NSA - NATIONAL SECURITY AGENCY

Tina Šijanec, absolventka, UM

Junij, 2001

1 Uvod

Nacionalna agencija za varnost NSA (National Security Agency) je ameriška kriptološka organizacija zadolžena za prisluškovanje drugim državam in sovražnikom z namenom zbiranja obveščevalnih informacij. Poleg tega za ameriško vlado razvija enkripcijsko opremo in komunikacijske sisteme, ki naj bi bili odporni na prisluškovanja drugih držav. Med drugim je tudi organizacija, ki zaposljuje največ matematikov v ZDA, kateri se ukvarjajo z raziskovanjem in razvojem predvsem na področju kriptografije.

NSA je največja ameriška obveščevalna organizacija o kateri se še danes ne ve veliko, celo njen proračun in število zaposlenih sta tajna. Njen obstoj je bil desetletja skriven, zaradi tega je kasneje tudi dobila vzdevek "No Such Agency". To ji je takrat omogočilo, da je puščala Kongres in tisk v nevednosti in se izognila preiskavam o njenih aktivnostih. Danes ima agencija poleg pritiskov s strani tiska in kongresa, še druge težave. Konec hladne vojne in razvoj informacijskih tehnologij sta zelo otežila njeno delo. Tehnologije (npr. enkripcija) nekoč dostopne samo agencijam kot je NSA so sedaj dostopne vsem, tako nekaterim drugim državam kot teroristom.

V 2. poglavju tega projekta se bom posvetila osnovnim podatkom o NSA, kot so njen nastanek, funkcije in njena organiziranost. Na eni strani kritiki danes obtožujejo NSA, da je "Veliki Brat" brez cilja, ki prisluškuje vsem možnim komunikacijam po celem svetu, po drugi strani pa ji očitajo nesposobnost v dobi interneta. Zato bomo v 3. poglavju povedali malo o njenem globalnem sistemu za prisluškovanje poimenovanem ECHELON in kakšne razprave je povzročilo njegovo razkritje. V 4. poglavju pa se bomo posvetili težavam, s katerimi se danes srečuje NSA kot so enkripcija, prevelika količina informacij in kontroliranje izvoza kriptografske opreme. V zadnjem 5. poglavju bomo poskusili oceniti računsko moč računalnikov, ki jih NSA uporablja in oceniti kakšna je njihova učinkovitost pri dekripciji na primeru varnih javnih sistemov.

2 Predstavitev NSA

Kljub temu, da danes NSA ni več skrivnost, jo še vedno veliko ljudi ne pozna ali pa je o njej slišalo zelo malo. Zato je namen tega poglavja okvirno predstaviti agencijo. V 1. podpoglavju si bomo na kratko pogledali njen nastanek, kje ima sedež in koliko naj bi imela zaposlenih. V naslednjem pa sem se posvetila nekaterim njenim osnovnim funkcijam in organiziranosti.

2.1 Nastanek NSA

Ameriška nacionalna agencija za varnost NSA je bila ustanovljena oktobra leta 1952 s predsedniško odredbo, ki jo je podpisal takratni predsednik Združenih držav Truman. V prvih povojnih letih so za kriptološke dejavnosti ameriških sil skrbele vojaške kriptološke službe treh rodov (kopenska vojska, mornarica, letalstvo). Kmalu je nastala potreba po neki enotni organizaciji, ki bi imela celoten pregled nad takim delovanjem, saj je prihajalo do konfliktov v komunikaciji med temi službami. Tako so leta 1949 ustanovili agencijo AFSA - Armed Forces Security Agency, ki je prevzela funkcije strateških komunikacijskih obveščevalnih služb in nalogo koordiniranje dela. Ker se je izkazalo, da ima tak skupni pristop velike prednosti, so se odločili, da ga razširijo tudi na kriptološke aktivnosti izven Ministrstva za obrambo, kar seveda vključuje tudi kriptosisteme Ministrstva za zunanje zadeve. Agencijo AFSA so ukinili, njen kader in opremo pa so premestili v agencijo NSA.

Trumanova odredba je imela status najbolj tajne direktive, zato se kar nekaj let v javnih dokumentih ni omenjalo imena NSA , niti ni bil omenjen njen obstoj. Nato pa so leta 1957 uvrstili njen opis v priročnik o organizaciji državne uprave Združenih držav (United States Government Organization Manual), ki pa je bil zelo kratek in namerno nejasen. Uradni opis agencije in njenih nalog se je glasil: "NSA je zasebna kriptološka organizacija znotraj ministrstva za obrambo. Podrejena je ministru za obrambo, ki z njo upravlja in kontrolira njeno delo. Agencija je izvršno telo za opravljanje določenih specializiranih tehničnih nalog v zvezi z obveščevalnim delovanjem Združenih držav. Njeni glavni nalogi sta skrb za varnost države in zbiranje obveščevalnih informacij."

Prva leta njenega obstoja je imela NSA svoje prostore razstresene po celem Washingtonu. Leta 1954 so pričeli z gradnjo sklopa objektov, ki še danes predstavlja sedež agencije. Nahaja se v vojni bazi Fort George G. Meade, v državi Maryland. Dela so bila končana leta 1957, skupna cena projekta je bila približno 35 miljonov dolarjev.

Veliko trinadstropno zgradbo, zgrajeno v obliki črke A, obkrožajo parkirišča in borov gozd. Ko so jo zgradili, je bila dolga 290 in široka 170 metrov. Poleg veliko pisarn in prostorov za računalnike je v njej še avditorij, lastna pošta, ambulanta z rentgenom in operacijsko sobo, banka... Imela je 130.000 m^2 koristnega prostora in je postala premajhna že po petih letih. Dogradili so devetnadstropni aneks med krake črke A.

Leta 1960 naj bi tam delalo že čez 10.000 ljudi [1]. Leta 1990 pa naj bi imela NSA v Fort Meadu zaposlenih približno 20.000 ljudi. Zadnja ocena izhaja iz primerjave s Pentagonom. NSA ima približno pol miljona kvadratnih metrov poslovnih prostorov v Ft. Meadu, kar je malo manj kot Pentagon, ki ima nekaj več kot 20.000 osebja. Nekateri viri ocenjujejo, da ima NSA vseh zaposlenih med 38.000 in 52.000 [2]. Seymour Hersh,

avtor članka Intelligence Gap [6], pa pravi, da je imela NSA med hladno vojno skoraj 95.000 vseh zaposlenih, vendar je bilo po vojni število osebja, ki je delalo zunaj ZDA, zmanjšano za polovico.

2.2 Funkcije in organizacija NSA

NSA je enotna organizacija, ki je zadolžena za signalno obveščevalnost (SIGINT - Signals Intelligence) Združenih držav in skrbi za varne komunikacijske sisteme (COMSEC - Communications Security) vseh ministrstev in agencij ameriške vlade.

SIGINT je kategorija obveščevalnih informacij, ki združuje komunikacijske (Comint-Communications Intelligence), elektronske (Elint-Electronics Intelligence) in telemetrične (Telint) obveščevalne informacije.
Comint informacije pridobivajo s prestrezanjem in obdelavo tujih komunikacij oddajanih preko elektromagnetnih načinov in z obdelavo tujih šifriranih komunikacij. Obveščevalne informacije Elint pridobivajo iz tujih elektromagnetnih nekomunikacijskih prenosov. Najbolj pogosti izvori teh informacij so tuji radarski signali. Telemetrične informacije pa pridobivajo s prestrezanjem, obdelavo in analizo tuje telemetrije.

Njihova druga naloga (COMSEC), varuje komunikacije Združenih Držav pred zlorabo od tujih obveščevalnih agencij in pred nepooblaščenimi razkritji. NSA oskrbuje 18 vladnih agencij in ministrstev s COMSEC sistemi, vključno z ministrstvom za obrambo, ministrstvom za zunanje zadeve, CIA in FBI.

NSA določa tehnične smernice za vse SIGINT operacije ameriške vlade. Oblikuje programe, plane, postopke, politiko in upravlja z dodeljenimi SIGINT sredstvi, osebjem in programi. Vodi raziskave, razvoj in konstrukcijo sistemov, da zadosti svojim potrebam in usklajuje z drugimi agencijami sorodne raziskave, razvoj in testiranja na SIGINT področju.

Agencija odgovarja na prošnje drugih članov obveščevalne skupnosti za določene signalne informacije. Vsako leto NSA dobi seznam SIGINT potreb, po katerih se naslednje leto ravna. Vse potrebe in zahteve morajo biti usmerjene na zbiranje tujih obveščevalnih informacij, vendar ta pojem ni natančno definiran. NSA naj bi se osredotočila na komunikacijske zveze, ki imajo vsaj en tuj terminal. Kljub temu lahko prestreže komunikacije med dvema Američanoma, kadar gre za mednarodne komunikacije. Kadar si NSA izbere določena vezja, za katera se ve, da prenašajo tuje komunikacije pomembne za zbiranje tuje obveščevalnosti, pobere vse prenose skozi ta vezja, med njimi so lahko tudi komunikacije državljanov Amerike. NSA sicer pravi, da take komunikacije izloča pri obdelavi podatkov, vendar se vsi ne strinjajo s tem. Dan Brown, ki je napisal kontraverzni triler o NSA - ju Digital Fortress, pravi da je knjiga nastala zaradi resničnega dogodka, ki potrjuje govorice. Ko je učil na neki akademiji v New Hampshire-u, se je nekega dne na šoli pojavila tajna služba in priprla njihovega študenta, ker naj bi predstavljal grožnjo nacionalni varnosti. Izkazalo se je, da je študent poslal elektronsko pošto prijatelju, da sovraži predsednika in da bi ga nekdo moral ustreliti. Nekdo je torej moral prestreči njegovo sporočilo.

Na čelu NSA je direktor, ki mora biti oficir vojaške službe in mora imeti stopnjo najmanj treh zvezdic. Direktor NSA je tudi vodilni v Centralni varnostni službi (CSS

Central Security Service), ki združuje vse vojaške elemente Združenih Držav (vojska, mornarica, letalstvo, marinci) in skrbi za partnerstvo med NSA in vojsko. Trenutni direktor je general Michael V. Hayden, pomočnica direktorja pa je Barbara McNamara. Direktorja podpira in mu svetuje izvršilna vodstvena skupina ELT (Executive Leadership Team), ki jo sestavljajo pomočnik Direktorja, pomočnik direktorja za Operacije, pomočnik direktorja za Tehnologijo in pomočnik direktorja za Informacijsko sistemsko varnost, vsi ti pomočniki so civilisti.

Od vseh obveščevalnih organizacij, kot sta CIA in FBI, je NSA daleč nabolj skrivnostna glede svoje notranje organizacijske strukture. NSA je organizirana v pet Direktoratov, vsak je razdeljen na nekaj skupin ali elementov. Direktorat za Operacije (Operations Directorate) je zadolžen za zbiranje in obdelavo SIGINT materijala. Direktorat za Tehnologijo in Sisteme (Technology and Systems Directorate) razvija novo tehnologijo za zbiranje in obdelavo SIGINT materijala. Direktorat za Informacijsko Sistemsko Varnost (Information Systems Security Directorate) je zadolžen za NSA -jeve komunikacije in aktivnosti na področju informacijske varnosti . Direktorat za Politiko in Program je zadolžen za osebje in splošno usmerjanje agencije. Direktorat za Podporno Dejavnost (Support Services Directorate) pa skrbi za logistične in administrativne podporne dejavnosti.

Več informacij o NSA si lahko preberete na neuradni strani NSA, ki so jo naredili ameriški znanstveniki (FAS-Federation of American scientists) [2]. Ta stran vsebuje veliko informacij o NSA (zgodovina, organizacija, njene lokacije,...) in veliko povezav do strani in člankov v zvezi z njo. NSA ima tudi svojo domačo stran (http://www.nsa.gov).

3 ECHELON

Že od samega začetka je v agenciji NSA vladalo prepričanje, da je za uspešno in učinkovito opravljanje obveščevalnih aktivnosti nujno potrebno strogo tajno delovanje. To dokazuje dejstvo, da se več desetletij ni nič vedelo o njenem obstoju zunaj obveščevalne skupnosti. Danes je razkritih že kar nekaj njenih skrivnosti, čeprav še vedno velja za najbolj tajno obveščevalno agencijo. V zadnjem desetletju buri javnost razkritje dosedaj največje elektronske vohunske mreže, danes znane pod projektom ECHELON, katerega pobudnica in ustanoviteljica je agencija NSA. Sistem uporabljajo za prestrezanje komunikacij, kot so elektonska pošta, faksi in telefonski pogovori, ki se prenašajo po svetovnih telekomunikacijskih mrežah.

ECHELON je rezultat UKUSA sporazuma, ki so ga leta 1948 podpisale angleško govoreče vlade Združenih Držav, Velike Britanije, Kanade, Australije in Nove Zelandije. Obveščevalne agencije, ki so povezane s tem sporazumom, so NSA, Government Communications Headquartes (GCHQ) v Angliji, Communications Security Establishment (CSE) v Kanadi, Defense Signals Directorate (DSD) v Australiji in Government Communications Security Bureau (GCSB) v Novi Zelandiji. Ta sporazum koordinira sodelovanje teh agencij pri zbiranju in obdelavi informacij iz elektronskih virov (SIGINT). NSA je razvila tehnologijo, katero uporablja sistem in jo ima pod nadzorom. To ji omogoča nadrejeni položaj nad zaveznicami in zato lahko drži niti v svojih rokah.

NSA in njene zaveznice so postavile verigo tajnih prisluškovalnih objektov in naprav po celem svetu, da lahko prisluškujejo vsem večjim komponentam mednarodne telekomunikacijseke mreže. Neketere postaje prisluškujejo satelitskim komunikacijam, druge zemeljskim komunikacijskim mrežam, ostale pa radijskim komunikacijam, ECHELON pa povezuje vse te objekte skupaj. Tako sistem prestreza komunikacije, ki jih prenašajo mednarodni telekomunikacijski sateliti (Intelsat) ter komunikacijski sateliti (Comsat). Velik del komunikacij prenašajo mikrovalovna omrežja v kombinaciji s podmorskimi kabli. NSA je uspešno prisluškovala starim bakrenim kablom, vendar te danes zamenjujeo optični kabli, katerim je težje prisluškovati. Optične kable sestavljajo steklene tanke vrvi ovite s plastičnim ovojem, preko katerih se podatki prenašajo v svetlobnih valovih namesto z električnimi pulzi, zato so optični kabli imuni na elektromagnetne motnje. Analitiki obveščevalnih dejavnosti pravijo, da optična vlakna predstavljajo težave tudi za NSA. Vendar si je agencija že priskrbela pomoč. Lansko leto je ameriška mornarica začela z, 1 bilijon dolarjev vredno, obnovo ameriške podmornice Jimmy Carter, ki naj bi zaplula v morje leta 2004 [7]. Opremili jo bojo z visoko razvito tehnologijo za podmorske optične kable in bo najbolj napredna vohunska podmornica.

Sistem ECHELON deluje tako, da na slepo prestreza veliko količino komunikacij in potem preko računalnikov določi in izloči sporočila, ki so pomembna od tistih, ki niso. Za ta namen je NSA razvila mrežo superračunalnikov, kateri se imenujejo ECHELON-ski slovarji. Ti pregledujejo miljone prestrezanih sporočil, za tiste, ki vsebujejo vnaprej sprogramirane ključne besede, ki so lahko imena oseb, organizacij, držav, zanimivih tem. Besede vključujejo tudi telefonske številke, fakse in internetne naslove posameznikov, podjetij, vladnih ministerstev, vseh, ki so tarče. Eno prvih podrobnejših razkritij sistema ECHELON je napisal Nicky Hager v knjigi Secret Power [3]. Več o ECHELON-u in današnjih prisluškovalnih zmožnostih si lahko preberete v poročilu Duncana Campbella Intelligence Capabilities 2000, ki ga je leta 1999 pripravil za evropski parlament, oziroma v njihovem delovnem dokumentu (STOA) [4].

V času hladne vojne je bil glavni namen ECHELON-a, da pazi na bivšo Sovjetsko zvezo, danes pa opravičujejo njegov obstoj in več biljonske stroške s trditvijo, da ga uporabljajo za boj proti terorizmu in drogi. Ameriška združenja za civilne pravice skrbi, da je NSA izrabila UKUSA sporazum in obšla zakonodajo, ki ji prepoveduje prisluškovanje ameriškim državljanom. Mike Frost, bivši uslužbenec kanadske CSE, je Hager-ju priznal, da jim je NSA naročila prisluškovanje američanom, v zameno pa je ona spremljala kanadske državljane. Po drugi strani, Duncan Campbell optožuje ZDA, da zbrane podatke izkorišča v vojaške, politične in poslovne namene. V njegovem poročilu je omenil kar nekaj primerov zlorab ekonomskih informacij. ECHELON naj bi pomagal ameriškim podjetjem pri prevzemanju poslov evropskim in drugim konkurentom. Tako naj bi leta 1995 pomagal Boeing-u in McDonnell Douglas-u prevzeti evropskemu Airbus-u več bilijonov dolarjev vredno prodajo civilnih letal Saudski Arabiji. Američane tudi optožujejo, da so s pomočjo ECHELONA izbrskali marsikatera pogajalska izhodišča evropskih držav in Japonske, kar jim je zelo pomagalo pri nekaterih pogajanjih, meddrugimi tudi na azijsko-pacifiški ekonomski konferenci leta 1997. NSA seveda vse te obtožbe strogo zanika in pravi, da nadzoruje samo tista podjetja, katera sumijo, da so povezana s podkupovanjem. Take informacije ponavadi posreduje naprej Ministrstvu za Zunanje zadeve. Težko je dokazati, kaj je res in kaj ni. Danes je mogoče vladati samo z ekonomsko močjo, gospodarska

uspešnost pa je v sodobnem svetu odvisna predvsem od informacij.

Danes ECHELON ni več skrivnost, saj je bilo o tem projektu že veliko napisanega. Pod pritiskom javnosti in ameriških združenj za civilne pravice je NSA leta 1999 z dveh dokumentov, ki potrjujeta obstoj ECHELON-a, odstranila oznako "strogo zaupno". S tem so bila potrjena dolgoletna ugibanja o obstoju globalnega sistema za prisluškuvanje.

V EU so po večletnem raziskovanju vedno bolj prepričani v zlorabo ECHELON-a, med drugim tudi za industrijsko špijonažo. V svojem zadnjem poročilu [5] svojim državljanom priporočajo uporabo enkripcijskih programov, saj mnogi pravijo, med njimi tudi Hager, da je ECHELON sistem, ki ogroža predvsem lažje dostopne in slabo šifrirane komunikacije. Z uporabo enkripcijskih programov pa bi le te postale težje za dešifriranje. Ker je danes učinkovita enkripcija dostopna vsakomur, bi s tem znatno zmanjšali učinkovitost ECHELON-ovih računalnikov. To sicer ne pomeni, da bi se prisluškovanje končalo, ampak le, da bo potrebno razviti nove sisteme in bolj učinkovito tehnologijo (npr. za prisluškovanje optičnim kablom). Prav gotovo se je NSA že posvetila tem ciljem.

4 Problemi NSA v obdobju enkripcijske dobe

Nacionalna agencija za varnost NSA, ki je v obdobju hladne vojne spodbudila ameriško računalniško revolucijo, z intenzivnim raziskovanjem na področju kriptografije in na področju elektronskega prisluškovanja, je sama postala žrtev tehnološko razvitega sveta, katerega je pomagala ustvariti. Kot posledica slabega vodenja, arogantnosti in strahu pred neznanim se vodilni pri NSA niso dobro pripravili na veliko količino informacij, ki se danes prenašajo preko interneta. Medtem pa so države po Evropi in Aziji že začele šifrirati sporočila, ki jih uporabljajo v diplomatske in varnostne namene, z "nezlomljivimi" digitalnimi kodami.

Najglasnejši kritiki agencije NSA so postali člani obveščevanih odborov ameriškega kongresa. John Millis, bivši uslužbenec CIE in član enega teh odborov, je leta 1998 odprto diskutiral s skupino upokojenih uslužbencev CIA o problemih NSA. Rekel jim je, da je signalna obveščevalnost v krizi, da je bila tehnologija včasih prijateljica agencije, v zadnji petih letih pa je postala njena sovražnica [6]. Z njim se strinja tudi senator Robert Kerrey, ki je na kolegiju Senata izrazil bojazni, da bodo zaradi visoko razvitih enkripcijskih programov za komunikacije, obveščevalni analitiki prihajali nazaj praznih rok, češ da ne znajo prevesti signalov, da je vse kar slišijo samo brenčanje in hrup v ozadju. Njegova zaskrbljenost se je povečala, ko je odbor organiziral študijsko skupino Technical Advisory Group, ki je vsebovala tudi nekaj zunanjih strokovnjakov, ki so zadolženi za razvoj in tehnologijo razvitih podjetij, kot je George Spix v Microsoftu. Ta skupina je imela dostop do večine najbolj občutljivih področij v centrali NSA. Njihovi zaključki so bili pogubni. Povedali so jim da, če ne bodo popolno obnovili obveščevalnih sistemov, bodo oglušeli najkasneje v desetih let. Svetovali so, da naj agencija začne s takojšno reorganizacijo in okrepitvijo z nekaj sto računalniškimi znanstveniki [6]. Očitno je bilo nekaj resnice v njihovih zaključkih. Namreč januarja lansko leto, se jim je sesula glavna računalniška mreža v Ft. Meadu, izpad je trajal kar štiri dni [7].

Po drugi strani so kritike posledica agencijinih neuspehov v zadnjih letih. Maja leta 1998 je Washington presenetila novica, da so v Pokhranu v Indiji opravili prvi krog testiranja jedrskega orožja. NSA je bila tista, ki ni zaznala znakov povečane aktivnosti in komunikacij v Pokhranu v dnevih pred detonacijo. Mnogi pravijo, da če bi bila agencija res sposobna izluščiti veliko smiselnega iz zbranih podatkov, potem do tega ne bi smelo priti [6]. Podobno se teroristi, kot Osama bin Laden, ne bi bili sposobni toliko časa skrivati pred zakoni.

NSA se je že od začetka trudila preprečiti javni dostop do enkripcijske tehnologije. Leta 1978 je računalniški znanstvenik George I. Davida, hotel patentirati enkripcijsko napravo, vendar je NSA privlekla na dan zakon o tajnosti iz leta 1951. Davida se je obrnil na medije, tako da se je NSA morala umaknit. Podobna zgodba se je odvijala leta 1993, ko se je pričela kriminalna preiskava proti Phillipu Zimmermannu, ki je naredil kriptografski program imenovan P.G.P (za Pretty Good Privacy). Ta program je bil nočna mora agencije NSA, saj je dovoljeval povprečnemu računalniškemu uporabniku lahko dnevno uporabo kriptografije. P.G.P je kmalu našel pot do interneta in se hitro razširil po svetu. Po treh letih so tožbo proti Zimmermannu opustili.

Bolj uspešna je bila pri kontroliranju izvoza enkripcijske opreme. Izvoz je bil možen le, če je bila velikost ključev strogo omejena, in ga je NSA odobrila. Iz tega razloga je bila enkripcijska oprema razdeljena na dva razreda: oprema z "močno" enkripcijo in oprema z "šibko" enkripcijo (enkripcijo za izvoz). Šibka enkripcija ponavadi pomeni, da je velikost ključa največ 56 bitov za DES, 512 bitov za RSA ter največ 112 bitov za eliptične krivulje. Vsi našteti kriptosistemi pa so bili za ključe teh velikosti že razbiti.

Da bi si omogočila oz. olajšala dešifriranje sporočil, je NSA vršila pritiske na vlado. Trudila se je prepričati vlado v sprejetje naslednjih dveh predlogov. Prvi predlog je bil, da se v enkripcijsko opremo vstavi enkripcijski čip, znan kot Clipper Chip, do katerega bi imeli direkten dostop državni organi. Pod drugim predlogom, pa bi ameriški izdelovalci računalnikov lahko izvažali enkripcijsko opremo, če bi imela država dostop do rezervnih ključev. Seveda sta bila oba predloga strogo napadena s strani industrije. Vseeno je leta 1997 prišlo na dan, da je podjetje Lotus v programsko opremo po dogovoru z NSA vgradil enkripcijo, ki so jo lahko Ameriški strokovnjaki zlomili. Komunikacijski sistem opremljen z Lotus Notes je uporabljala švedska vlada. Predstavnik podjetja Lotus je takrat priznal časopisu Svenska Dagbladet, da so dobavljali sisteme s 64 bitnimo enkripcijo, vendar so v izvozni različici 24 bitov ključa deponirali pri ameriški vladi [4].

Kljub upiranju je NSA januarja 2000 izgubila nadzor nad izvozom enkripcijske opreme, saj so bile takrat restrikcije za izvozne zakone drastično omiljene. Danes lahko vsako enkripcijsko opremo izvozijo brez licenc razen, če izvažajo tujim vladam oz. območjem pod embargom (Kuba, Irak, Srbija ,...). Izvoz tujim vladam je tudi mogoč, toda le z licenco.

Zaradi povečanja komunikacij (globalizacija, internet, ...) je za obdelavo vedno večjega števila informacij, poleg večje količine računalnikov potrebno tudi veliko novih strokovnjakov s področja krptografije. Zato je bila tudi NSA, nekdaj skrivna organizacija o kateri se je zelo malo vedelo, primorana v javno iskanje bodočih kadrov. Tako so letos v reviji Math Horizons (feb.) objavili članek, v katerem so se na kratko predstavili in v katerem vabijo diplomirane matematike, da se jim pridružijo v čim večjem številu. Pomankanje kadrov

Horizons (feb.) objavili članek, v katerem so se na kratko predstavili in v katerem vabijo diplomirane matematike, da se jim pridružijo v čim večjem številu. Pomankanje kadrov oz. njihovo "panično" iskanje lahko potrjuje domneve, da je bila NSA nepripravljena na tako hiter razvoj kriptografije in njeno široko uporabo.

Vse kaže na to, da je NSA izgubila vodstvo v informacijski revoluciji, katero je sama pomagala ustvariti. Strokovnjaki na področju obveščevalnosti krivijo za te težave zmanjšanje proračuna in osebja po hladni vojni, težje tarče in težje protiukrepe, najbolj od vsega pa birokracijo agencije. Vendar se vsi ne strinjajo s tem. James Bamford, avtor The Puzzle Palace, edine knjige napisane o NSA, pravi da NSA namerno daje tak vtis, ker bi s tem rada zmedla sovražnike in si pridobila naklonjenost Kongresa [7]. Močan skeptik glede NSA-jinih problemov je tudi strokovnjak na področju kriptografije Whitfield Diffie [6]. Njegovo mnenje je, da agencija sama potencira te govorice: "Bili so odlični, danes pa imajo probleme, internet je prezakompliciran zanje, preveč je prometa in ne morejo najti kar iščejo. To govorijo že leta in ustreza jim, da njihove tarče verjamejo tem problemom." Te razlage so zelo možne, verjetno ima NSA nekaj problemov, vendar je to lahko prav en od načinov s katerim jih rešujejo. NSA pravi, da so sedaj njihovi računalniški problemi sicer rešeni, vendar prosi Kongres za financiranje novega računalniškega sistema imenovanega "Trailblazer", ki bo sposoben bolje obdelovati in pridobivati uporabne obveščevalne podatke iz velikih količin informacij, ki jih zbira po svetu. Kongres jim je oddobril tudi financiranje sklopa majhnih nizko višinskih vohunskih satelitov v naslednjih petih letih. Nove ptice naj bi NSA pomagale izboljšati svoje prisluškovalne aktivnosti [7].

Kakšne težave ima NSA in kolikšen je njihov obseg, ne moremo zagotovo trditi. Argumenti tistih, ki trdijo, da so v resnih težavah in tistih, ki mislijo drugače, so enako verjetni. Če je vse to govorenje o njihovih težavah le "jamranje", in ker jim je Kongres že odobril nekaj finančne pomoči, so očitno dosegli svoj namen.

5 Računska moč NSA

NSA je že od vsega začetka vlagala v razvoj napredne tehnologije. To ji je omogočilo, da ima danes kar lepo zbirko visoko zmogljivih računalnikov. Vendar bomo videli, da so pri napadih na javne sisteme z večjimi dolžinami ključev tudi taki računalniki dokaj nemočni. V 1. podrazdelku bomo na kratko predstavili javne sisteme in časovne zahtevnosti najhitrejsih algoritmov, ki se danes uporabljajo za napade. V 2. podrazdelku si bomo ogledali ocene računskih moči potrebnih za te napade. V 3.podrazdelku pa bomo ocenili zmogljivost osebnih računalnikov v MIPS-ih in kolikšno je razmerje med inštrukcijami in flop operacijami. Nato bomo v zadnjem podrazdelku poskušali oceniti, kako uspešni so NSA-jevi Cray-i pri napadih na javne sisteme.

5.1 Javni kriptosistemi

Leta 1976 sta Diffie in Hellman predlagala sistem z javnimi ključi, pri katerem se uporabljata dva različna ključa, privatni in javni. Privatni ključ se ponavadi uporabja za dešifriranje in podpisovanje sporočil, medtem ko javni ključ uporabimo za šifriranje

sporočil oziroma preverjanje podpisa. Do danes je bilo razbitih veliko predlaganih sistemov. Varnost javnih sistemov temelji predvsem na težkih matematičnih problemih, kot sta faktorizacija celih števil in problem diskretnega logaritma.

Sistemi faktorizacije

Najbolj znani predstavnik prve skupine je sistem RSA [13], kateri je dobil ime po svojih iznajditeljih (Rivest, Shamir in Adleman). Kriptosistem izvaja računske operacije v množici $\mathbb{Z}_n$, kjer je modul n produkt dveh različnih praštevil p in q. Poglejmo si formalni opis kriptosistema:
Naj bosta prostora čistopisov P in tajnopisov C enaka $\mathbb{Z}_n$ in prostor ključev enak

$$K = \{(n, p, q, a, b); n = pq, p, g \text{ praštevili}, \ ab \equiv 1 \pmod{\phi(n)}\},$$

kjer je $\phi(n) = (p-1)(q-1)$. Za vsak ključ $k \in K$ definiramo enkripcijsko funkcijo

$$e_k(x) = x^b \bmod n$$

in dekripcijsko funkcijo

$$d_k(y) = y^a \bmod n,$$

kjer sta $x, y \in \mathbb{Z}_n$. Par (b, n) predstavlja javni ključ, katerega objavimo. Medtem ko trojica (p, q, a) predstavlja privatni ključ, ki ostane skriven.

Najbolj očiten napad na RSA je poskus faktorizacije modula n, saj bi potem napadalec lahko izračunal $\phi(n) = (p-1)(q-1)$ in $a = b^{-1} \bmod \phi(n)$ z uporabo razširjenega Evklidovega algoritma. Ko napadalec pozna število a, lahko dešifrira vsa nadaljna sporočila. Trenutno ne poznamo učinkovitih algoritmov za faktorizacijo, kateri bi pomenili zlom kriptosistema. Vseeno so najhitrejši algoritmi sposobni faktorizirat do 155 mestna števila, kot bomo videli v naslednjem razdelku, zato si je priporočljivo izbrati vsaj 100 mestna praštevila p in q, tako da je RSA modul n vsaj 200 mestno desetiško število. Pri faktorizaciji velikih števil so trenutno najučinkovitejši algoritmi: kvadratično rešeto (Quadratic Sieve Algorithm), algoritem z eliptičnimi krivuljami (Eliptic Curve Factoring Algorithm) in GNFS (General Number Field Sieve). Za faktorizacijo RSA modula, kjer sta p in q približno enako veliki praštevili, je najbolj uporabna metoda GNFS [15]. Računska zahtevnost te metode za faktorizacijo števila n je

$$L_1(n) = O(e^{(1.92+o(1))(\ln n)^{1/3}(\ln \ln n)^{2/3}}).$$

Kaj to pomeni za 155 mestna števila (512 bitna) in nekatera večja števila, glej Tabelo 1 (naslednji razdelek).

Sistemi diskretnega logaritma na eliptičnih krivuljah

Ti sistemi temeljijo na problemu diskretnega logaritma v grupi točk na eliptični krivulji. Eliptična krivulja nad končnim obsegom F je množica točk $(x, y) \in F \times F$, ki so rešitve enačb posebne oblike. Če je $F = \mathbb{Z}_p$, potem ima enačba obliko $y^2 = x^3 + ax + b$, kjer $a, b \in \mathbb{Z}_p$ in velja $4a^3 + 27b^2 \not\equiv \pmod{p}$. Operacija na eliptični krivulji je seštevanje dveh točk po enostavnem pravilu, ki uporablja operacije (seštevanje, množenje, deljenje)

v obsegu F. Več o eliptičnih krivuljah si lahko preberete v Koblitz-u [14]. Problem diskretnega logaritma na eliptičnih krivuljah (ECDLP-Elliptic Curve Discrete Logarithm Problem) predstavimo na naslednji način. Izberemo si naprimer eliptično krivuljo E nad $\mathbb{Z}_p$, točko $P \in E(\mathbb{Z}_p)$ reda n in točko $Q \in E(\mathbb{Z}_p)$. Določiti je treba tako celo število ℓ, $0 \leq \ell \leq n-1$, da je $Q = \ell P$. Predstavnik te skupine je digitalni podpis ECDSA (Eliptic Curve Digital Signature Algoritem), katerega opisuje spodnji algoritem.

Algoritem: digitalni podpis (ECDSA)
Generiranje ključa osebe A:

1. Izberi eliptično krivuljo E nad $\mathbb{Z}_p$, ki ima število točk deljivo s praštevilom n.
2. Izberi točko $P \in E(\mathbb{Z}_p)$ reda n in naključno število $a \in [2, .., n-2]$.
3. Izračunaj $Y = aP$.
4. Objavi javni ključ (E, n, P, Y), privatni ključ je a.

Podpis sporočila m osebe A:

1. Izberi naključno število $k \in [2, .., n-2]$.
2. Izračunaj $kP = (x_1, y_1)$ in $r = x_1 \bmod n$.
3. Izračunaj $s = k^{-1}(m + ar) \bmod n$.

Preverjanje podpisa:

1. Izračunaj $w = s^{-1} \bmod n$..
2. Izračunaj $u_1 = mw \bmod n$ in $u_2 = rw \bmod n$.
3. Izračunaj $u_1 P + u_2 Y = (x_0, y_0)$ in $v = x_0 \bmod n$.
4. Podpis sprejmi natanko tedaj, ko je $v = r$.

Najboljši algoritem za reševanje problemov ECDPL v splošnem je Pollard-rho metoda [13], katere računska zahtevnost je približno $L_2(n) = \sqrt{(\pi n/2)}$ korakov, kjer en korak pomeni seštevanje na eliptični krivulji, glej Tabelo 2.

5.2 Ocene računskih zahtevnosti

Računsko moč bomo merili z enoto MIPS (Million Instructions Per Second) let, ki pomeni število let na MIPS računalniku. MIPS računalnik je zmožen opraviti milijon operacij na sekundo, torej MIPS leto pomeni $3,1 \times 10^{13} = 10^6 \times 3600 \times 24 \times 365$ aritmetičnih operacij.

Poglejmo si na kakšen način ocenjujemo računsko moč asimptotskih algoritmov, kot je GNFS (glej $L_1(n)$).
Naj bo $L(n)$ funkcija, ki predstavlja približno računsko zahtevnost algoritma, kjer n pomeni dolžino vhodnih podatkov v bitih.
Ko imamo enkrat dano računsko moč X, ki jo je potreboval algoritem za določeno m bitno število, lahko predvidimo potrebno računsko moč za večje število n, tako da izračunamo $X \times L(n)/L(m)$. Ta metoda ni najbolj natančna, saj zanemarja nekaj praktičnih zadev, kot je potreba po količini spomina, vendar se je v preteklosti dobro obnesla.

Najprej ocenimo koliko računske moči (časa v MIPS letih) je potrebno za faktoriziranje različnih števil n z GNFS metodo.
Leta 94 so Contini, Dodson, Lenstra in Montgomery faktorizirali 119 mestno desetiško

število z uporabo GNFS, za katerega so potrebovali 250 MIPS let. Na tej faktorizaciji temelji Odlyzkova tabela (Tabela 1) [8], ki predvideva računske moči potrebne za faktorizacijo večjih števil izračunane po prej omenjeni metodi.

Velikost števila n (v bitih)	MIPS let
512	3×10^4
768	2×10^8
1024	3×10^{11}
1536	3×10^{16}
2048	3×10^{20}

Tabela 1: Potrebna računska moč za faktorizacijo z NFS metodo

Podobno ocenimo koliko računske moči potrebujemo, da s Pollard-rho metodo izračunamo diskreten logaritem na eliptičnih krivuljah. Predpostavimo, da MIPS računalnik lahko opravi približno 40.000 seštevanj točk na eliptični krivulji na sekundo. (Ocena temelji na posebej prirejenem vezju s frekvenco ure 40 MHZ, katerega namen je izvajanje operacij na eliptičnih krivuljah nad $GF(2^{155})$ in lahko izvede 40.000 seštevanj na sekundo [9].) Torej to pomeni, da v enemu letu opravi $1,2 \times 10^{12} \doteq 2^{40}$ seštevanj. Če vzamemo za velikost n-ja v bitih 160 (število točk na krivulji), Pollard-rho metoda potrebuje približno 2^{80} seštevanj, kar za MIPS računalnik pomeni $2^{80}/2^{40} = 10^{12}$ MIPS let. Tabela 2 prikazuje koliko računske moči potrebujemo za izračun diskretnega logaritma z uporabo Pollard-rho metode za različne vrednosti števila n (red točke, ki nam določa ciklično podgrupo) [9].

Velikost števila n (v bitih)	$\sqrt{\pi N/2}$	MIPS let
112	2^{56}	$5,7 \times 10^4$
160	2^{80}	$9,6 \times 10^{11}$
186	2^{93}	$7,9 \times 10^{15}$
234	2^{117}	$1,6 \times 10^{23}$

Tabela 2: Računska moč za Pollard-rho metodo

Če primerjamo ti dve tabeli, opazimo da 512 bitni ključ za RSA prinaša isti nivo varnosti kot 112 bitni ključ za ECDL. Enako velja tudi za 1024 bitni RSA in 160 bitni ECDL ključ. Avgusta leta 1999 je skupina strokovnjakov uspela faktorizirati 155 mestno desetiško število RSA-155 (512 bitno število), ki je bilo podano na internetu kot izziv za faktorizacijske algoritme. Za njega so porabili 8000 MIPS let na 300 PC računalnikih (v povprečju 400 MHz-nih in z vsaj 64 MByte-ov RAM-a), katere so poganjali dva meseca [10]. To potrjuje, da 512 bitni ključ res predstavlja samo še šibko varnost, isto velja za 112 bitni ključ pri ECDL. Zaenkrat je 1024 bitni ključ še varen, saj bi za tako število potrebovali 7 milijonov krat več časa in 2650 krat več spomina. To pomeni, da bi potrebovali $1,4 \times 10^9$ računalnikov (v povprečju 500 MHz-nih in z vsaj 170 GByte-ov RAM-a), da bi razbili 1024 bitno število v istem času kot 512 bitno število.

gljivejši računalniki, zraven so podane pripadajoče maksimalne zmogljivost v GFlopih/s (10^9 floating point operations per second).

	Tip računalnika	zmogljivosti (v Gflopih)
1	Cray SV2-27/864 [+4Q02]	2073,6
2	Cray T3E-1200E LC1536	1843,2
3	Cray T3E-900 LC1324	1191,6
4	SGI 2800/250-2304	1152
5	Cray T3E-1350 LC800	1080
6	SGI 3800/400-1064	851,2
7	Cray SV1-18/576 [-4Q02]	691,2
8	Cray T3E-1200E LC540	648
9	Cray T3E-1200 LC396	475,2
10	Paracel FDF3-8T/5460	390
11	Paracel FDF3-8T/5460	390
12	Cray T3E-1200 LC284	340,8

Tabela 3: Cray-evi superračunalniki vgrajeni v Fort Mead-u urejeni po rač. moči

Vzemimo oceno iz prejšnega podpoglavja, da je 1 MFlop/s približno 7 MIPS-ov. Skupna zmogljivost računalnikov v Tabeli 3 je 10^7 MFlopov/s, torej to pomeni $1,4 \times 10^6$ MIPS-ov. Če vzamemo ocene iz Tabele 1, bi ti računalniki za razbitje 512 bitnega ključa za RSA potreboval približno $3 \times 10^4/1,4 \times 10^6 \doteq 8$ dni. Ta številka je sicer zelo nizka, vendar glede na to, da so strokovnjaki uspeli s 300 osebnimi računalniki razbiti ključ v dveh mesecih, verjetno ni daleč od resnice, saj so Cray-i skupaj 1000 krat močnejši. Poglejmo si sedaj večje dolžine ključev. Za 768 bitni ključ, ki pomeni približno 230 mestno desetiško število, potrebujemo 6×10^3 krat več časa. Torej bi ti izbrani Cray-i potrebovali več kot 100 let. Oziroma NSA bi rabila vsaj 100 takih računalnikov, ki bi bili sposobni delati ves čas s polno zmogljivostjo, da bi rešila ta problem v enem letu. Za 1024 bitni ključ pa trenutno tudi NSA sigurno nima dovolj računske moči, saj bi zanj potrebovala kar $3 \times 10^{11}/1,4 \times 10^6 \doteq 2 \times 10^5$ let s Cray-i iz Tabele 3. Tudi 10000 teh Cray-ev ne bi bilo dovolj, saj bi ti rešili problem šele v 20 letih. Odlyzko je v svojem članku iz leta 1995 [8] ocenil, da je bilo takrat 1000 vseh supperračunalnikov po celem svetu.

Te ocene nas pripeljejo do zaključkov, da NSA res izgublja v boju z enkripcijo. Naj se še tako trudi in razvija hitrejše računalnike, je to še vedno premalo, da bi lahko dešifrirala sporočila zašifrirana z daljšimi ključi v sprejemljivem času. To pa zato, ker se lahko hkrati s hitrejšimi računalniki, uporabljajo primerno večji ključi. Tuje vlade danes verjetno uporabljajo vsaj 1024 bitne ključe za skrivanje pomembnih podatkov, to pa je omogočeno tudi teroristom. Zato ni čudno, da se je tako bojevala za kontrolo nad izvozom enkripcijske opreme in omejevala dolžino ključev. To je tudi razlog, zakaj verjetno nismo zadnjič slišali o zlorabi njenega vpliva, pri prodaji enkripcijske opreme, kot je bilo v primeru podjetja Lotus (glej prejšnje poglavje). Za zbiranje informacij jim ostanejo predvsem nešifrirana in šifrirana sporočila s krajšimi ključi. Vendar pa bo takih informacij, uporabnih za NSA, vedno manj, saj se Evropa in ostali vedno bolj zavedajo pomembnosti varovanja svojih podatkov z močnejšo enkripcijo.

5.3 Meritve

Zanima nas kolikšno je razmerje med inštrukcijo in flop (floating point) operacijo ter koliko MIPS-ov (glej prejšnje podpoglavje) so sposobni današnji osebni rčunalniki. S pomočjo teh ocen bomo v naslednjem poglavju ocenili zmogljivost NSA-jevih računalnikov. V ta namen sem napisala preprost program v Borlandc++ (verzija 5.01).

```
Program: Meritev.cpp
//Program izvede count operacij (xor ali floating point mnozenje).

#include <time.h>
#include <stdio.h>
#include <stdlib.h>

#define  count 1000000000

int main(void)
{
   register unsigned long i;  //stevec
   register int a,b;  //Ko merimo flope, sta a in b tipa double.

   randomize();

   for (i=0;i<count;++i) {
     a=rand();
     b=rand();
     a^b;     //Za merjenje flopov imamo na tem mestu a*b.
   }

   return 0;
}
```

Meritve sem opravila na osebnem računalniku Intel Celeron (633 MHz). Najprej sem izmerila čas, ki ga potrebuje zanka, v kateri sta samo dva rand() ukaza brez operacije. Nato sem izmerila čas zanke z operacijo. Ta dva časa sem odštela in delila s count, pri čemer sem dobila čas, ki ga potrebuje Celeron za xor operacijo (ali množenje).

Izmerjen čas za xor je bil 5×10^{-9}, za flop množenje pa 35×10^{-9}. Torej smo dobili oceno, da je 1 MFlops približno 7 MIPS-ov. Ker tudi za xor potrebujemo par inštrukcij (shranitev vrednosti spremenljivk v register, izračun xor-a,...), lahko ocenimo, da je zmogljivost računalnika Celeron 500 do 1000 MIPS-ov. Na Intelovi domači strani ocenjujejo, da je na primer Pentium II (350 MHZ) sposoben 770 MIPS-ov.

5.4 Zmogljivost NSA-jinih računalnikov

Gunter Ahrendt-ov seznam (Most Powerful Computing Sites) [11] uvršča NSA v FT. Meadu na drugo mesto po računski zmogljivosti. V spodnji tabeli 3 so našteti njeni najzmo-

Literatura

[1] D. Kahn: The Codebreakers, hrvaški prevod: (K. in M. Miles), Šifranti protiv Špijuna, tretja knjiga, str. 383-451, Centar za informacije i Publicitet, Zagreb 1979

[2] NSA: organization and functions, facilities, operations, http://www.fas.org/irp/nsa/index.html.

[3] N.Hager: Exposing the global surveillance system, članek. CAQ(2.2.1998), http://mediafilter.org/caq/echelon

[4] P.Becker, D.Campbel, D.Holdsworth, C.Elliot in N.Bogolikos: Development of surveillance technology and risk of abuse of economic information, delovni dokument Evropskega parlamenta (STOA) (1999), http://www.europarl.eu.int/dg4/stoa/en/publi/default.htm

[5] Osnutek najnovejšega poročila Evropskega parlamenta o ECHELONU, (18.5. 2001), http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon_en.pdf

[6] S.Hersh: The Intelligence gap, članek, The New Yorker (6.12.1999), http://cryptome.org/nsa-hersh.htm

[7] B.Drogin: Blackout Reveals Downside of Secrecy, članek, L.A. Times (13.3.2000).

[8] Andrew M. Odlyzko: The Future of Integer Factorization, CryptoBytes **1** (1995), str. 5-12.

[9] The Certicom white paper, The Elliptic Curve Cryptosystem, September 1997, http://www.certicom.com/research.html.

[10] Robert D. Silverman: A cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, Bulletin **13** (April 2000).

[11] Gunter Ahrendt, List of the world's most powerful computing sites, http://www.gapcon.com/listg.html

[12] RSA Laboratories: RSA Laboratories' Frequently Asked Questions About Today's Cryptography, http://rsasecurity.com/rsalabs/faq/index.html

[13] Menezes, Oorschot, Vanstone: Handbook of Applied Cryptography, CRC Press, 1997

[14] Menezes: Eliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993

[15] H. COHEN: A Course in Computational Algebraic Theory, Springer-Verlag, 1993.

Merjenja sem naredila na Intel Celeronu 633 MHz, v BorlanduC++, verzija 5.01

1.merjenje na roke(stoparica)

```
#include <time.h>
#include <stdio.h>
#include <stdlib.h>

#define  count 1000000000

int main(void)
{
   register unsigned long i;
   register int a,b;  //ko merimo flope sta a in b tipa double

   randomize();

   for (i=0;i<count;++i) {
     a=rand();
     b=rand();
     a^b;     //pri flopih je  a*b;
   }

   return 0;
}
```

REZULTATI: tabela pove koliko sekund trajajo zanke (10^9)

	xor	flop
samo zanka	28	32
zanka + operacija	33	68
Razlika	5	36

Razmerje je 7.2

2.merjenje s clock funkcijo (to ste uporabili vi)

```
#include <time.h>
#include <stdio.h>
#include <stdlib.h>

#define  count 1000000000
int main(void)
{
   clock_t start, end;
   double cas;
   register unsigned long i;
   register int  a,b;  //ko merimo flope sta a in b tipa double

   randomize();

   start = clock();
   for (i=0;i<count;++i) {
      a=rand();
      b=rand();

   }
   end = clock();
   cas=(double)(end - start)/(double)CLK_TCK;
   printf("Cas je %8.3f\n",cas);

   return 0;
}
```

REZULTATI: tabela pove koliko sekund trajajo zanke (10^9)

	xor	flop
samo zanka	32	32
zanka + operacija	33	55
Razlika	1	23

Razmerje je 23

****
****

3.merjenje s timing fnc.

```
#include <stdlib.h>
#include <stdio.h>
#include <time.h>
#include <dos.h>
#include <conio.h>


#define count 1000000000

double timing(struct time t2)
//Funkcija timing izmeri cas izvajanja v sekundah glede na cas shranjen v t.
//Ne poganjaj je cez polnoc!!!
{
  struct time t1;   //V t1 shranimo trenutni cas.
  double  casm1, casm2;   //V casm pa izracunamo cas v sekundah.

  gettime(&t1);
  casm1 = t1.ti_hour*360000 + t1.ti_min*6000 + t1.ti_sec * 100 + t1.ti_hund;
  casm2 = t2.ti_hour*360000 + t2.ti_min*6000 + t2.ti_sec * 100 + t2.ti_hund;

  return (double)(casm1 - casm2)/(double)100;
}

int main(void)
{

   struct time t1;
   double cas;
   register unsigned long i;
   register int a,b;     //ko merimo flope sta a in b tipa double

   randomize();

   gettime(&t1);

   for(i=0;i<count;++i){
    a=rand();
    b=rand();
    a^b;        //pri flopih je  a*b;
   }
   cas = timing(t1);

   printf("\nCas za zanko %.2f ", cas);
   return 0;
}
```

REZULTATI: tabela pove koliko sekund trajajo zanke (10^9)

	xor	flop
samo zanka	28	28
zanka + operacija	33	46
Razlika	5	18

Razmerje je 3.6

****
****
poskus merjenja vec xor operacij (samo stopanje)

```
for (i=0;i<count;++i) {
   a=rand();
   b=rand();
   c=rand();
   d=rand();
   e=rand();
   f=rand();

   a^b;
   c^d;
   e^f;
```

Za count < (10^9) je zanka brez treh xor trajala isto kot s tremi xori,
na primer za (5*10^8) 50 sekund, pri (10^9) pa je bila razlika samo 3 sekunde.
Identicne rezultate sem dobila, ce sem naredila vseh 15 razlicnih xor operacij
(a^b; c^d; e^f; b^d; c^e; a^f; d^e; a^c; b^e; c^f; a^d; b^c; d^f; a^e; b^f;)