DŽEJMS KONOR

ČITANJE SKRIVENIH PORUKA U SAJBER-PROSTORU: SEMIOTIKA I KRIPTOGRAFIJA

U svojim ranim danima Fi Beta Kapa pomalo je oponašala tajna društva. Osnivačko telo iz Viljemsburga je 1780. poslalo povelju Harvardu kojom se tražilo da "sva prepiska ide preko predsednika svakog društva i to primenom ovde priložene tablice". Tablica, kriptografska shema od 13 recipročnih supstituta, bila je prilično standardna, jednostavna, ne naročito teška za shvatanje, a ipak je, samim svojim postojanjem, demonstrirala fascinaciju kriptogramima i tajnim šiframa. Predsednik harvardskog ogranka poslao je 23. marta 1782. predsedniku jelskog šifrovanu poruku koja je počinjala sa IZ BUGZ BPWX ZUNDWZXB FHHFNBARWBG, u prevodu "najranije što smo mogli...". U suštini, pismo je najavljivalo osnivanje harvardskog ogranka i pozivalo jelski ogranak da im se pridruži "u prednostima književne prepiske". Čovek bi se normalno upitao šta će 'književnoj prepisci' šifrovanje, ili da li je Fi Beta Kapa imala tajne za čije čuvanje je bio nužan sistem šifrovanja. Takva pomisao, međutim, ne uzima u obzir zavodljivost tajnosti i moć tajne da formira zajednice. Po Dejvidu Kanu (David Kahn) (772), članovi Fi Beta Kape su u to vreme napravili poentu od svoje kriptografije. Predsednik jelskog ogranka je s puta jednom pisao harvardskom odeljku, žaleći se: "moram primetiti da sam sada napisao mnoge stvari koje je trebalo napisati po t(ablici), ali zaboravio sam da

je ponesem kad sam napuštao N. Heven i nisam u mogućnosti da se njome poslužim".[1]

Ne znam da li je bilo ikakve praktične koristi od Fi Beta Kapine šifrantske tablice, ili je bila tek onovremena afektacija. Sumnjam na ovo drugo, pošto su tajna društva bila u modi. Ipak, ima nešto zavodljivo u umeću skrivanja poruka, nešto iznad uobičajene erotike čuvanja tajni. Zamislite da držite šifrovano pismo predsednika jednog Fi Beta Kapa ogranka drugome; bez šifrantske tablice poruka izgleda besmislena, a ipak znate da ima neko značenje, zakopano negde u svom tom besmislu. Značenje nedostupno pukom gledanju.[2]

Poriv da se sakrije značenje u tekstovima skoro da je star koliko i samo pisanje. Egipćani su imali običaj da obriju glave robovima, ispišu poruke na njihovim golim lobanjama i, kad im kosa opet izraste, pošalju ih u strane zemlje kao tajne kurire.[3] Julije Cezar običavao je da šalje šifrovane poruke u kojima je svako slovo bilo tri mesta naniže pomereno u abecedi. Samo je general od poverenja koji je znao za trik mogao da pročita poruke. Ono što ovde tvrdim je,

1 Kanova obimna istorija kriptografije jedno je od velikih dela u toj oblasti. Preporučujem je svakome koga zanima da sazna više o toj stvari. Kanov argument je da su tajnost i šifrovanje svojevremeno bili pitanje stila u akademskim krugovima.

2 Tu zavodljivost upoređujem s nekom vrstom šapata. Kad ne bi znao da tekst ima značenje, izgledao bi mu besmisleno i izgubio bi svaku moć nad čitačem. Ako čitač, s druge strane, zna za poruku skrivenu šifrovanjem a ipak ne može da je pročita, tekst ima zavodljivu moć nad čitačem, mučeći ga misterijom koju treba da reši, zagonetkom koju treba da odgonetne. To liminalno svojstvo teksta, nešto između značenja i besmislice, daje mu moć.

3 Prema Džulijanu Bjelevicu (Julian Bielewicz), *Secret Languages* (Tajne jezika), jednu od prvih rasprava o kriptografiji napisao je Aeneas Tacticus, Grk koji je živeo i pisao oko 100 godina posle Termopila (480 p.n.e.). U njoj je opisao većinu ranih grčkih kodova. Modernu matematičku osnovu šifrovanja razvili su Arapi, naslednici grčke i rimske nauke. U stvari, reč *cipher* je originalno arapska reč. Moderno umeće šifrovanja, međutim, svoje početke ima u renesansi, u okrilju rastuće moći nacionalnih država. Zaveru Meri, kraljice Škotske, za ubistvo Elizabete I otkrio je njen državni sekretar ser Frensis Volsinhem (Francis Walsinham) kad su njegovi agenti uspeli da dešifruju tajna pisma koja je Meri slala svojim agentima.

zapravo, da je umeće skrivanja poruka direktna implikacija umeća pisanja, pošto pisanje stvara trenutno odsustvo. Nije to vrsta odsustva o kome sada govori književna teorija (to jest, "nestajanje autora" kao takvog), već nešto neuporedivo osnovnije. Tip odsustva o kome govori književna teorija zapravo je proizvod vrste odsustva o kojoj ovde pišem. U stvari, cela poenta pisanja je u tome da ja, pisac, mogu fizički da budem uklonjen sa scene onog časa kad su moje ideje zapisane. Ne moram da budem u prostoriji da bi se one pročitale. Izgovorena reč, kao što je istakao Valter Ong (Walter Ong) (32) čili već dok se izgovara. Ona živi od sekunde do sekunde i zahteva fizičku prisutnost govornika. S druge strane, napisano ostaje. Zato kad jednom kodiram govor u niz znakova, više nisam potpuni gospodar svog govora.[4] Pisanje, moje pisanje, može da pročita bilo ko dugi posle moje smrti, neko ko nije bio ni rođen za mog života. Ako u govoru želim da sačuvam tajnu, dovoljno je da nekog povučem na stranu, šapnem u njeno ili njegovo uvo i onda ćemo samo ta osoba i ja znati šta je rečeno. To je jednostavno stvar kontrole glasnosti, uz malo poverenja da će osoba kojoj je rečena, sa svoje strane, čuvati tajnu. Međutim, u pisanju svako kome dođe do ruku to parče papira, može da ga pročita. Kako da sačuvam svoju tajnu? Kako da sačuvam kontrolu nad vlastitom komunikacijom, ako mi je to potrebno?

O svemu tome raspravljano je na drugom mestu i nije potrebno da to ovde podvlačim. Važno je to što je kriptografija neposredna implikacija te činjenice. Jedini način da svoju komunikaciju učinim sigurnom, na primer u ratu ili diplomatiji (ili pismima jednog Fi Beta Kapa ogranka drugome) je ili da sakrijem tekst (možda na lobanje egipatskih robova) ili da sakrijem značenje (kao što je radio Cezar). Ova druga tehnika pokazala se korisnijom. U pisanju, biram niz znakova koji zamenjuju moj govor. Izbor je istovremeno racionalan i proizvoljan: racionalan, jer počiva na kulturno stvorenim pravilima, a proizvoljan, jer su pravila jednostavno zasnovana na prethodno proizvolj-

4 Nije uvek bilo tako. Po mišljenju Anri-Žana Martena (Henri-Jean Martin) (67), antički grčki i rimski tekstovi bili su namenjeni čitanju naglas. Do raskida veze između pisane i izgovorene reči došlo je postupno, a u potpunosti neko vreme po pronalasku štampanja.

nim pravilima. Nema ničeg nužnog u jednom skupu pravila u odnosu na neki drugi. I šifrovanje funkcioniše na vrlo sličan način. Jednostavno uzmem jedan proizvoljan skup pravila, kao što je uradio Julije Cezar, da ih primenim na slovima moga teksta. Mogu da premestim slova tri mesta niže u abecedi, ili pet mesta, ili dvadeset mesta manje četiri mesta. Ako samo vi i ja znamo koja su pravila izabrana, onda samo vi i ja možemo da pročitamo tekst. Otuda, opet, zavodljivost. Ista moć da prenosim ideje, značenja i zvuke preko jedne mreže vizuelnih znakova omogućava mi da sakrijem te iste ideje, značenja i zvuke. Što tekstualnost otkriva, tekstualnost i sakriva. U tom smislu, šifrovanje je sistematski inhibitor čitanja. Ono čini tekstove nečitljivim, i to čini sistematično, to jest, uz pomoć racionalnih postupaka i matematičkih algoritama.

Dakle, to što imamo u kriptografiji je tekstualna igra, igra koja je izazov za čitača. Pročitaj me ako možeš, kaže ona. Pravila igre, metode korišćene u stvaranju šifrovanog teksta (koji se čita kao besmislica) uvek imaju element matematike u sebi. Kad je Julije Cezar pomerao slova u svojim porukama za tri mesta koristio je matematički koncept. Taj matematički element bivao je sve složeniji tokom vekova, s velikim skokom u doba renesanse, da bi u naše vreme algoritmi, matematička pravila postali toliko komplikovani da je za njihovo korišćenje potreban kompjuter velike brzine, ili niz kompjutera velike brzine. Ono što tvrdim jeste da, mada smo navikli da o kriptografiji mislimo kao o igri za matematičare, u osnovi ona je, još uvek igra s tekstovima. To je igra pisanja i čitanja i pravljenja poruka nečitljivih jednima ali ne i drugima. To je igra moći i ekskluzivnosti, transformisanja tekstova iz jedne stvari, *alakazam!* u drugu, i obrnuto.

Ovo poglavlje spaja nekoliko specijalnosti i povezuje tehnologiju šifrovanja sa procvatom World Wide Web-a. Web vidim kao ogromnu livadu na kojoj se informacije plaste u ogromne stogove kao seno, nekad se prenose napred-natrag, nekad gomilaju ovde, nekad onde. Razni ljudi poseduju delove livade, ali retki su koji imaju zaštitu za svoje informacije. Međutim, kako raste cena sena, rašće i potreba za ogradama i kapijama s bravama. Tehnologija šifriranja je važan oblik ograde i kapije na Web-u. Zasnovana je na tekstu, utoliko što digitalne tekstove čini nečit-

ljivim, digitalne zvuke nedostupnim sluhu, digitalne slike nerazgovetnim. A kako je sve što se kreće ovamo-onamo po Web-u u digitalnoj formi, sam Web bi se mogao nazvati "prijateljsko šifrovanje". Sve što se stavi na Web može da bude šifrovano i vremenom će sve češće i biti.

Najbolje ćemo skupiti sve ove različite niti uz pomoć semiotike, "nauke o znacima". Ako se jezik može objasniti kao mreža znakova i simbola, onda bi se, unekoliko, i svet mogao "čitati" kao tekst. Razumeti svet znači tumačiti njegove znake. Ova verzija lingvističke teorije sasvim je primenljiva za objašnjenje WWW-a koji je, sa svoje strane, mreža povezanih tekstova. Za primenu ću se osloniti na semiotičku teoriju Umberta Eka, jer je njegovo shvatanje semiotike najprimerenije raspravama o tehnologiji. Ovde je metod pre šetnja no marš, posredovanje kroz lavirint ideja koji vodi jednom jedinom zaključku: tehnologija šifrovanja postaje sve važniji deo našeg sistema elektronske komunikacije. Sve doskora, bila je klasifikovana kao municija i imala je tretman supertajnog ratnog oružja. Sad je gotovo obična. Oni među nama koji se bave izučavanjem jezika u elektronskom dobu, valjalo bi da nauče ponešto o njenom funkcionisanju.

Sajber-prostor je zaista čudan. On postoji u neposrednoj blizini onoga što je Poper nazivao trećim svetom (106). Poperov prvi svet je svet objekata, stvari-negde-izvan, koje stoje na neki način suprotstavljene subjektu; svet subjekta, ideja u svesti, je drugi svet. Treći svet je svet fizičkih reprezentacija ideja, tekstova, govora, ideja koje svoje poreklo imaju u drugom svetu a ipak postoje na istom nivou kao prvi. Sajber-prostor je neobičan čak i pod ovom svetlošću. Pošto nema egzistenciju kakvu ima hartija s tekstom, bliži je misli nego knjizi. A ipak je prostor u kome postoji neka vrsta figurativnog kretanja. U WWW-u (koji nije istinski potpun sajber-prostor, kakva bi trebalo da bude sasvim virtuelna realnost), položaj u prostoru nije geometrijski nego logički. Veze se uspostavljaju na osnovu (a) kategorija predmeta, kao na Yahoo-u, Lycos-u ili ma kom drugom pretraživaču; i (b) metaforičkim vezama, kao u hipertekstualnoj fikciji. U ovom drugom slučaju, reči imaju implikacije u okvirima sistema teksta, a implikacije grade i podržavaju vezu s drugim rečima i frazama, i slično.

Pošto je WWW globalna mreža hipertekstualnosti od svega što imamo najbliža sajber-prostoru, ona je i jedini aktuelni model koji imamo. Sačinjen je od tekstova, URL-a (čvorišta), veza i tako dalje, koji su tek delom vezani za stvarni životni prostor. Dva servera mogu biti na različitim kontinentima, ali između sajtova na njima nema prelaznih punktova. Linkovi su bukvalno trenutni i, kao takvima, ne treba im "putovanje" da stignu od jednog do drugog. Kliknem na linkovani tekst i izleće linkovana stranica. Benedikt je tvrdio (126) da se i fizički i sajber-prostor mogu definisati u kategorijama slobode kretanja. On je istakao sedam načela prostora (132) koje svaki sajber--prostor prepoznatljiv kao model životnog "stvarnog" prostora nužno mora da sledi.[5] U, na hipertekstu zasnovanom sajber prostoru kakav je Web koji se više oslanja na Hypertext Markup Language (HTML) nego na Virtual Reality Markup Language (VRML), kretanje u prostoru stvar je sleđenja linkova od čvorišta do čvorišta, od teksta do teksta. Mesto u sajber--prostoru je, pak, karakter čitanog teksta. U tom smislu, Web prostor ne bi bio pravi izraz sajber-prostora o kome govori Benedikt jer krši neka od njegovih načela.[6] Dva čitaoca mogu u isto vreme da čitaju istu Web stranu bez ometanja, pa bi takva ideja mesta u prostoru kršila njegovo načelo ekskluzivnosti, koje u osnovi glasi da *dva objekta ne mogu zauzimati isti prostor u istom vremenu*. Ali ako je mesto uglavnom stvar tekstualne a ne fizičke lokacije, onda načelo ekskluzivnosti ne bi važilo. Osim toga, krećući se od jednog do drugog čvorišta, surfer po Web-u ne putuje kroz prolazne punktove, već skače sa sajta na sajt. To bi kršilo Benediktovo načelo tranzita, po kom je bitno da putovanje kroz prostor od jedne do druge tačke mora da prođe sve prolazne punktove. Dakle, Web nije sajber-prostor u punom Benediktovom smislu, a ipak u njemu postoji sloboda kretanja. Kre-

5 Mislim na Web kao na nepotpun sajber-prostor, jer on ne ispunjava mnoga od Benediktovih pravila pravog modela prostora. Drugim rečima, u njemu kao tekstualnom prostoru čitač skače s teksta na tekst, ali ne prolazi kroz međutačke. Čitač ne 'putuje' onako kako bi se putovalo u potpuno operacionalnoj virtuelnoj realnosti.

6 Benediktovi principi su sledeći: princip ekskluziviteta, princip maksimalnog ekskluziviteta, princip indiferencije, princip skale, princip tranzita, princip lične vidljivosti i princip učestalosti.

tanje je sličnije okretanju strana knjige, ili kretanju od jedne do druge knjige u biblioteci. Do inhibicije kretanja može da dođe na nivou linkova kada se ne može ući na neki server bez ispunjenja uslova bezbednosti, kao u Fire Wall bezbednosnom sistemu, ili na nivou teksta, kao kod šifrovanja.

Stoga je kretanje po Web-u, bar delom, funkcija čitanja. Kultura postavlja pravila čitanja, načine na koji tekst dobija smisao za mene. Ne mogu da čitam tekstove koji krše pravila čitljivosti koje je ustanovila kultura. Svaka kultura ima svoja pravila, čineći tako svoj jezik neprozirnim za druge kulture. Međutim, kod šifrovanja imam tekst koji sistematično krši pravila svih kultura, koji se ne može čitati ni u jednom kulturnom kontekstu, pošto su slova namerno šifrovana tako da izgledaju kao besmislica. Sve dok ne znam skriveno pravilo šifrovanja tog teksta, neću biti u stanju da ga pročitam. Tako šifrovanje postaje nužni deo svakog informatičkog prostora kao što je Web, delujući kao neka vrsta vrata, zida, brave i ograde unutar sajber-prostora. Ono to čini menjajući odnos teksta prema kulturi koja ga je stvorila.

Što se osetljivije informacije budu prenosile Web-om, kao što je slučaj s digitalnim novcem ili ličnim medicinskim dosijeima, rašće potreba za zaštitom tih informacija. Zato će i tehnologija šifrovanja postajati sve važnija. Ona je već uobičajenija no što bi mnogi ljudi pretpostavili. Većina kompjutera ima ugrađene algoritme za šifrovanje. Ulazak u Mrežu zahteva lozinku, koja je često varijanta ključa za dešifrovanje.[7] Kad god se s jednog na drugi kompjuter preko Interneta šalje neka lična informacija, kao što su imena i adrese, brojevi kreditnih kartica i socijalnog osiguranja, ta informacija mora da bude šifrovana iz razloga sigurnosti. Ako je transfer bez sigurnosnih mera, često izleće poruka na ekranu koja pošiljaoca

7 Jedna od sadašnjih kontroverzi oko Web-a je u tome što ne postoje standardi šifrovanja, što ima mnogo različitih tipova šifrovanja i da svaki špijun ili lopov s dovoljno sofisticiranom opremom za 'njuškanje' može da se domogne nečijih brojeva kreditne kartice. Otud i sve veća potreba za novim standardom šifrovanja, što nas vodi tekućoj raspravi o Clipper čipu u kojoj Klintonova administracija i, naročito, potpredsednik Gor, predvode pokret za usvajanje novog "jakog" standarda šifrovanja koji ne samo što će obezbediti sigurnost na Web-u, već i dati vladi "zaklopna vratanca" za pristup celokupnoj šifrovanoj komunikaciji.

opominje da linija nije sigurna te da stoga informacije mogu biti predmet presretanja ili zloupotrebe. S nekoliko sajtova na Web-u može se skinuti Pretty Good Privacy (PGP), "moćan" program za šifrovanje koji se zasniva na toliko složenom algoritmu koji čak ni najbrži današnji kompjuteri ne mogu lako da provale. Program je besplatan i dostupan svakom ko ga želi. Šifrovanje, dakle, ima brojne implikacije na osećaj ja i ličnog identiteta u informatičko doba. Zar u takvom dobu, moja lična informacija – medicinski dosije, finansijsko stanje, porez, i slično – nije deo mog ličnog identiteta? Koliko puta nedeljno mi traže moj broj socijalnog osiguranja? Čitavog života me proverava, kontroliše, analizira više agencija i korporacija nego što mogu da izbrojim. Smešten sam u kategoriju kupca, starosnu grupu, rasnu, rodnu, po obrazovnom nivou, kreditnoj istoriji. U određenoj meri, te informacije čine moje ja u okvirima moje vlastite kulture. Ko ih kontroliše ima veze s tim ko mene kontroliše.

Čitanje

Pisanje postoji na onome što je Umberto Eko nazvao nivoom "šifara" (*The Role*, 48-49) na kom je plan sadržine u korelaciji s planom ekspresije. To znači da pisanje uzima ono što ja želim da kažem, ideje u mojoj glavi, i stavlja ih u korelaciju sa sistemom oznaka koje mogu da zabeležim na parčetu papira. U kineskim ideogramima, složene ideje često su u korelaciji sa individualnim likovima. Recimo ideja "dobro" piše se kao lik žene koju prati lik deteta. "Dobro" se, dakle, opisuje kao majka i dete. Ono implicira "mir", "smirenost" i slično. Kao što je istakao Logan (19-20), zapadna azbuka više dovodi u korelaciju znake sa zvucima nego s idejama. Ona šifruje govor pre nego pojmove. Pojmovi se na strani javljaju kao faksimil izgovorenih reči.

Šifrovanje, kao što je istakao Eko, može ne biti ni u kakvoj korelaciji sa realnim svetom. Zato ga je nazvao znakovnom funkcijom a ne znacima. On je u *Travels in Hyperreality* (14) pisao o muzeju voštanih figura koji je jednom posetio u Kaliforniji, u blizini Diznilenda. Tamo je bila izložena kompletna rekonstrukcija budoara Marije Antoanete, tačna do poslednjeg detalja, na istoj turi sa isto toliko detaljnom rekonstrukcijom Alisinog susreta s Ludim šeširdžijom. To što budoar Marije Antoanete ima istorijski original, a čajanka Ludog šeširdžije je postojala je-

dino u pričama, filmu i animaciji, bilo je irelevantno. Znakovne funkcije zajedno su radile na stvaranju iskustva, bilo ono istinito ili ne.

Ali, nije li to normalno stanje jezika? Često uzimamo da jezik postoji da bi se govorila istina, ali nije li to pre ideološka pretpostavka nego pretpostavka zasnovana na iskustvu? Deci, na primer, često treba vremena i truda da shvate razliku između "stvarnih" i "izmišljenih" ljudi. Mali sin mog prijatelja je, posle gledanja crtane verzije *Lepotice i zveri*, odlučno rekao ocu da je odmah znao da su Lepotica i Zver stvarni ljudi, a Svetiljka i gospođa Šerpa samo ljudi iz priče. Potrebna je određena količina sofisticiranosti da se jezik poveže s realnim svetom, dok je često sasvim lako, čak i prirodno na nekim nivoima razvoja, povezati jezik s fikcijom. Stoga, znakovne funkcije obuhvataju i uključuju svetove fikcije i stvarne svetove i dovoljno često se odnose na realnost stvarajući korisne fikcije o njoj. Čini se, dakle, da smo na terenu kulture.

Vrednost jezika je delom u njegovoj moći da izazove verovanje u vezu između znaka i nečeg realnog u meri da se onaj koji veruje ponaša na odgovarajući način. Jezik menja stvari podstičući stanje verovanja, koje opet podstiče akcije koje menjaju svet. Znaci funkcionišu u kulturi, a u toj kulturi postoje činjenice, mitovi, bajkovite priče, želje, nade, snovi, strasti i potpune laži. Kultura je, stoga, šira od istina koje sadrži. Kultura se može tačnije definisati sistemima verovanja koje sadrži i pričama koje priča, nego istinama koje možda obuhvata. Kulture se, dakle, mogu čitati kao sistemi znakovnih funkcija baš kao što se i tekstovi mogu čitati kao sistemi znakovnih funkcija. Za Eka je pozadina koja to čini mogućim laž ili, možda manje bezobrazno, fikcija. Znakovne funkcije su posuda koja sadrži komunikaciju. Sve što se može upotrebiti za prenošenje nečeg što nije istina, može se upotrebiti i za prenošenje nečega što jeste istina.

Šifrovanje funkcioniše na analogan način. Međutim, baš kao što su laži i fikcije pozadina iza koje znakovne funkcije govore istine, besmislica je pozadina iza koje šifrovanje prenosi smislene poruke. Šifrovati poruku znači inhibirati čitanje i kontrolisati čitalačku publiku. To je kontrola na semiotičkom nivou, pošto je komunikacija osujećena na nivou tipografije. Kad je predsednik harvardskog odeljka pisao predsedni-

ku jelskog ogranka Fi Beta Kape, pismo je počinjalo sa IZ BUGZ....

Mnogo razvijenije kompjutersko šifrovanje zapravo razbija kucani tekst tako da su čak i slova šifrovana. Čitava kriptografija je, dakle, niz manipulacija znakovima. Prema Šnajeru (Schneier), nešifrovana poruka je *razumljiv tekst* ili *čist tekst*, a proces skrivanja poruke je *šifrovanje*. Šifrovana poruka naziva se *ciphertext*, dok je proces vraćanja ciphertext-a u razumljiv tekst *dešifrovanje*. Razumljiv tekst je, dakle, čitljiva poruka, dostupna svakome ko može da čita jezik na kom je napisana. To je poruka pre i posle šifrovanja i dešifrovanja, koji se obavljaju uz pomoć ključa koji je, po sebi, komad kompjuterskog teksta koji obezbeđuje operater, u većini slučajeva kompjuter, s informacijama potrebnim za dešifrovanje poruke.

Šifrovanje se razlikuje od kodiranja: drugo funkcioniše na nivou reči, a prvo na nivou slova. U kôdu možete da pročitate pismo navodnog dvostrukog agenta njegovoj babi u Grin Beju. U njemu se govori o divnim plavim čarapama koje mu je poslala za Božić. "Plave čarape" bi se, u ovom slučaju, na osnovu prethodnog sistema zamene, mogle čitati kao "rampe za nuklearne projektile". Šifrovano pismo bi, naravno, izgledalo kao besmislen govor. Kôd bi, u originalnom značenju reči, bio eksponencijalno jednostavniji od šifre, pošto je broj mogućih kombinacija na nivou azbuke eksponencijalno veći nego na nivou reči. Što su jedinice manje, veća je mogućnost skremblovanja. Ako imate slagalicu od samo četiri komadića, to nije nikakav izazov. Ali ako imate slagalicu od hiljadu komada, interesovanje raste. Ako su komadići iste veličine, postaje jasno da što je manja jedinica podele, potreban je veći napor za ponovno sklapanje. Ovo je veoma važna poenta jer, kako ja to vidim, kriptografski algoritmi su uglavnom neprovaljivi zbog svoje složenosti, što povećava količinu rada potrebnog za pronalaženje ključa pre no stvar postane zaštićena. Kriptografska korisnost algoritma uglavnom zavisi od rada uloženog u proizvodnju znakova. Stoga bi radna definicija *kriptografije* koja bi nam ovde koristila bila da je to poduhvat ponovne proizvodnje (re-production) znaka. To je umeće i nauka skrivanja razumljivog teksta sistematičnim skremblovanjem izraza teksta, tako da razumljiv tekst mogu da obnove jedino oni koji imaju ključ za njegovo ponovno pretvaranje u razumljivi tekst.

Čitanje znakova

Praktičari semiotike, "nauke" o znacima, upućuju na De Sosirov *Kurs opšte lingvistike* kao početak njihove discipline, iako su mu prethodili radovi Č.S. Pirsa (C.S. Pierce) i Čarlsa Morisa (Charles Morris) s kraja 19. veka. Po De Sosirovom shvatanju koje se većinom zasnivalo na njegovom istraživanju odnosa govora i pisanja, znak je definisan kao tačka susretanja između oznake, izraza koji obavlja reprezentaciju, i označenog, stvari koja je reprezentovana. Čak i kad oznaka ima svojstva označenog kao u onomatopeji, to ne mora da bude slučaj i, zapravo, najčešće i nije. U stvari, odnos između oznake i označenog je arbitraran, stvar konvencije, pa čak i u slučaju reči kao što su "beng" ili "plop" koje imaju neka od svojstava označenog, izbor tih izraza a ne nekih drugih stvar je kulturne istorije a ne semiotičke nužnosti.

Kako već biva sa svim intelektualnim stvarima i semiotika se, od objavljivanja *Kursa opšte lingvistike* podelila. Prvi pravac kojim dominira misao Rolana Barta (Roland Berthes) u osnovi je humanistički, a u metodologiji imitira književnu kritiku. U *Elementima semiologije* (11) Bart tvrdi da je "Možda zbog toga semiologija osuđena da se utopi u *translingvistiku* čiji materijal mogu da budu mit, narativ, novinarstvo ili, s druge strane, objekti naše civilizacije ukoliko su *izgovoreni* (u štampi, prospektu, intervjuu, razgovoru i možda čak unutrašnjem jeziku, kojim vladaju zakoni imaginacije)."

Po ovom shvatanju, semiologija ne liči toliko na nauku koliko na humanističku analizu izraza, izgovorenog ili napisanog, viđenog kao izraz izgovorenog.

Drugi pravac oličen u delu Umberta Eka, posebno njegovoj *Teoriji semiotike* i *Ulozi čitača*, izučavanje je znakova kao reproduktivnog sistema. Zbog toga su Ekove ideje primerene istraživanju tehnologije. Ako se sistemi znakova mogu reprodukovati, oni imaju šta da nam kažu o tehnološkom svetu koji se sav vrti oko izrade, reprodukovanja do tačke od koje se vrti u glavi. Ekova analiza počiva na teoriji informacija. *Teorija semiotike* počinje iscrpnom raspravom o funkcionisanju brane. Nivo vode šalje različite signale operateru koji diže i spušta branu zavisno od primljenog signala. To je, kaže Eko, osnov kodirane komunikacije. Bart je bio usredsređen na znake kao ljudsko delo; Eko je mehaničke signale uveo kao deo

semiotičkog sveta. To je od velike važnosti za novi univerzum elektronske komunikacije u kojoj se dva nivoa komunikacije odvijaju istovremeno – komunikacija između ljudi i komunikacija između mašina. U stvari, moglo bi se reći da prva jaše na drugoj.

Kao što je već pomenuto, za Eka je odnos koji postoji između oznake i označenog – znakovna funkcija. One su arbitrarne, bez nužne veze s činjenicama; više su materijal priča nego istina. Kulturne konvencije su, dakle, nosioci po kojima govorimo, pišemo i programiramo naše kompjutere. Svi znaci su deo mreže tumačenja, a sva čitanja proces asocijacije znakova s drugim znacima posredstvom kulturnih konvencija. Tako su znaci međusobno povezani kulturnim konceptima pomoću kojih ih čitamo. Ubacivanjem kulturnih konvencija Eko, kako kaže Olso (71–73), stvara sistem koji "omogućava srazmerno specifično i ponovljivo raspravljanje o znacima, njihovim međusobnim odnosima i socijalnim reakcijama na njih".

Ovo poslednje je najkorisnije za izučavanje kriptografije, pošto su znaci usađeni u sisteme povezane kulturnim konvencijama i kulturno uslovljenim obrascima tumačenja. Kao što je već rečeno, u kriptografiji se radi o tome da se tekstovi učine nečitljivim. Ona to čini kidanjem veza između sadržaja i izraza, samim tim i kidanjem veze između znaka i kulturnih konvencija pomoću kojih se on razumeva. Ako mogu da ubacim skup skrivenih pravila razumevanja teksta između samog teksta i čitača tog teksta, imam kontrolu nad tekstom. Šifrovanjem izmeštam tekst iz mreže kulture. I više od toga, da bih imao efikasnu kontrolu nad tekstom, moram ga odvojiti od svih kulturnih konteksta. Sve manje od toga ne bi bilo šifrovanje već prevod. Tekst moram da učinim nečitljivim za svakog, u svakom referentnom okviru, bez primene ključa koji samo ja posedujem. Prosto rečeno, IZ BUGZ BPWX ZUNDWZXB FHHFNVARWBA nečitjivo je na svim jezicima sveta. Njegov horizont, njegova pozadina je besmislica. Tako, koristeći šifriranje, posedujem sam tekst. U stvari, šifriranje je možda jedini način da se tekst zaista poseduje. Autorstvo je neodređeno, autorska prava prolazna. Osim toga, u činu čitanja, čitač preuzima tekst i polaže pravo na njega. Jedino šifrovanjem tekst može da ima značenje i da u isto vreme bude lišen svake mogućnosti čitanja. Sve dok interesovanje potencijalnih čitača ne zgasne, to mi daje znatnu moć.

Proizvodnja znaka i rad

Na početku drugog dela *Teorije semiotike* (151) Eko piše:

"Šta se događa kad proizvodim znak ili niz znakova? Pre svega moram da obavim zadatak u smislu čisto fizičkog napora, jer moram da 'iskažem'. Iskazi se obično smatraju emitovanjem zvukova, ali bi se pojam mogao proširiti tako da se 'iskazima' smatra svako proizvođenje signala. Tako, dakle, iskazujem kad crtam lik, činim svrhovit gest ili proizvodim objekt koji, osim svoje tehničke funkcije, teži da komunicira nešto."

U svakom slučaju, dakle, komuniciranje zahteva neki oblik rada, neki oblik svrhovito utrošene energije. Iz tog rada ishodi proizvod, rezultat, čak artefakt. Ovo shvatanje, pod uticajem evropskog marksizma, vidi znake gotovo kao finalni proizvod pokretne trake, za čiji nastanak su potrebni ljudska invencija, inteligencija i prefinjenost.

Eko pominje (153-156) jedanaest vrsta tipova rada potrebnih za proizvođenje znakova, koji su svi uključeni u svaki čin komunikacije ili implicirani njim.[8]

8 Ekovih 11 tipova rada su sledeći:
1. fizička proizvodnja signala;
2. rad na formiranju jedinice izraza (npr. rad uvažavanja svih kulturnih zakona formiranja razumljivih kodova);
3. rad na stvaranju novog kôda u okviru kulture (npr. koji na novi način dovodi u korelaciju izraz i sadržinu);
4. rad (pomenut kao tip 2) utrošen kad i pošiljalac i primalac nastoje da poštuju sva kulturna pravila (npr. rad uložen kad dvoje ljudi u razgovoru nastoje da poštuju pravila komunikacije koja važe u toj kulturi);
5. rad uložen da bi se promenio kôd u okvirima neke kulture (npr. rad uložen da bi se promenio deo jezika);
6. rad retoričkog i ideološkog diskursa;
7. rad uložen u pokušaj da se interpretira neki tekst složenim procesom zaključivanja;
8. rad uložen kad dvoje ljudi nastoje da razumeju iskaze jedan drugog i artikulišu iskaze koji su razumljivi, koji zahteva i semiotičke (jezičke) sudove i činjenične sudove;
9. rad uložen da bi se utvrdilo da li se iskazi odnose na neko postojeće stanje stvari u svetu (npr. da li jezik planira neko stanje stvari);
10. rad utrošen da bi se razumeli iskazi u odnosu na kodirane ili nekodirane okolnosti (npr. okolnosti koje nadilaze same iskaze);
11. rad koji pošiljalac ulaže da bi privukao pažnju primaoca.

Tako je rad, kako je ovde definisan – rad ekspresije, rad ekspresije na smislen način (to jest, u okviru kulturnog konteksta), i rad tumačenja – deo proizvođenja znakova, smislenog iskazivanja unutar kulture. Ti individualni znaci stoje na leđima kulturnih pravila šifrovanja, tradicionalnih načina povezivanja sadržine sa izrazom, od azbuka do gramatičkih pravila i tradicija uličnog žargona.

Kao što je već rečeno, šifrovanje je tekstualna igra, vrsta ogromne akrostike koja teži da uspostavi kontrolu nad različitim tekstovima. Ta igra se, međutim, igra u širokom društvenom krugu. Kao što je Šnajer istakao (4), projekt kriptologije kao takav podrazumeva postojanje neprijatelja. Kao u šahu ili savršenom plesu, stručnjak za šifrovanje smišlja algoritme, protokole i slično, s jednim okom na potencijalnim napadačima, uljezima, prepadačima, neprijateljima, itd. U stvari, šifrovanje bi bilo besmisleno kad takvi ne bi postojali. Jedan od ciljeva novih algoritama je da što je moguće više oteža posao kriptoanalitičara, onih koji pokušavaju da provale šifru. To podrazumeva dve vrste aktivnosti: prvo, predviđanje i ograničavanje mogućih ili verovatnih tipova napada; i, drugo, povećavanje količine rada potrebnog za svaki pokušaj iznalaženja ključa. Ako takav rad nadilazi ono što bi pojedinac ili narod mogli da izvedu, šifrovanje bi se moglo smatrati uspelim.

Napadi se najčešće zasnivaju na količini informacija kojima kriptoanalitičari raspolažu. Ako analitičar ima samo nekoliko šifrovanih tekstova, onda je to napad samo na osnovu šifrovanih tekstova; napad na osnovu poznatih razumljivih tekstova imamo ako analitičar ima šifrovane poruke i njihov razumljiv tekst; napad na osnovu izabranog razumljivog teksta je kad analitičar poseduje ne samo šifrovane poruke i njihove razumljive tekstove, već može i da izabere šifrovani razumljivi tekst; napad na osnovu adaptiranog razumljivog teksta, kad analitičar može da modifikuje šifrovani razumljivi tekst na osnovu rezultata svakog pokušaja; i najzad, napad na osnovu izabranog šifrovanog teksta, kad analitičar može da bira različite šifrovane tekstove za dešifrovanje a može da nabavi i razumljiv tekst. Rezultat je složeni informatički ples – ko je šta i kako nabavio i kako šifrovani tekst može učiniti njihove informacije beskorisnim. Upamtite da je svrha ovih napada da se dođe do ključa za dešifrovanje svih budućih poruka. To

znači da analitičar mora tako da rekonstruiše šifrovanu poruku da time kaže kompjuteru da dešifruje tekst. A to je više od mogućnosti da se dešifruje bilo koji tekst. To je sposobnost da se dešifruju svi budući tekstovi koji koriste isti sistem što često, mada ne i nužno, podrazumeva obrnuto projektovanje hardvera koji je korišćen za šifrovanje i dešifrovanje, kao i otkrivanje mišljenja koje je ubačeno u upotrebljeni sistem šifrovanja. Drugim rečima, pravi kriptoanalitičar mora biti u stanju da rekonstruiše sisteme a ne toliko pojedine tekstove.

Svi ovi napadi su strategije upotrebljive jedino ako kriptoanalitičar ima nekoliko komada slagalice. Ali, šta ako nema od čega da počne? Tada preostaje jedino "brutalni napad": analitičar koristi kompjutere da isproba sve moguće kombinacije slova koje bi mogle biti ključ. Brutalni napad je prosto stvar brzine kompjutera, pokušaj rešavanja problema golom snagom rada. Može li moj kompjuter ili niz kompjutera da prorešeta broj mogućnosti za dovoljno razumno vreme? Pošto je cilj projektanta šifrantskih sistema stvaranje sistema sa sve složenijim ključevima, rad brutalnog napada ili ma kog drugog, eksponencijalno raste. Na ovom nivou se veliki ples, mačevanje, igra napada i odbrane između napadača i branilaca, kriptoanalitičara i projektanata šifara svodi na golu snagu kompjutera. Ako možete da projektujete sistem koji je toliko složen da nikakav niz kompjutera ne može da rekonstruiše ključ u razumnom vremenskom roku, recimo ni za milijardu godina, vaš bi se sistem mogao nazvati uspešnim. Tako se uspešna kriptografija i uspešna kriptoanaliza sve češće svode na pitanje rada.

Jedna od najozbiljnijih rasprava o politici šifrovanja sada se vodi povodom razvoja Clipper čipa, novog zaštićenog mikročipa koji sadrži tajni algoritam za šifrovanje za koji kažu da je nerešiv na postojećem nivou razvoja tehnologije. Čak i Agencija za nacionalnu bezbednost, vladina agencija koja je prva i razvila čip, priznaje da ne bi mogli da otkriju algoritam bez ključa za dešifrovanje koji se sastoji iz dva dela, od kojih je svaki deponovan u drugoj vladinoj agenciji. Poenta ovog novog standarda, primene tog novog algoritma nazvanog "Skipjack" je da vlada želi da primeni zasad neprovaljiv kriptografski standard, mnogo složeniji od DES-a iz 1982, radi zaštite od indu-

strijske špijunaže i osiguranja od prisluškivanja kad se završi digitalizacija telekomunikacija.

Skipdžek čine neprovaljivim njegova složenost, uvećana tajnošću koja okružuje strukturu samog algoritma i činjenica da je Clipper čip za šifrovanje i dešifrovanje tako dobro zaštićen da se ne može reprojektovati. Po rečima Doroti Dening (Dorothy Denning) (113), jednog od prvih prikazivača novog algoritma i jedne od njegovih glavnih zagovornica: "U pogledu napada 'brutalnom snagom' to jest iscrpne pretrage, koristili smo DES kao polaznu osnovu i uzeli dodatnu snagu ključeva skipdžeka od 80 bajta u poređenju sa DES-ovim od 56 bajta. Pošto su skipdžekovi ključevi 24 bajta duži od DES-ovih, ima 224 puta više mogućih kombinacija za isprobavanje. Stoga, pod pretpostavkom da se cena snage procesovanja upola smanjuje svakih godinu i po dana, proći će 1,5 x 24 godine = 36 godina pre no što cena provaljivanja skipdžeka iscrpnim pretraživanjem bude uporediva s današnjom cenom provaljivanja DES-a."

Dakle, ovaj novi algoritam tako je jak da, čak uzevši u obzir projektovani razvoj kompjutera, za sledećih 25 ili 30 godina spreči napade kriptoanalitičara. Ovde se *rad* uglavnom odnosi na kompjutersko procesovanje. Da bi se, u slučaju skipdžeka, obavila neka iscrpna pretraga potrebna za rekonstruisanje ključa, trebalo bi 2^{24} više pokušaja nego za otkrivanje DES-ovog ključa.

To daje sasvim novi obrt ideji rada, pošto bi količina rada koju bi provaljivanje šifrantskog algoritma od 80 bajta podrazumevalo, bila jednostavno neizvodljiva sa sadašnjom tehnologijom. Efikasnost nekog algoritma uglavnom se meri količnom rada potrebnog za njegovo provaljivanje i po toj meri, skipdžek bi stvarno bio vrlo efikasan.[9]

Po Ekovom mišljenju, proizvodnja znakova uglavnom je rad biranja i povinovanja: "U svim slučajevima ovaj čin izricanja pretpostavlja *rad*. Pre svega, rad *proizvođenja* signala; potom rad *biranja* između skupa signala koje imam na raspolaganju onoga koji se mora artikulisati da bi se komponovao izraz, kao i rad izolovanja izraza-jedinice da bi se komponovao

9 Po mnogim stručnjacima za šifrovanje, sad govorimo o broju pokušaja potrebnih za uspešan brutalni napad koji znatno prevazilazi broj čestica u univerzumu.

izraz-nit, poruka, tekst." U svemu ovome, Eko govori o radu proizvođenja razumljivog teksta, jednostavnom činu govorenja, biranju reči, pisanju, prerađivanju, slanju razumljivih i jednostavnih poruka. U šifrovanju je, međutim, tu i dodatni rad, pokušajima i greškama ili zaključivanjem, biranja između različitih kombinacija onog ključa koji će, kad se pronađe, moći da dešifruje šifrovani tekst i iznova sklopi razumljiv tekst proizveden na način koji opisuje Eko.

Zaključak

Smatram da nije pametno da humanisti raznih uverenja ostanu neupućeni u tehnologiju šifrovanja. Razume se da nije potrebno da svi pojurimo i uradimo postdoktorske studije iz teorije brojeva, ali će za one koji žele da razumeju rastući uticaj elektronskih medija na društvo i pojedinca kriptografske tehnologije bivati sve važnije. Svaki novi put komunikacije stvara vlastite dileme. To je delom i zbog potrebe da se kontroliše taj put. Što se više naših svakodnevnih poslova bude obavljalo onlajn, samo će rasti potreba za sigurnom komunikacijom. Digitalni novac, digitalni medicinski dosijei, digitalni porezi, digitalna registracija automobila, digitalni obrazovni dosijei – svi ti izvori informacija moraće da se zaštite.

Ali ne smemo da zaboravimo da je doskoro šifrovanje bilo klasifikovano kao municija. U velikom delu naše istorije, zapravo, u velikom delu istorije samog šifrovanja, ono je bilo ratno oružje i oruđe diplomatije. Da bi ga razumeli, moramo da znamo nešto o tome kako funkcioniše i nešto o njegovom mestu u univerzumu pisanja i čitanja. Moramo da razumemo ne samo značaj čitanja, već i onoga što se preduzima da se inhibira čitanje. Mogli bismo biti suočeni s izborom između dva nasilja – nasilja reprezentacije i nasilja činjenja reprezentacije nemogućom. Uveren sam da je zato potrebna politika čitanja koja uključuje šifrovanje kao temu. Što više ličnih informacija bude ulazilo na Mrežu, ta politika čitanja mogla bi iznedriti novu psihologiju i novu sociologiju zajednica organizovanih i održavanih delom na tehnologiji šifrovanja. Staro pitanje – ko ima pravo da prisluškuje ili ko ima pravo pristupa ličnim informacijama, moglo bi postati sporno kad moć da se to radi postane tek malo više od pritiska na dugme ili uključivanja programa.

S engleskog prevela:
Vera Vukelić

NAVEDENA DELA

Barthes, Roland, *Elements of Semiology*, prev. Annette Lavers & Colin Smith, New York, Hill&Wang, The Noonday P, 1967.

Benedict, Michael, "Cyberspace: Some Proposals", *Syberspace: First Steps*, ur. Michael Benedict, Cambridge, MIT P, 1991, str. 119-224.

Bielewicz, Julian A., *Secret Languages: Communicating in Codes and Ciphers*, New York, Elsevier Books, 1976.

de Saussure, Ferdinand, *Course in General Linguistics*, prev. Roy Harris, ur. Charles Bally & Albert Sechehaye, LaSalle, Il., Open Court, 1972.

Denning, Dorothy E., "The U.S. Key Escrow Encryption Technology", *Builging in Big Brother: The Cryptographic Policy Debate*, ur. Lance J. Hoffman, New York, Springer-Verlag, 1995.

Eco, Umberto, *A Theory of Semiotics*, Bloomington, Indiana UP, 1976.

Eco, Umberto, *The Role of the Reader: Explorations in the Semiotics of Texts*, Bloomington, Indiana UP, 1979.

Eco, Umberto, *Travels in Hyperreality*, prev. William Weaver, San Diego, Harcourt, 1983.

Kahn, David, *The Codebreakers: The Story of Secret Writing*, London, Weidenfeld & Nicholson, 1967.

Logan, Robert K., *The Alphabet Effect*, New York, St. Martin's P, 1986.

Martin, Henri-Jean, *The History and Power of Writing*, prev. Lydia G. Cochrane, Chicago, University of Chicago Press, 1988.

Olson, Scott, R., "Renewed Alchemy: Science and Humanism in Communication Epistemology", *Building Communication Theories: A Socio/Cultural Approach*, ur. Fred L. Casmir, Hillsdale, NJ, Lawrence Erlbaum Associates, 1994, str. 71-73.

Ong, Walter J., *Orality and Literacy: The Technologizing of the Word*, London, Routledge, 1982.

Popper, Karl R., *Objective Knowledge: An Evolutionary Approach*, 2nd edition, Oxford, Claredon Press, 1979.

Schneier, Bruce, *Applied Cryprography: Protocols, Algorithms, and Source Code*, New York, Wiley, 1994.