

Matej Kovačič

Javno dostopna kriptografija

NEST, 2005

sobota, 23. julij 2005

I. del
Osnovni pojmi

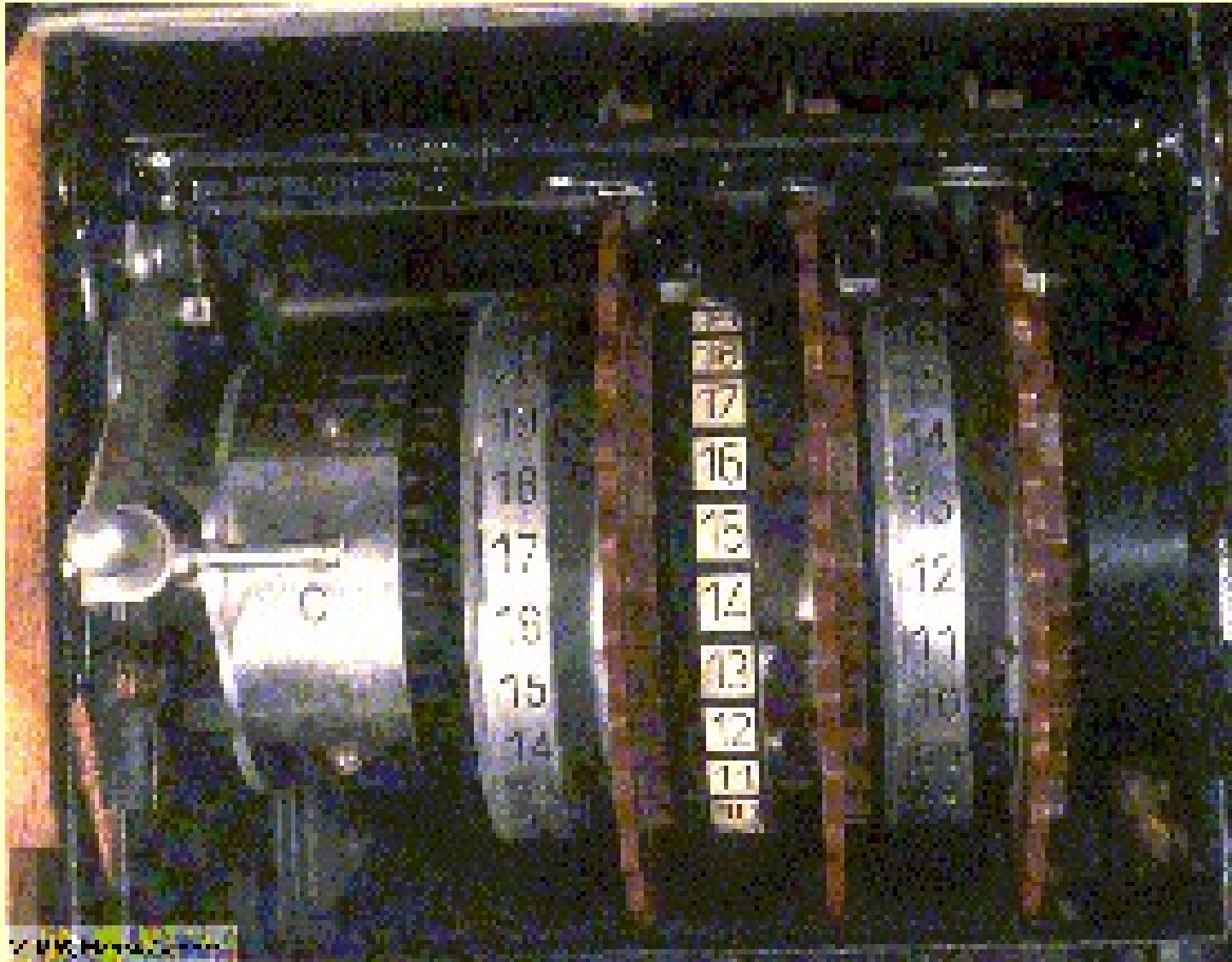
Osnovni pojmi

- **Varnostna aplikacija mora zagotoviti naslednje:**
 - **zaupnost (*confidentiality*);**
 - **celovitost (*integrity*);**
 - **overjanje (*authentication*);**
 - **preprečevanje tajenja (*nonrepudiation*);**
 - **kontrolno dostopa (*access control*).**

- **Beseda kriptologija izvira iz grškega izraza *kryptos logos*, ki pomeni skrita beseda, prvi pa jo je v angleščini uporabil sir Thomas Browne leta 1658.**

- **Kriptologija - veda o tajnosti, šifriranju, zakrivanju sporočil (*kriptografija*) in o razkrivanju šifriranih podatkov (*kriptoanaliza*). Uporabljata se še pojma enkripcija (*šifriranje*) in dekripcija (*dešifriranje*). Osnovno sporočilo ponavadi imenujemo čistopis (*cleartext, plaintext*), zašifrirano pa šifropis ali tajnopis (*kriptogram, ciphertext*).**

- **Sporočilo po nekem postopku (*algoritmu, metodi*) spremenimo v kriptirano sporočilo, pri tem uporabimo določene vrednosti za parametre v algoritmu, ki jim rečemo ključ. Sogovornika se morata torej dogovoriti o algoritmu in ključu, da si lahko pošiljata šifrirana sporočila.**



- **Šifrirni stroj Enigma.**

Vojak je sporočilo šifriral tako, da je vtipkal posamezno črko in zapisal črko, ki se mu je osvetlila. Za presledke je vtipkal črko Z, števila pa je vtipkal z besedami. Naslovnik šifriranega sporočila je moral imeti stroj z enakimi rotorji (letalstvo je imelo svoje kombinacije, mornarica svoje,...). Spreminjali so tako začetne položaje rotorjev kot njihov vrstni red.

Osnovni pojmi - algoritmi

- Pri varovanju podatkov uporabljamo simetrične, asimetrične in zgostitvene algoritme.
- **Simetričnimi algoritmi** ali algoritmi z zasebnim ključem: imamo samo en ključ, s katerim zašifriramo in dešifriramo sporočilo. Običajno so ti algoritmi hitri, težko pa je varno izmenjati ključ. Problem predstavlja tudi število ključev - vsak uporabnik mora imeti za vsakega dopisovalca svoj ključ.
- **Asimetrični algoritmi** ali algoritmi z javnim ključem: uporabnik ima dva ključa, enega objavi, drugi ostane tajen. Vsi, ki mu hočejo poslati sporočilo, bodo uporabili njegov javni ključ za šifriranje sporočila. Dešifriral pa ga bo lahko le on sam s svojim tajnim ključem in javnim ključem pošiljatelja. Te metode so računsko bolj zahtevne in zato počasnejše kot simetrične.
- **Zgostitveni algoritmi** poljubno dolg tekst preslikajo v število fiksne dolžine, kar je uporabno za digitalni podpis. Najbolj znana algoritma sta MD5 in SHA.

Osnovni pojmi – varnost algoritmov

- Kdaj je algoritem varen? Bistveno je, da je algoritem **javno objavljen** in da so ga imeli možnost preizkusiti vodilni kriptanalitiki.
- Kerchoffsov zakon, pravi, da je dober šifrirni sistem varen, tudi če je o njem znano vse, razen šifrirnega ključa. Varnosti ni mogoče zagotoviti s pomočjo skrivanja (tim. '*security through obscurity*').
- Bruce Schneier: "*Ne spominjam se nobenega kriptografskega sistema razvitega na skrivaj, v katerem ne bi, potem ko je bil razkrit javnosti, kriptografska skupnost našla napake.*"
- Napad s preizkušanjem vseh možnih kombinacij bitov ključa (*brute-force attack*), napad s slovarjem (*dictionary attack*), napad v primeru znane dolžine ključa, ostali "matematični" napadi.
- **Analiza prometa** med posameznimi vozlišči.
- Leta 1924 je Alexander von Kryha začel prodajati šifrirno napravo, katerega kriptogram so štirje ameriški kriptanalitiki uspeli razbiti v dveh urah in 41 minutah. Kljub temu se je naprava še naprej uspešno prodajala, nemška diplomacija pa naj bi jo uporabljala še do 50-tih let 20. stoletja.
- Martin Gardner je avgusta 1977 v reviji Scientific American objavil 129 številko dolgo število in ponudil 100 dolarjev za razbitje na faktorje. Uganko je rešila mednarodna skupina z več kot 600 prostovoljci jeseni 1994.

Osnovni pojmi – simetrični algoritmi

- Delimo jih na dve skupini:
 - algoritmi za tekoče šifriranje (*stream ciphers*): sporočilo šifriramo bit za bitom;
 - algoritmi za šifriranje blokov (*block ciphers*): sporočilo razbijemo na bloke in vsak blok posebej šifriramo.
- Pri prvem načinu šifriramo tako, da kombiniramo bit ključa in bit sporočila. Če uporabimo kratek, ponavljajoč ključ, postopek ni varen - s kombiniranjem zašifriranega teksta je razmeroma lahko ugotoviti najprej dolžino ključa, potem vrednost ključa in nato dešifrirati sporočilo. Nasprotno pa je ta sistem nezlomljiv, če se ključ ne ponavlja in je povsem naključen niz bitov (*one-time pad*), vendar je velik problem kako zagotoviti naključnost.
- Večina algoritmov, ki jih danes uporabljamo v civilnih organizacijah, je blokovnih: sporočilo razbijemo na bloke, in vsak blok preoblikujemo in kombiniramo s ključem. Zagotoviti je potrebno, da so v izhodnem bloku zabrisani vsi vzorci iz vhodnega bloka - skratka, da izgleda kot naključen niz bitov.
- Za vse dobre simetrične algoritme velja, da se izhoda **ne da kompresirati** za več kot nekaj odstotkov.

Osnovni pojmi – simetrični algoritmi

- Najbolj znani simetrični algoritmi so:
 - DES ali DEA (Data Encryption Standard/Algorithm), ki sta ga razvila NIST (National Institute of Standards and Technology) ter IBM;
 - RC2, RC4, RC5 - je razvil Ronald Rivest. RC4 je tekoč šifrirni algoritem z variabilno dolžino ključa do 2048 bitov. Vgrajen je v brskalnike kot del protokola SSL oziroma TLS, uporablja pa 128-bitni ključ;
 - IDEA (International Data Encryption Algorithm): razvila sta ga James L.Massey in Xuejia Lai v Zuerichu;
- Ameriška organizacija za standarde NIST je septembra 1997 razpisala natečaj za naslednika algoritma DES. Izmed 15 kandidatov so se v finale uvrstili naslednji algoritmi, ki so vsi uspešno prestali testiranja:
 - MARS (IBM)
 - RC6 (RSA Laboratories)
 - Rijndael (Joan Daemen, Vincent Rijmen)
 - Serpent (Ross Anderson, Eli Biham, Lars Knudsen)
 - Twofish (Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson)
- Postopek za izbiro AES (Advanced Encryption Standard) je bil zaključen 2. oktobra 2000, ko je bil izbran algoritem Rijndael.

Osnovni pojmi – asimetrični algoritmi

- Asimetrični algoritmi za šifriranje uporabljajo drugačen ključ kot za dešifriranje.
- Asimetrični algoritmi se uporabljajo za izmenjavo skupnih ključev in za digitalno podpisovanje, za masovno šifriranje podatkov pa ne, ker so počasnejši od simetričnih algoritmov.
- Asimetrični algoritmi uporabljajo za šifriranje tako transformacijo, za katero je težko ali nemogoče izvesti inverzno transformacijo, če nimamo dodatne informacije oz. zasebnega ključa.
- Za take transformacije se uporablja izraz *One-Way Function* oziroma *Trap-door one-way function*: če imamo neko dodatno informacijo (trap-door, zasebni ključ) je inverzna operacija lahka, sicer pa skoraj nemogoča.

Osnovni pojmi – asimetrični algoritmi

- Prvi znani algoritem z javnim ključem za šifriranje podatkov je Merkle-Hellmanova metoda z nahrbtniki, vendar ni več v uporabi.
- Danes se najbolj uporablja algoritem RSA, razvit leta 1977, ki ima ime po svojih avtorjih (Ronald Rivest, Adi Shamir, Leonard Adleman). Metoda je bila v ZDA patentirana. Ker pa je bil opis metode objavljen pred vložitvijo zahtevka za patent, so lahko RSA uporabljali brez licenčnine povsod po svetu, razen v ZDA.
- Asimetrični algoritmi, ki temeljijo na eliptičnih krivuljah (*ECC - Elliptic Curve Cryptosystems*). Ideja je znana že od leta 1985. V primerjavi z RSA zadoščajo krajši ključi, zato kaže, da bodo v bodočnosti ti algoritmi prevladali.
- Diffie-Hellman: postopek za izdelavo in izmenjavo skritega ključa po javnem omrežju
- ElGamal: digitalni podpis, enkripcija
- RSA: digitalni podpis, enkripcija
- ECC: digitalni podpis, enkripcija

Osnovni pojmi – primer šifriranja

- **Primer šifriranja besede "INTERNET"**
- **Cezarjev algoritem (a -> a+1 po modulu 25):**

JOUFSOFU

- **PGP:**

-----BEGIN PGP MESSAGE-----

Version: PGP Personal Security 7.0.3

qANQR1DBwU4DSfeOJ5LXyx4QCADL1H+hJPOSTwCVqDkzHv1fwzwL3V5vOegelXOg
SH/HF3qlCkhgfK4Qa2gp7SBuoXVenfY7vEzmCFLekc9ZJWgrtiyo9oVN6jzyBPgf
JmicJTBzrVAGY/CdS5F/N66e/KgVxfNGJo4oHxQWGdvyi/p4AayQMdV0RzQeWxZk
9t1Yp0bDD08dM0xEgm190ZUIBwgwY7LLnZd+la+DWeLoZmf8D4LUwq/bNNmVCH0Z
TkQY7fis4X9bYqFnpHodtkbgyN3/SE0sdE4rOVxHyKcVcgVrCbhFrnUMj+c1/XVA
ELiHA8JGQc+W1Rxs5sBQ9uBvnOAoB4/6t4JyrgPFtyOL9bUmCAD0ta+kLHVXWZLZ
1dMVI2CnHzTXxV6LdcQRrGhOU1J+9rtAZIMNdKUuoTwgH1ReFRAY3hSQYxaVrSul
4qj2Mt+Vm0KY1sXTFGZGCJZVrWeLWNtSr2kU02h6j9kBLR7LwvHwA2/LZ+yRDB/c
NMHhSGm9qghkKr9rpEqc+fpMNXxvBTiRcM9YFNhvLA6xaWJmtch/+xLmQdeci4on
bV1ZbUgVtCKFmvIzI+4WRRIZXi7ndB0PanhGhThQwa0R/n+HgX5iVUNVrJf2Nz19
/LaAuF93aEdIxGdn6hqttxd5weLQI9DMXGiuvYBVHAtpoCcQ1TWBJ1umulxhpEGt
eJJrXjXlyWwgehYpDAPAJn4rU5BUH3ca1C58AnSk6pACwZiT8Vk4w5u2skiTp1Gc
Fs3tRApGtQCEcn1Ea8fQ415qfO23WjPgv3w7OjGEC9ZV84ac0uRRTQECgFY3w4g/
PGIKIYMK2bBqzb6t70XwGo2YOsY=

=Dim8

-----END PGP MESSAGE-----

II. del

Vojna proti javno dostopni kriptografiji

Pojav javno dostopne kriptografije

- Kriptografija je znana že skoraj 4000 let. Prvi primer zapisane kriptografije so egiptovski nestandardni hieroglifi, ki so se pojavili okrog leta 1900 pr. n. š.
- Sodobna zahodna kriptografija razvila kot posledica moderne diplomacije. V Benetkah je Giovanni Soro leta 1506 in 1510 opravil prve večje uspešne kriptanalize šifriranih sporočil.
- Leta 1861 se v ZDA pojavi prvi kriptografski patent.
- Leta 1923 je Arthur Scherbius začel proizvajati šifrirne stroje Enigma, katerih izboljšane različice so kasneje med drugo svetovno vojno v vojaške namene uporabljali Nemci.
- V 30-tih letih 20. stol. je kriptografija začela postati mehanizirana. Sprva so za šifriranje in razbijanje šifer uporabljali mehanske naprave (npr. pojska Bombe), kasneje pa računalnike s procesorji.
- Moderno kriptografijo je ustvaril telegraf. S pojavom radia, ki je omogočal enostavno nepooblaščno prisluškovanje, pa se je razvila moderna kriptanaliza.

Pojav javno dostopne kriptografije

- Revolucijo v kriptografiji je povzročilo odkritje asimetrične kriptografije (Whitfield Diffie in Martin E. Hellman, leta 1976) oziroma odkritje algoritma RSA leta 1977 (Ronald L. Rivest, Adi Shamir in Leonard M. Adleman).
- Po nekaterih ugibanjih naj bi asimetrično kriptografijo že pred tem verjetno odkrili v ameriški NSA v 1960-tih letih, zagotovo pa nekoliko kasneje tudi v britanski tajni službi *Government Communications Headquarters* (GCHQ), vendar pa svojih odkritij niso nikoli javno objavili.
- Leta 1991, je računalniški programer Philip R. Zimmerman napisal računalniški program PGP (*Pretty Good Privacy*), namenjen šifriranju elektronskih sporočil in računalniških datotek. PGP je za šifriranje uporabljal algoritem RSA. Program je tekel na popolnoma običajnih računalnikih PC in je bil za tedanje standarde uporabniške prijaznosti razmeroma enostaven za uporabo, predvsem pa zelo učinkovit.
- Zimmerman je PGP javno objavil na internetu, ostalo je zgodovina.

Vojna ameriške vlade proti javno dostopni kriptografiji

DES

- V poznih 60-tih letih 20. stoletja so pri IBM zaradi strahu pred računalniškim kriminalom pričeli razvijati kriptografijo za komercialne namene.
- Leta 1971 so razvili šifrirno napravo Lucifer - poseben algoritem, ki je bil implementiran v majhnem čipu. V tistem času je bila to najmanjša šifrirna naprava na svetu.
- Leta 1973 je ameriški *National Bureau of Standards* (NBS; iz njega je kasneje nastal NIST) želel pripraviti standard za šifriranje civilnih komunikacij.
- Uslužbenci NSA so redno obiskovali IBM in spremljali njihov napredek. Lucifer je uporabljal 128-bitni šifrirni ključ, vendar pa je NBS v sodelovanju z NSA Lucifer za civilno uporabo priredila. 128-bitni šifrirni ključ so skrajšali na 64 bitov, pri čemer pa je bilo 8 bitov kontrolnih in je bila torej dejanska dolžina ključa samo 56 bitov, poleg tega pa so priredili še nekatere matematične postopke v samem algoritmu (S-boxe).
- Modificiran algoritem je NBS januarja 1977 potrdil kot standard *Data Encryption Standard* (DES) in sicer potem, ko je revizija NSA ugotovila, da naj bi v njem ne bilo nobenih statističnih ali matematičnih slabosti.

Vojna ameriške vlade proti javno dostopni kriptografiji

DES

- Preden je spremenjeni Lucifer postal standard, je bil deležen številnih kritik. Hellman in Diffie sta izračunala, da bi bilo mogoče s posebnim računalnikom za 20 milijonov USD 56-bitni DES v povprečju razbiti v manj kot pol dneva, vsaka rešitev (razbitje kriptograma) pa bi stala 5000 dolarjev. V 10 letih bi tak računalnik stal samo 200.000 USD, vsaka rešitev pa le 50 USD.
- NBS je v odgovor kritikam osnoval dve delavnici na temo DES-a, na katerih so prišli do zaključka, da bi razbijanje DES-a trajalo 17.000 let.
- Vendar pa naj bi IBM že med razvojem algoritma odkril matematično bližnjico za razbijanje civilne različice DES-a, to odkritje pa je zaradi zahtev ameriške NSA ostalo v tajnosti. V letih 1990 in 1991 sta kriptografa Eli Biham in Adi Shamir predstavila novo vrsto kriptanalize, ki sta jo poimenovala diferencialna kriptanaliza (ang. *differential cryptanalysis*). Civilna različica DES naj bi bila prirejena tako, da je bila učinkovitost do tedaj neznanega napada z diferencialno kriptanalizo povečana.
- Julija 1998 je John Gillmore iz fundacije *Electronic Frontier Foundation* predstavil napravo DES Cracker, ki je s pomočjo metode grobe sile (ang. *brute-force*) in s pomočjo distribuiranega procesiranja podatkov prek interneta razbila DES v 22 urah. Istega leta je skupina kriptografov predstavila tudi DES Cracker za 250.000 dolarjev, ki je DES razbila v manj kot treh dneh.

Vojna ameriške vlade proti javno dostopni kriptografiji

Omejevanje svobode govora

- NSA je že leta 1957 ugotovila, da je potrebno zagotoviti dotok znanja iz akademskih krogov (poročilo Bakerjevega komiteja). Vendar pa si v NSA niso želeli odprtega sodelovanja, saj niso želeli, da kriptološki izsledki postanejo javno znani.
- Med leti 1956 in 1962 je potekal projekt *Lightening*, pri katerem so sodelovale ameriške univerze. Projekt je služil za zagon raziskav na področju kriptografije.
- Po objavi RSA algoritma septembra leta 1977 je bil Rivest povabljen na konferenco *Institute of Electrical and Electronics Engineers*, kjer naj bi predstavil svoje delo. Vendar pa je organizator konference prejel pismo nekega uslužbenca NSA, v katerem je bilo zapisano opozorilo, da bo Rivestovo predavanje verjetno predstavljalo kršitev zakona *International Traffic in Arms Regulations* (ITAR), saj bodo na konferenci prisotni tudi tuji državljani, IEEE pa je sodelovala tudi s Sovjetsko zvezo.

Vojna ameriške vlade proti javno dostopni kriptografiji

Omejevanje svobode govora

- NSA je kasneje zanikala povezavo z Meyerjevim pismom in zaradi prvega amandmaja ameriške ustave je bil prispevek na konferenci vseeno predstavljen.
- Kljub temu je NSA želela preprečiti vsakršno javno razpravo o kriptografiji. Direktor NSA Bobby Ray Inman je v javnem govoru marca 1979 dejal: *“obstaja zelo realna in kritična nevarnost, da bo neomejena javna razprava o kriptoloških zadevah resno ogrozila zmožnost vlade, da opravlja obveščevalne dejavnosti (ang. signals intelligence – SIGINT), in zmožnost vlade, da zaščiti informacije v zvezi z nacionalno varnostjo pred tujimi sovražnimi izrabami”*.
- Vendar pa je bilo zaradi svobode govora nemogoče raziskovalcem preprečiti javno objavo svojih odkritij, zato se je NSA odločila na raziskovalce pritisniti s finančnimi ukrepi.

Vojna ameriške vlade proti javno dostopni kriptografiji

Finančni pritiski na raziskovalce

- NSA je preko ekonomskih pritiskov lahko dosegla sodelovanje velikih podjetij, tega pa ni mogla storiti pri svobodnih in akademskih raziskovalcih.
- Vendar pa se je izkazalo, da večino svobodnih raziskovalcev financira *National Science Foundation* (NSF).
- Leta 1977 sta dva uslužbenca NSA obiskala direktorja NSF in ga obvestila, da verjetno krši zakon, ker financira kriptografske raziskave *Massachusetts Institute of Technology*. NSA je trdila, da obstaja predsedniška direktiva, ki daje NSA pooblastilo, da se edina ukvarja s kriptografijo.
- Po preverjanju se je izkazalo, da ne obstaja noben takšen ukaz. NSA je nato predlagala sodelovanje v procesu recenziranja predlaganih projektov.
- Kasneje je predlagala, da naj bi v okviru sodelovanja z NSF kriptografske raziskave financirali oni, raziskovalci pa bi bili **prisiljeni** sprejeti financiranje NSA (in njihove pogoje glede objav).
- Kasneje je bil ta sistem zavržen in sprejeta je bila odločitev, da se raziskovalci smejo sami odločiti, čigavo finančno pomoč bodo sprejeli.

Vojna ameriške vlade proti javno dostopni kriptografiji

Omejevanje patentiranja

- V povojnih letih je večino kriptografskih patentov imela v lasti NSA, plačevanje licenčnine pa je celo povzročalo manjše napetosti med NSA in GCHQ.
- Leta 1977 sta samostojni raziskovalec Carl Nikolai in profesor iz University of Wisconsin George Davida neodvisno želela prijaviti vsak svoj patent iz področja kriptografije. Nicolai je izumil šifrirni telefon, ki ga je imenoval *Phasorphone*, prodajati pa ga je nameraval po zelo dostopni ceni okrog 100 dolarjev. Davida pa je želel patentirati tokovni šifrirnik (ang. *stream cipher device*, naprava za šifriranje toka podatkov, npr. zvoka).
- Vendar pa sta oba izumitelja iz patentnega urada dobila ukaz, da je njun izum postal tajen na podlagi leta 1951 sprejetega *Invention Secrecy Acta* in da o njem ne smeta govoriti.

Vojna ameriške vlade proti javno dostopni kriptografiji

Omejevanje patentiranja

- Izumitelja sta se na to odločitev pritožila in o vsem skupaj obvestila revijo Science. Nicolai je za Science izjavil, da gre po njegovem mnenju za načrt NSA, kako omejiti zasebnost Američanov, in da se argument o nacionalni varnosti uporablja samo kot krinka
- Direktor NSA je kasneje izjavil, da je šlo v primeru Nicolaia za nestrinjanje med ocenjevalci, zaradi česar je prišlo do napake, prav tako pa naj bi do birokratske napake prišlo tudi v primeru Davide. NSA je tajni ukaz umaknila, kasneje pa je ameriško pavo sodno ministrstvo presodilo, da so takšne omejitve neustavne.
- Vendar pa je bilo ravnanje Davide in Nicolaia prej izjema kot pravilo, saj takšni tajni ukazi podjetjem navadno koristijo, ker se s tem čas patentne zaščite poveča.

Vojna ameriške vlade proti javno dostopni kriptografiji

Omejevanje izvoza kriptografskih proizvodov

- Najprej so se pojavili predlogi, naj se v ZDA dovoli samo uporaba šibke kriptografije, vendar to ne daje ustrezne zaščite, takšne omejitve pa bi bile zelo verjetno v nasprotju s svobodo govora.
- NSA je zato skušala s pomočjo zakona *International Traffic in Arms Regulations* oziroma *US Export Regulations*, zaustaviti izvoz kriptografskih proizvodov iz ZDA. Od podjetij so zahtevali, naj opustijo določene kriptografske produkte ali pa naj vanje vgradijo 'stranska vrata'.
- Tako so skušali omejiti izvoz programa *Pretty Good Privacy* leta 1991, kar pa je bilo zaradi interneta in brezplačnosti programa neučinkovito.

Vojna ameriške vlade proti javno dostopni kriptografiji

Omejevanje izvoza kriptografskih proizvodov

- Kasneje se je izkazalo, da ameriški izvozni predpisi prepovedujejo samo izvoz kriptografske programske opreme v elektronski obliki, kar so izkoristili člani organizacije PGP International, ki so leta 1997 izvorno programsko kodo programa PGP 5.0 natisnili v 12 knjigah (preko 6000 strani) in jo povsem v Evropi pretvorili nazaj v digitalno obliko.
- Izvozni predpisi so bili neučinkoviti ter deležni številnih kritik zaradi finančne škode, ki so jo povzročali ameriškim podjetjem. Ameriški proizvajalci so morali za zunanja tržišča proizvesti oslABLJENE kriptografske proizvode. Pridobitev izvoznega dovoljenja je za podjetje pomenila priznanje, da njihovi proizvodi niso dovolj varni.
- Francija je konec 90-tih let odločila liberalizirati svojo politiko do kriptografije z argumentom, da bi *"liberalizacija šifrirne tehnologije omogočila francoskim podjetjem poln vstop na trg elektronske trgovine, ki ga trenutno obvladujejo podjetja iz ZDA"* (izjava francoskega ministra za industrijo Christiana Pierreta 29. avgusta 1997. ZDA so izvzna dovoljenja sprostile leta 2000.

Vojna ameriške vlade proti javno dostopni kriptografiji

Vsiljevanje kriptografskih standardov

- Naloga *National Bureau of Standards* oziroma njegovega naslednika *National Institute of Standards and Technology* je priprava državnih standardov za civilno sfero. Za kriptografske standarde velja, ki se jih morajo držati vse državne agencije, za podjetja pa niso obvezni, razen če sodelujejo z državnimi agencijami. Kljub temu se jih podjetja prostovoljno držijo in sicer zaradi večje združljivosti in povezljivosti.
- NSA in FBI sta sjušali kot standard postaviti take kriptografske produkte, ki bi državnim organom omogočali dostop do šifriranih podatkov. Drugi kriptografski pripomočki, ki tem standardom ne bi ustrezali, ne bi dobili licence, njihova uporaba pa bi bila omejena.
- Ena izmed različic tega predloga je celo predvidevala zakonsko prepoved uporabe nekaterih (močnih) kriptografskih metod, ki ne bi bile v skladu s standardi.
- Drugi predlog je predvideval, da bi močno šifriranje dovolili samo v zaprtem omrežju (mrežno šifriranje (ang. *link encryption*), podatke je mogoče prestrezati pri izhodu iz sistema.

Vojna ameriške vlade proti javno dostopni kriptografiji

Vsiljevanje kriptografskih standardov

- RSA zaradi nasprotovanja NSA ni postal standard. NBS je skupaj z NSA začel razvijati standarde za javno dostopno kriptografijo, projekt se je imenoval *Capstone*.
- Člani *House Government Operations Committee* so temu nasprotovali, saj se je NSA v preteklosti trudila zaustaviti ali pa omejevati raziskave v kriptografiji.
- Kljub temu NIST ni dobil ustreznega financiranja. V primerjavi z NSA, ki je imela leta 1987 na *netajnem* računalniško-varnostnem programu 300 zaposlenih in proračun v vrednosti 40 mio. USD, je imel NIST istega leta na voljo le 1,1 mio. USD in 16 zaposlenih, do leta 1990 pa se je njegov proračun povečal na 1,9 mio. USD, število zaposlenih pa na 33.
- Poleg tega sta NIST in NSA podpisala poseben memorandum, kjer se je NIST zavezal, da se bo o vseh vprašanjih povezanih s kriptografijo posvetoval z NSA. NSA si je tako zagotovila, da bo še naprej igrala pomembno vlogo pri omejevanju javno dostopne kriptografije. Kasneje je NSA ponudila svoj algoritem, ki pa je bil počasen in oslabljen.

Vojna ameriške vlade proti javno dostopni kriptografiji

Sistem depozita šifrirnih ključev

- Septembra 1992 je podjetje AT&T najavilo novo napravo namenjeno šifriranju telefonskih komunikacij, imenovano *Surity 3600*, naprava pa ni uporabljala šifrirnih algoritmov odobrenih s strani NSA.
- Aprila 1993 je ameriška vlada objavila predlog *Escrowed Encrypted Standarda*. Gre za sistem depozita šifrirnih ključev (t.i. *key escrow* sistem), ki bi dopuščal uporabo močnih kriptografskih algoritmov, od posameznikov pa bi zahteval, da svoje ključe deponirajo pri za to pooblaščenih agenciji.
- Kmalu se je pojavila implementacija tega sistema za telefone, Clipper čip. Clipper je uporabljal šifrirni algoritem Skipjack, ki ga je razvila NSA in je bil do junija 1998 tajen.

Vojna ameriške vlade proti javno dostopni kriptografiji

Sistem depozita šifrirnih ključev

- Pravosodno ministrstvo je kmalu po javni predstavitvi Escrowed Encrypted Standarda pri AT&T-ju naročilo 9000 telefonov s Clipper čipom, poleg tega pa so začeli pritiskati na vse proizvajalce kriptografskih produktov, naj 'prostovoljno' sprejmejo njihovo rešitev.
- NSA je celo začela kampanjo pri tujih državah, da bi sprejele Clipper standard, seveda pa pri tem niso bili preveč uspešni. ZDA so začele pritiskati na OECD, naj sprejme kriptografske smernice, po katerih bi sistem depozita šifrirnih ključev postal mednarodni standard. Pritiskali so tudi na EU, G7, G8 in Svet Evrope.
- Matt Blaze iz AT&T je maja 1994 dokazal, da je mogoče polje šifrirane podatke pokvariti na tak način, da bo sejni ključ ne bo dostopen preiskovalnim organom. To je celotno idejo sistema depozita gesel povsem izničilo. Dva meseca kasneje je podpredsednik ZDA predlog javno umaknil.

Mednarodni poskusi omejevanja kriptografije

Wassenaarski sporazum

- Wassenaarski sporazum je dokument o prepovedi izvoza tehnologije dvojne rabe (ang. *dual use technology*) v nekatere nedemokratske države. Wassenaarski sporazum nima statusa mednarodne pogodbe, pač pa izdaja neobvezna priporočila.
- Leta 1998 je Wassenaar Secretariat predstavil nov seznam tehnologije dvojne rabe, na katerem so se znašli tudi nekateri kriptografski proizvodi. Ti produkti, ki so ostali tudi na revidiranem seznamu iz leta 2003, so simetrični algoritmi, ki uporabljajo šifrirne ključe daljše od 56 bitov, rešitve za faktorizacijo celih števil večjih od 512 bitov ter rešitve za izračun nekaterih diskretnih algoritmov.
- Izključeni pa so tisti produkti, ki šifriranje uporabljajo za zaščito avtorskih pravic in intelektualne lastnine (npr. regijska zaščita na DVDjih), ter nekateri produkti, ki se uporabljajo v bančništvu.

Mednarodni poskusi omejevanja kriptografije

Kriptografske smernice OECD

- ZDA so leta 1996 preko pravosodnega ministrstva, FBI in NSA začele pritiskati na OECD, naj sprejme kriptografske smernice, s čimer bi sistem depozita šifrirnih ključev postal mednarodni standard.
- A OECD je marca 1997 sprejela smernice o kriptografski politiki, v katerih je podprla neomejen razvoj in uporabo kriptografskih proizvodov. Razlogi za to pa so bili predvsem ekonomski (razvoj elektronskega poslovanja), in ne človekove pravice.
- Smernice pravijo: *“razvoj in nabava kriptografskih metod sme biti omejena samo s trgom v odprtem in konkurenčnem okolju”*.
- Te smernice je podprla tudi G8 na vrhunskem zasedanju v Denverju leta 1997.

Mednarodni poskusi omejevanja kriptografije

Svet Evrope

- Septembra 1995 je Svet Evrope sprejel Priporočilo Sveta Evrope št. R(95) 13 glede problemov kazensko procesnega prava povezanega z informacijskimi državami. V njem so zapisali, da *"morajo imeti preiskovalni organi pooblastilo, da osebam, ki imajo nadzor nad podatki v računalniških sistemih, ukažejo, da jim omogočijo dostop do računalniškega sistema in podatkov"* (10. člen).
- Poudarili so, da imajo operaterji javnih telekomunikacijskih storitev posebno dolžnost izvesti vse tehnične ukrepe, ki omogočajo zakonito prestrezanje telekomunikacij ter identifikacijo uporabnikov (11. in 12. člen).
- Glede uporabe šifriranja pa 14. člen priporoča sprejem ukrepov, ki bodo zmanjšali negativne učinke uporabe kriptografije, pri čemer pa ti ukrepi *"ne smejo prizadeti legitimne uporabe kriptografije bolj, kot je to nujno potrebno"*.

Zagotavljanje možnosti za nadzor kljub uporabi kriptografije

- Ker s prepovedjo kriptografije niso uspeli, so se preiskovalni organi vrnili nazaj k bistvu problema: kako si zagotoviti možnosti za nadzorovanje.

Operacija 'Root Canal' in vgrajevanje 'stranskih vrat'

- Konec 80-tih let 20. stoletja je FBI začel izvajati operacijo Root Canal (*Operation Root Canal*), v okviru katere je želel telefonske operaterje prepričati, da v svoje telefonske centrale vgradijo tehnične zmožnosti za oddaljeno prisluškovanje ter dostop do nešifriranih komunikacij.
- FBI-jevi predstavniki so trdili, da je preiskovanje kaznivih dejanj v krizi, saj naj ne bi bilo več mogoče uporabljati prisluškovanja.
- FBI je leta 1991 Kongresu predlagal sprejem določila, ki bi od proizvajalcev in ponudnikov elektronskih komunikacijskih sistemov zahteval, da v svoje proizvode vgradijo nadzorno tehnologijo, tim. 'stranska vrata'.
- Telekomunikacijska podjetja so FBI-jeve zahteve zavrnila v glavnem zaradi visokih stroškov.

Zagotavljanje možnosti za nadzor kljub uporabi kriptografije

Operacija 'Root Canal' in vgrajevanje 'stranskih vrat'

- Po nekaj letih lobiranja in po tem, ko je vlada telekomunikacijskim podjetjem ponudila pol milijarde dolarjev za pokritje stroškov, je leta 1994 Kongres sprejel *Communications Assistance for Law Enforcement Act* (CALEA), znan tudi pod imenom *Digital Telephony Act*.
- Kasneje se je izkazalo, da je FBI v okviru operacije Root Canal sprožil usklajeno javno kampanjo za sprejem ustrezne zakonodaje. Pridobljeni FBI-jevi dokumenti dokazujejo, da FBI ni imel nikakršnih tehničnih problemov s prisluškovanjem.
- ACLU v odprtem pismu kongresniku Brooksu 22. septembra 1994: predlog CALEA "ustvarja predpostavko, ki je nevarna in brez primera, da namreč vlada ... lahko od zasebnikov zahteva da ustvarijo poseben dostop". To je po njihovem mnenju primerljivo z "zahtevo, da bi vsi graditelji morali v nove hiše vgraditi nadzorne kamere, ki bi jih lahko uporabljala vlada".
- EPIC: "Prvič se bo zgodilo, da bo zakonodaja zahtevala, da morajo biti naša sredstva za komuniciranje oblikovana tako, da olajšajo vladno prestrezanje. Če smo vedno priznali potrebo preiskovalcev, da dobijo preiskovalne informacije na podlagi sodnega naloga, pa nikoli nismo sprejeli stališča, da mora biti uspeh take preiskave zagotovljen...".

Zagotavljanje možnosti za nadzor kljub uporabi kriptografije

Izogibanje kriptografski zaščiti

- Nekaterе države so poiskušale sprejeti določila, ki bi od posameznikov zahtevala, da na podlagi sodne odredbe preiskovalcem izročijo svoje ključe, ali pa dovolijo dostop do nešifriranih podatkov.
- Vendar pa zakonodajalec k razkritju šifrirnih ključev lahko prisili le posameznike, ki te ključe hranijo za druge osebe, ne more pa prisiliti osumljencev, da izdajo svoje lastne ključe.
- Na podlagi 6. člena Evropske konvencije o človekovih pravicah imajo namreč posamezniki pravico do molka v kazenskem postopku, enako v ZDA, kjer 5. amandma prepoveduje samoobtožbo.

Zagotavljanje možnosti za nadzor kljub uporabi kriptografije

Primer Scarfo

- Leta 1999 je FBI vodil preiskavo proti domnevnemu mafijcu Nicodemu S. Scarfu iz New Jerseya.
- Agenti FBI so sumili, da ima na računalniku v svojem uradu shranjene podatke o svojih nezakonitih poslih, zato so mu podatke januarja 1999 zasegli, vendar so odkrili, da so datoteke s podatki zašifrirane s programom PGP. Agentje FBI so poiskovali zlomiti kriptogram, vendar neuspešno.
- Zato so 7. maja 1999 agenti FBI zaprosili za sodni nalog za tajni vstop v njegov urad in namestitev posebne programske opreme, s katero bi prestregli Scarfovo geslo.
- Na ta način so prestregli njegovo geslo za PGP. FBI je razvil orodje za prestrezanje gesel *Magic Lantern*, ki deluje kot program za prestrezanje tipkanja.

Zagotavljanje možnosti za nadzor kljub uporabi kriptografije

Primer Scarfo

RDW/1999R00192

ORIGINAL FILED
MAY 8 1999
G. DONALD HARKNE, U. S. MAGISTRATE

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN THE MATTER OF THE APPLICATION :
OF THE UNITED STATES OF AMERICA :
FOR AN ORDER AUTHORIZING THE : *Mag.*
SURREPTITIOUS ENTRY INTO THE : *misc. No. 99-4061-01*
PREMISES OF MERCHANT SERVICES OF :
ESSEX COUNTY, LOCATED AT 149 :
LITTLE STREET, BELLEVILLE, NEW :
JERSEY, FOR THE PURPOSE OF :
CONDUCTING A SEARCH FOR EVIDENCE :
OF VIOLATIONS OF TITLE 18, U.S.C. :
§§ 371, 892-894, 1955 AND 1962 :

APPLICATION

1. Pursuant to Rule 41(b) of the Federal Rules of Criminal Procedure and the All Writs Act, 28 United States Code, Section 1651, the United States of America by and through Faith S. Hochberg, United States Attorney for the District of New Jersey, and Ronald D. Wigler, Assistant United States Attorney for said District, hereby makes application to this court for an order authorizing the surreptitious entry of the premises of Merchant Services of Essex County, 149 Little Street, Belleville, New Jersey, which is more fully described as the rear one-room, lowest-level office of a two-to-three story commercial and residential building on the southeast corner of the intersection of Washington Avenue and Little Street, whose main entrance faces Washington Avenue and whose walls have light-brown siding except for the walls of the rear lowest level, which have a white stucco like material; Merchant Services' office has a silver metal door with darkened glass facing Little Street, a single window on both

Zagotavljanje možnosti za nadzor kljub uporabi kriptografije

Primer Scarfo

- Kmalu po potrditvi obstoja tega orodja, se je razvnela debata o tem, ali naj podjetja, ki prodajajo protivirusno programsko opremo, svoje programe priredijo tako, da protivirusni program uporabnika ne bi obvestil, če bi na njegovem računalniku zaznal *Magic Lantern*.
- Associated Press, je trdil, da FBI sodeluje s protivirusnim podjetjem McAfee, kar pa so pri podjetju zanikali. Novinar AP Ted Bridis je kasneje izjavil, da za svojim člankom kljub temu stoji. Protivirusna podjetja so kasneje javno zatrdila, da z FBI ne bodo sodelovala in da se bodo trudila še naprej odkrivati vse viruse, ne glede na njihov izvor.

Zagotavljanje možnosti za nadzor kljub uporabi kriptografije

Primer Crypto AG

- Leta 1919 je švedski kriptolog Arvid Gerhard Damm zaprosil za patent za mehanični šifrirni stroj. Skupaj s kriptologom Borisom Caesarjem Wilhelmom Hagelinom sta nato razvila v tistem času edino uspešno kriptografsko podjetje. Leta 1952 se je podjetje preselilo v Švico. Podjetje se je imenovalo Crypto AG in je v šestdesetih letih veljalo za največje kriptografsko podjetje na svetu.
- Vendar pa se je okrog podjetja spletlo mnogo govoric, češ, da je v preteklosti sodelovalo z NSA. V prvi izdaji knjige *The Puzzle Palace* leta 1982 je Bamford prvič omenil domnevno povezavo med NSA in Crypto AG.
- Bamford trdi, da se je NSA začela dogovarjati s podjetjem Crypto AG o sodelovanju. Hagelin naj bi NSA posredoval podrobnosti o svojih šifrirnih strojih, kar naj bi NSA omogočilo, da v precej krajšem času razbijejo kriptograme narejene s temi napravami.

Zagotavljanje možnosti za nadzor kljub uporabi kriptografije

Primer Crypto AG

- Bamford navaja dve izjavi neimenovanih uslužbencev GCHQ in NSA, ki sta trdila, da je bila večina kriptogramov držav tretjega sveta enostavno zlomljivih, saj so večinoma uporabljale Hagelinove šifrirne stroje.
- Leta 1992 so v Iranu aretirali uslužbenca Crypto AG, mediji pa so potem špekulirali, da je razlog za aretacijo sodelovanje podjetja s tajnimi službami. Uslužbenec naj bi bil obtožen vohunstva za ZDA in Nemčijo, podjetje Crypto AG pa naj bi devet mesecev po njegovi aretaciji za njegovo izpustitev plačalo 1 milijon mark.
- Crypto AG je proti njemu leta 1995 vložilo tožbo, ker je domnevno nameraval o svoji zgodbi izdati knjigo in ker je govoril z mediji, vendar je v zadnjem hipu prišlo do poravnave, zato javnega sojenja nikoli ni bilo.

Zagotavljanje možnosti za nadzor kljub uporabi kriptografije

Kleptografija

- Na konferenci Crypto leta 1996 in Eurocrypt leta 1997 sta raziskovalca Adam Young in Moti Yung prvič predstavila idejo o *kleptografiji*.
- V članku "*Mitigating Insider Threats to RSA Key Generation*", objavljenem v reviji *Cryptobytes*, je Young opisal metodo SETUP (*secretly embedded trapdoor with universal protection* - tajno vključena stranska vrata z univerzalno zaščito), ki s pomočjo prirejenega algoritma zgenerira tak par šifrirnih ključev (pri asimetrični kriptografiji), da je na videz (matematično) povsem enak kot navaden par ključev, poleg tega pa je tudi enako varen **razen** pred napadalcem, saj tajno vključena stranska vrata predstavljajo napadalčev javni ključ.
- SETUP napad oz. kleptografija napadalcu daje ekskluzivno prednost, saj je zaradi lastnosti prirejenih ključev le-te nemogoče ločiti od neprirejenih – torej je nemogoče ugotoviti, ali je bil SETUP napad izvršen ali ne.
- Young in Yung sta pokazala, da je napad mogoče implementirati v RSA, DSA (*Digital Signature Algorithm*) ter Diffie-Hellmanovo izmenjavo ključev.
- V začetku 1970-tih let je NSA sodelovala pri "razvoju" algoritma DES...

KONEC