmatos) ir įvairios kitos. Veiksmažodžiui priklauso irrieveiksmiai, kurie išreiškia, ar patyrė kalbėtojas tai, apie ką šneka, ar tai tik gandai. Taigi vienas veiksmažodis gali prilygti visam sakiniui, todėl užsienietis faktiškai niekaip nesupras jo reikšmės.

Nepaisant pranašumų, navachų kodas vis tiek turėjo du didelius trūkumus. Pirma, žodžius, kurių navachai savo žodyne neturėjo ir jie nebuvo įtraukti į 274 patvirtintų kodinių žodžių sąrašą, reikėjo išsakyti ar parašyti paraidžiui naudojant specialų raidyną. Tai užimdavo daug laiko, todėl buvo nutarta žodynėlį papildyti dar 234 plačiai paplitusiais žodžiais. Pavyzdžiui, šalims buvo duotos pravardės navachų kalba: Australija – Skrybėlė Riestais Kraštais, Britanija – Vandens Apsuptoji, Kinija – Pinta Kasa, Vokietija – Geležinė Skrybėlė, Filipinai – Plūduriuojanti Žemė, Ispanija – Avių Skausmas.

Antra problema buvo žodžiai, kuriuos vis tiek reikėjo išsakyti paraidžiui. Jei japonams būtų paaiškėję, kad žodžiai išsakomi paraidžiui, jie būtų suprastę, kad gali pasinaudoti pasikartojimų analize ir nustatyti, kokie navachų kalbos žodžiai kokias raides atitinka. Tuomet greitai būtų paaiškėję, jog dažniausiai vartojamas žodis „dzeh“ – *elk* („taurusis elnias“), atitinka raidę *e*, dažniausiai vartojamą anglų abėcėlės raidę. Vien paraidžiui išsakius Gvadalkanalio salos pavadinimą ir keturis kartus pakartojant žodį „wol-la-chee“ (*ant* – „skruzdė“) būtų beveik aišku, koks žodis atitinka raidę *a*. Buvo nuspręsta pridėti daugiau žodžių (homofonų), kurie pakeistų dažnai vartojamas raides. Du papildomi žodžiai buvo įvesti kaip kiekvienos iš šešių dažniausiai pasitaikančių raidžių (*e*, *t*, *a*, *o*, *i*, *n*) pakaitalai ir vienas papildomas žodis kitoms šešioms dažniausiai pasitaikančioms raidėms (*s*, *h*, *r*, *d*, *l*, *u*). Pavyzdžiui, dabar raidę *a* buvo galima pakeisti žodžiais „be-la-sana“ (*apple* – „obuolys“) ar „tse-nihl“ (*axe* – „kirvis“). Nuo tada Gvadalkanalį buvo galima išsakyti ar parašyti paraidžiui tik su vienu pasikartojimu: „klizzie, shi-da, wol-la-chee, lha-cha-eh, be-la-sana, dibeh-yazzie, moasi, tse-nihl, nesh-chee, tse-nihl, ah-jad“ (*goat* – „ožys“, *uncle* – „dėdė“, *ant* – „skruzdė“, *dog* – „šuo“, *apple* – „obuolys“, *lamb* – „ėriukas“, *cat* – „katė“, *axe* – „kirvis“, *nut* – „riešutas“, *axe* – „kirvis“, *leg* – „koja“).

Karui Ramiajame vandenyne smarkėjant ir amerikiečiams iš Saliamono salų veržiantis į Okinavą, navachų radistų šifruotojų vaidmuo buvo itin svarbus. Per pirmąsias Ivo salos puolimo dienas buvo išsiųsta



53 pav. 1943 m. tankiose Bugenvilio salos džiunglėse kapralas Henris Bleikas jaunesnysis (*Henry Bake Jr.*) (kairėje) ir vyresnysis eilinis Džordžas H. Kirkas (*George H. Kirk*) naudojasi navachų kodu.

daugiau kaip aštuoni šimtai pranešimų navachų kalba ir visuose – nė vienos klaidos. Pasak generolo majoro Hovardo Konerio (*Howard Conner*), „jei ne navachai, jūrų pėstininkai niekada nebūtų užėmę Ivo salos“. Kai pagalvoji, kad vykdant savo pareigas jiems dažnai tekdavo susidurti su giliai išsisknijusiomis vidinėmis baimėmis ir jas įveikti, navachų radistų šifruotojų indėlis atrodo dar svaresnis. Navachai tikėjo, kad, neatlikus apeigų su mirusiojo kūnu, mirusiųjų dvasios – *chindi* – keršys gyviesiems. Karas Ramiajame vandenyne buvo ypač kraugeriškas – mūšio laukai būdavo nusėti lavonais, o radistai šifruotojai sukaupe drąsą vykdė savo pareigas, nepaisydami juos persekiojusių mirusiųjų dvasių.

Doris A. Paul knygoje „*The Navajo Code Talkers*“ („Navachų kodakalbiai“) vienas iš navachų prisimena atvejį, kuris parodo jų narsą, atsidavimą ir savitvardą:

„Vos tik pakelsi galvą per sprindį, tau galas – tokia smarki buvo ugnis. O po kelių valandėlių išivyraudavo mirtina tyla, bet nei mūsų, nei jų pusėje įtampa neatslūgdavo. Vienas japonas, matyt, nebeištvėrė. Jis pakilo, suriko, iš visos gerklės sušuko ir metėsi per mūsų tranšėją mojuodamas ilgu samurajų kalaviju. Manau, kad prieš jam nukrintant į jį šovė kokius 25–40 kartų.

Tranšėje su manimi buvo bičiulis. Tačiau tas japonas jam perėžė gerklę iki pat balso stygų. Draugužis vis dar žiopčiojo per trachėją. O tas jo skleidžiamas garsas, kai jis kvėpavo, buvo siaubingas. Jis, žinoma, mirė. Kai japonas kirto, ranką, kuria laikiau mikrofoną, užliejo šiltas kraujas. Aš kodu šaukiausi pagalbos. Man buvo pasakyta, kad, nepaisant to, kas nutiko, praėjo kiekvienas mano pranešimo skiemuo.“

Navachų radistų šifruotojų buvo 420. Juos įvertino už narsą kovoje, tačiau ypatingas jų vaidmuo užtikrinant saugius ryšius buvo įslaptinta informacija. Valdžia uždraudė navachams kalbėti apie savo veiklą, ir jų ypatingas indėlis liko nepaviešintas. Apie navachus, kaip ir apie Tiuringą su Blečlio parko kriptanalitikais, tylėta ne vieną dešimtmetį. Galų gale 1968 m. navachų kodas buvo išslaptintas ir kitais metais radistai šifruotojai surengė savo pirmąjį susitikimą. Vėliau, 1982 m., JAV valdžia juos pagerbė ir rugpjūčio 14-ąją paskelbė nacionaline navachų radistų šifruotojų diena. Tačiau labiausiai navachų veiklą išgarsino paprastas faktas, kad jų kodas yra vienas vos iš kelių, kurio niekas niekada neįveikė. Japonijos

žvalgybos vadas generolas leitenantas Seizo Arisue pripažino, kad nors jie ir nulaužė Amerikos oro pajėgų kodą, navachų kodo taip ir nesugebėjo įveikti.

Mirusiųjų kalbų ir senovinių raštų iššifravimas

Navachų kodas tokį pasisekimą turėjo todėl, kad vieno asmens gimtoji kalba tam, kas jos nepažįsta, visiškai nieko nereiškia. Uždavinys, su kuriuo susiduria japonų kriptanalitikai, daugeliu atžvilgių yra toks pats, su kuriuo susiduria archeologai, norėdami iššifruoti seniai pamirštą kalbą, užrašytą išnykusiu raštu. Jei jau taip, archeologų uždavinys yra kur kas sunkesnis. Juk japonai nuolat girdėdavo navachų žodžius, kuriuos mėgindavo atpažinti, o informacija, kuri prieinama archeologams, kartais gali būti vos kelios molinės lentelės. Be to, dažnai archeologas iššifruotojas neturi nė menkiausio supratimo apie senovinio teksto kontekstą ar turinį – užuominas, kuriomis paprastai remiasi kariuomenės dekoduootojai, bandydami nulaužti šifrą.

Senovinių tekstų iššifravimas atrodo kaip beviltiškas siekinys, vis dėlto šiam sunkiam ir daug pastangų reikalaujančiam užsiėmimui atsidėjo ne vienas. Šią maniją kursto noras perprasti mūsų protėvių raštus, suteikiančius mums galimybę kalbėti jų žodžiais ir nors šiek tiek prisiliesti prie jų minčių bei gyvenimų. Šį potraukį šifruoti senovinius raštus geriausiai apibendrina knygos „*The Story of Decipherment*“ („Iššifravimo istorija“) autorius Morisas Poupas (*Maurice Pope*): „Iššifruoti tekstai – akinantys erudicijos pasiekimai. Nežinomas veikalas turi kažkokių kerų, ypač jei jis iš tolimos praeities, ir žmogus, kuris pirmas įmins jo mįslę, būtinai bus vainikuotas atitinkama šlove.“

Senovės raštų iššifravimas neįveikia koduotojų ir dekoduootojų kovą už būvį, nes nors dekoduootojų archeologų yra, kodų kūrėjų nėra. Kitaip tariant, daugeliu archeologinių iššifravimo atvejų raštininkas nesiekė tyčia nuslėpti teksto reikšmės. Todėl toliau šiame skyriuje, kuriame aptariamas archeologinis iššifravimas, šiek tiek nukrypstama nuo pagrindinės šios knygos temos. Tačiau archeologinio iššifravimo principai iš esmės yra tokie patys, kaip ir įprastos karinės kriptanalitikos. Iš tikrųjų ne vieną kariuomenės dekoduootoją traukia atskleisti senovinio rašto paslaptis. Turbūt todėl, kad archeologiniai iššifravimai – atgaivą teikianti permaina po karinio dekodavimo ir tikras galvosūkis, o ne karinė užduotis. Kitaip tariant, motyvuoja smalsumas, o ne priešiškus.

Pats garsiausias ir, be abejonės, romantiškiausias iš visų iššifravimų buvo Egipto hieroglifų perskaitymas. Hieroglifai šimtmečius buvo slėpinys ir archeologai negalėjo nieko kito, kaip tik spėlioti, ką jie reiškia. Tačiau klasikinis dekodavimo aspektas padėjo iššifruoti hieroglifus, ir nuo to laiko archeologai gali perskaityti pirminius šaltinius apie senovės egiptiečių istoriją, kultūrą ir įsitikinimus. Hieroglifų iššifravimas sujungė mus ir tūkstantmečiais nuo mūsų nutolusią faraonų civilizaciją.

Ankstyviausieji hieroglifai siekia 3000 m. pr. Kr., ir ši įmantri rašto forma gyvavo dar tris su puse tūkstančio metų. Nors įmantrūs hieroglifų ženklai puikiai tiko didingų šventyklų sienoms (sen. gr. kalbos žodis hieroglifas reiškia „šventi raižiniai“: sen. gr. ἱερός, *hieros* – „šventas“ + γλύφω, *glyphō* – „graviruoti / raižyti“), bet buvo pernelyg sudėtingi žemiškiems reikalams tvarkyti. Todėl kartu su hieroglifais formavosi ir hieratinis raštas – kasdien naudojamas greitraštis, kuriame kiekvieno hieroglifo ženklą atitiko stilizuotas ženklas, kurį būdavo greičiau ir paprasčiau užrašyti. Maždaug 600 m. pr. Kr. hieratinį raštą pakeitė dar paprastesnis raštas, vadinamas demotiniu: pavadinimas kildinamas iš graikų kalbos žodžio *dēmotikos* – „liaudiškas“ ir atspindi jo pasaulietišką funkciją. Hieroglifai, hieratinis ir demotinis raštai – galima sakyti, vienas ir tas pats raštas ir juos galima laikyti tiesiog skirtingais šriftais.

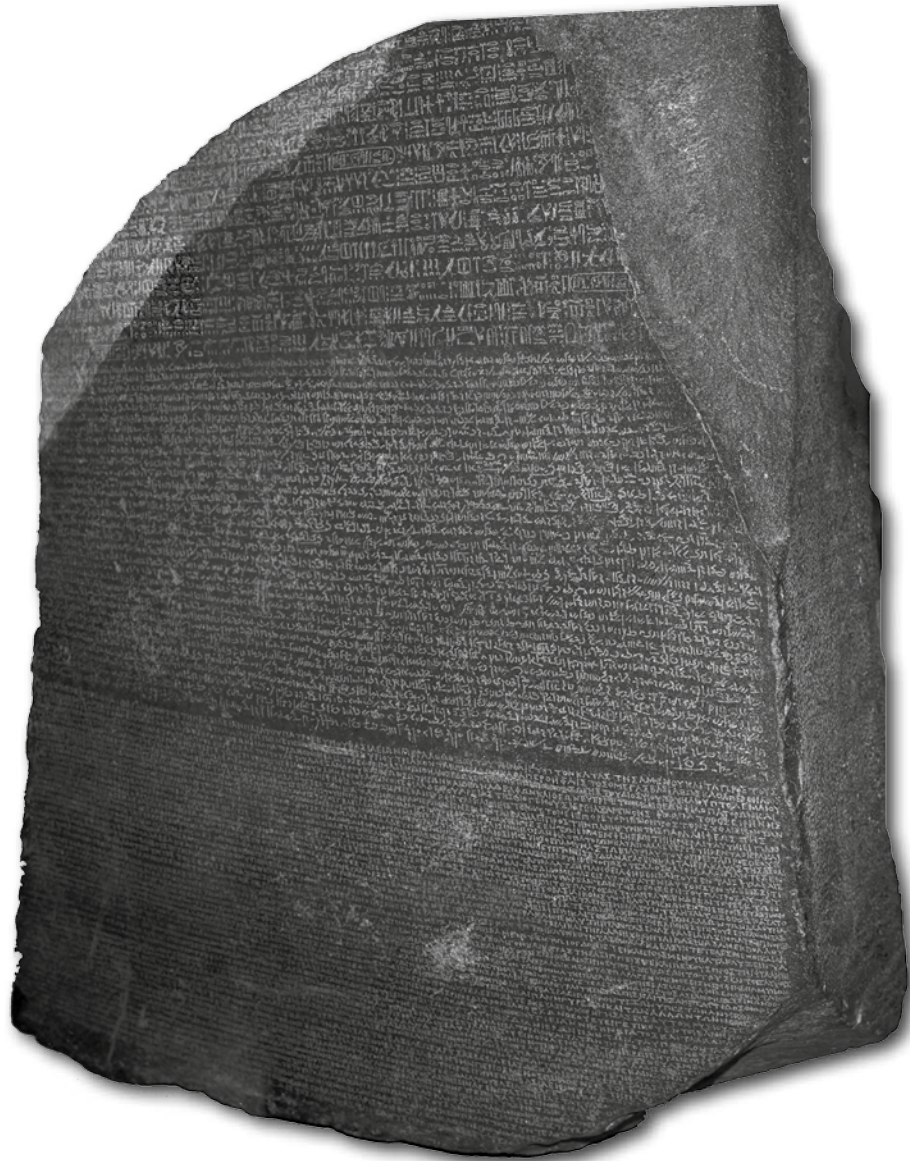
Visos trys rašto formos yra fonetinės, tai yra ženklai atitinka atskirus garsus taip pat, kaip anglų kalbos abėcėlės raidės. Daugiau kaip tris tūkstančius metų senovės egiptiečiai naudojo šiais raštais visose gyvenimo srityse – kaip mes šiais laikais naudojame raštą. Bet IV a. einant į pabaigą, sulig viena karta egiptiečių raštai išnyko. Paskutiniai datuojami senovės egiptiečių rašto pavyzdžiai rasti Filės saloje. Šventyklos hieroglifų įrašai buvo iškalti 394 m., o demotinio rašto fragmentas datuojamas 450 m. Egiptiečių raštai išnyko dėl krikščionių bažnyčios plitimo, kuri uždraudė jais naudotis tam, kad sunaikintų bet kokias sąsajas su pagoniška Egipto praeitimi. Senovinius raštus pakeitė koptų raštas, sudarytas iš 24 graikų abėcėlės raidžių ir papildytas šešiais demotiniais ženklais, naudojamais egiptiečių kalbos garsams, kuriems nebuvo atitinkamų graikų rašte, žymėti. Koptų raštas taip įsitvirtino, kad mokantieji skaityti hieroglifus, demotinį ir hieratinį raštus visiškai išnyko. Senovine egiptiečių kalba kalbėta ir toliau, tik vėliau ji išsirutuliojo į mums dabar žinomą koptų kalbą, bet tam tikru metu koptų kalbą ir jos raštą pakeitė XI a. išplitusi arabų kalba. Paskutinė kalbinė sąsaja su senovės Egipto

karalystėmis nutrūko ir žinios, reikalingos pasakojimams apie faraonus perskaityti, buvo prarastos.

Susidomėjimas hieroglifais atgijo, kai XVII a. popiežius Sikstas V pertvarkė Romos miestą pagal naują gatvių tinklą ir kiekvienoje gatvių sankirtoje pastatė po obeliską, atgabentą iš Egipto. Mokslininkai mėgino iššifruoti ant obeliskų iškaltų hieroglifų reikšmę, tačiau jiems trukdė klaidinga prielaida: niekas nebuvo pasirengęs patikėti, jog hieroglifai gali būti fonetinių ženklų ar fonogramų atitikmuo. Manoma, kad mintis apie fonetinę rašybą buvo pernelyg drąsi kalbant apie tokią seną civilizaciją. XVII a. mokslininkai buvo įsitikinę, kad hieroglifai – semagramos, tie painūs ženklai, kad šie sudėtingi ženklai išreiškėdavo visą mintį ir buvo ne kas kita, kaip primityvios piktogramos. Užsieniečiai, kurie lankėsi Egipte dar tuo metu, kai hieroglifai buvo gyvas raštas, laikėsi plačiai paplitusios nuomonės, kad hieroglifai – tai tik piktogramos. I a. pr. Kr. graikų istorikas Diodoras Sicilietis rašė:

„Taip jau yra, kad egiptietiškos raidės įgauna visokiausių būtybių, žmogaus kūno galūnių ar kokių reikmenų pavidalą, <...> nes jų rašmenys apibūdinamą sąvoką išreiškia ne skiemenu deriniu, kai vienas skiemuo jungiamas su kitu, o per išorinį vaizdą to, kas matyta, ir per metaforas kartojant įsirežia į atmintį. <...> Todėl jiems sakalas reiškia viską, kas vyksta greitai, nes ši būtybė kone pati greičiausia iš visų sparnuočių. Ir mintis apie viską, kas greita ar kam būdingas greitis, perteikiama per atitinkamą metaforinį atspaudą.“

Perskaičius tokius pasakojimus turbūt ne taip ir stebina, kad XVII a. mokslininkai mėgino iššifruoti hieroglifus kiekvieną hieroglifą suprasdami kaip atskirą sąvoką. Pavyzdžiui, 1652 m. vokiečių jėzuitas kunigas Athanasijus Kircheris (*Athanasius Kircher*) išleido alegorijų išaiškinimų žodyną „*Oedipus aegyptiacus*“ ir juo naudojosi leisdamas keistus ir stulbinančius vertimus. Kai kuriuos hieroglifus, kurie, kaip dabar žinome, tiesiog yra faraono Hofros vardas, Kircheris išvertė kaip „dieviškojo Ozyrio palankumas įgyjamas per šventas apeigas ir aukščiausias kūrybines galias tam, kad būtų įgytas Nilo palankumas“. Šiais laikais Kircherio vertimai atrodo absurdiškai, tačiau jų įtaka būsimiems iššifruotojams buvo milžiniška. Kircheris buvo ne vien egiptologas: jis parašė knygą apie kriptografiją, sukonstravo muzikinį fontaną, išrado magišką žibintą (kino pirmtaką) ir



54 pav. 196 m. pr. Kr. išraižytas ir 1799 m. atrastas Rozetės akmuo, kuriame trimis skirtingais rašmenimis (viršuje hieroglifais, per vidurį demotiniu raštu, o apačioje graikų kalba) išraižytas tas pats tekstas.

nusileidęs į Vezuvijaus kraterį pelnė „vulkanologijos tėvo“ vardą. Jėzuitų kunigas buvo plačiai pripažintas iškiliausiu savo amžiaus mokslininku, todėl jo mintys turėjo įtakos būsimų egiptologų kartoms.

Praėjus 150 metų po Kircherio, 1798 m. vasarą, kai Napoleonas Bonapartas išsiuntė istorikų, mokslininkų ir braižytojų būrį paskui besiveržiančią kariuomenę, senovės Egipto liekanos vėl sulaukė didelio dėmesio. Tie mokslininkai, arba pekinai*, kaip juos vadino kareiviai, atliko įspūdingą darbą sukartografavę, nubraižę, perrašę ir aprašę visa tai, ką matė. 1799 m. prancūzų mokslininkai susidūrė su viena garsiausių archeologijos istorijoje akmenų plokštė, kurią rado Nilo deltos Rozetės** miesto Žuljeno forte dislokuoti prancūzų kareivių daliniai. Kareiviams buvo duota užduotis išardyti senovinę sieną ir išvalyti teritoriją tvirtovės priestatui. Sienoje buvo akmuo su įspūdingais įrašais: tas pats teksto fragmentas užrašytas akmenyje tris kartus – graikų kalba, demotiniu raštu ir hieroglifais. Pasirodo, Rozetės akmuo, kaip jis buvo pavadintas, prilygo kriptanalitikų ruošiniui, visai kaip tie ruošiniai, kurie padėjo Blečlio parko dekodotojams įveikti „Enigmą“. Tekstas graikų kalba, kurį buvo galima lengvai perskaityti, iš esmės buvo tekstogramos fragmentas, kurį buvo galima palyginti su demotinio rašto ir hieroglifų kriptogramomis. Rozetės akmuo potencialiai buvo priemonė senovės egiptiečių ženklų reikšmei atskleisti.

Mokslininkai iškart suprato akmenų svarbą ir išsiuntė jį į Kairo nacionalinį institutą išsamiam tyrimui. Tačiau prieš institutui imantis rimtų mokslinių tyrimų paaiškėjo, kad puolancios britų pajėgos jau beveik sutriuškino prancūzų kariuomenę. Prancūzai pervežė Rozetės akmenį iš Kairo į palyginti saugią Aleksandriją, bet kokia ironija, kad kai prancūzai galiausiai pasidavė, pagal Kapituliavimo sutarties XVI straipsnį visos senovės liekanos Aleksandrijoje buvo perduotos britams, o buvusias Kaire leista gabenti į Prancūziją. 1802 m. neįkainojama juodo bazalto plokštė (118 cm aukščio, 77 cm pločio, 30 cm storio, sverianti apie 750 kg) prancūzų fregata „L’Egyptienne“ buvo nuplukdyta į Portsmutą, o vėliau tais pačiais metais įkurdinta Britų muziejuje, kur nuo to laiko ir yra.

Vertimas iš graikų kalbos greitai parodė, kad Rozetės akmenyje buvo užrašytas 196 m. pr. Kr. paskelbtas bendrosios Egipto žynių tarybos potvarkis. Tekste surašytos malonės, kurias faraonas Ptolemajus suteikė Egipto liaudžiai, ir smulkiai surašyti garbės ženklai, kuriais atsidėkodami

* Pekinų veislės šunys.

** Dab. ar Rašidas, miestas Egipto šiaurėje.