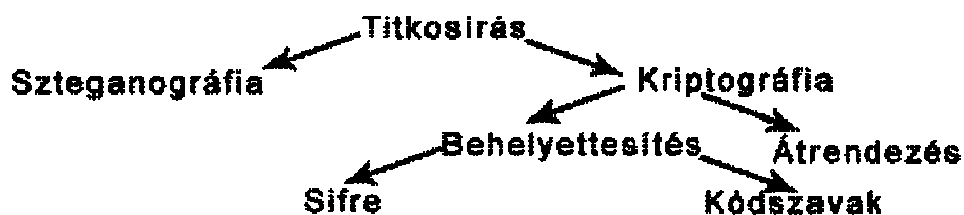


Reflektorfényben a
TITKOSÍRÁS



Modern kriptográfia

A számítógép létrejöttével gyorsabb és hatékonyabb kódolásra képes. Emellett a kódolás alapja bináris, különböző kódokkal, például ASCII-vel készül a kódolás.

DES

Probléma volt viszont az, hogy különböző cégek különböző szabványrendszereket használhattak, ami jelentős mértékben lassította a kódolást és dekódolást. Emiatt az Amerikai Szabványügyi Hivatal 1973-ban pályázatot

írt ki. Az egyik esélyes a Lucifer nevű kód volt. A következőképp történik a kódolás: a szöveget az algoritmus bináris füzéreké alakítja, majd 64 számjegyből álló szakaszokra tördeli. Egy szakaszon a következő műveleteket hajtja végre: két (Bal^0 és $Jobb^0$) szakaszra felezi a szövegrészt, aztán a $Jobb^0$ számjegyeit egy bonyolult módszerrel megcserélik és hozzáadják a Bal^0 -hoz. Ez lesz a $Jobb^1$. A $Jobb^0$ -ból Bal^1 lesz. Ezt tizenhatszor végzik el. A szöveg megkeverése a kulcstól függ. A Luciferből 1976 novemberében Data Encryption Standard (DES) néven szabvány lett.

A kulcsmegosztás problémája



Martin Hellman

A kódoknak, ahogy a DES-nek is egy jelentős problémája volt: a kulcs szétszátása. A kulcs csak személyesen biztonságos, hiszen a telefon lehallgatható. A bankok kellő mennyiségű információval rendelkező, megbízhatónak tartott futárokat küldtek ki, de ez az ügyfelek számának növekedésével működésképtelen.

A probléma egy másik megközelítése, hogy A B-nek küld egy lezárt kazettát, de B azt nem tudja kinyitni és az esetleges lezártan elküldött kulcsokat sem. Ha viszont A elküldi B-nek a lezárt vaskazettát, amire ő rárakja a kulcsot, visszaküldi és A leveszi róla a magáét, akkor a probléma megoldott. Ennek a jelentősége az, hogy bemutatja, hogy létezik kulcsmegosztás. Az alapvető probléma az volt, hogy nem mindegy a kódolás és dekódolás sorrendje.

Az 1960-as években az ARPANet kialakulásakor Whitfield Diffie úgy vélte, hogy mindenkinek joga van szabadon írni, biztonságosan, ezért elkezdett a kulcsmegosztás problémájával foglalkozni. 1974-ben hallott arról, hogy egy Martin Hellman tartott előadást. Diffie rögtön elindult megkeresni őt. A csapathoz Ralph Merkle is csatlakozott. Hónapokig sikertelenül próbálkoztak különféle függvényekkel. A legfontosabbnak az egyirányú függvényeket tartotta Hellman, amik nehezen visszafordíthatók. Ilyenek találhatók például a moduláris aritmetikában. Például a $3^x \pmod{2} = 1$ függvénynek végtelen sok megoldása van.

Hellman egy módszert talált: A és B is választ egy A és egy B számot. Ezután kiszámolják az $x^A \pmod{y}$ és $x^B \pmod{y}$ értéket és ezt elküldik. A végtelen sok megoldási lehetőség miatt a lehallgató személy nem tudja megfejteni sem A-t, sem B-t. A B-től kapott számot A az A-adik hatványra emeli, az A-tól kapottat B a B-edikre és mindkettőn vesznek ennek az y-as maradékát. Ez lesz a kulcs.

Nyilvános kulcs

Amíg Hellmann a saját módszerével foglalkozott, Diffie más irányból közelítette meg

a megoldást. *Aszimmetrikus kulcsot* tartalmazó eljárást talált ki, ami a korábbi szimmetrikus kulcsoktól, ahol az eljárás fordítottja az eredetinek. Bár konkrét példát nem tudott mutatni, ez is előrelépés volt. Megfelelő módszerrel írni lehet egy bárki által elérhető *nyilvános kulccsal*, de megfejteni csak a *privát kulccsal* lehet.

RSA



Adi Shamir

Ron Rivest az újságcikket olvasva Leonard Adleman meggyőzte és elhatározták, hogy megkeresik a szükséges függvényt. Hozzájuk Adi Shamir is csatlakozott. Rivest és Shamir is sorra mondott új ötleteket, de ezekben valaki, többnyire Adleman hibát talált. A megoldást végül Rivest találta meg 1977 áprilisában egy húsvéton. Másnap megmutatta ezt Adlemannek, aki ezúttal nem talált benne hibát. Ez lett az RSA algoritmus. A kódhoz két nagy prímszám szükséges, az üzenet csak azok ismeretében fejthető meg.

A nyilvános kulcs tulajdonsága, hogy prímtényező felbontásokat kell keresni a privát kulcshoz. A jelentős biztonsághoz 10^{308} nagyságrendű prímek kellenek 1977-ben Martin Gardner megjelentetett egy feladatot, hogy a 114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 561 842 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541 prímtényező felbontását keressék meg és ezáltal dekódolnak egy üzenetet. Egy hatszáz önkéntesből álló csoport 1994-ben találta meg a megoldást.

Egy bejelentés szerint a Government Communications Headquartersben korábban megvolt az alapötlet. Egy James Ellis nevű kriptográfus szándékos zajkeltést talált ki. Az elképzelése hasonlított a Diffie-Hellman-Merkle elképzelésre. 1973-ban egy frissen bekerülő kriptográfus, Clifford Cocks Ellis elképzeléseit hallva a saját állítása szerint fél óra alatt megoldotta a problémát. Az egy évvel később csatlakozó Malcolm Williamson a Diffie-Hellman-Merkle féle módszert velük körülbelül

egy időben kidolgozta. Az RSA-n kívül léteznek más nyilvános kulcsú titkosítások is, például a Rabin, az ElGamal, a McEliece módszerek.

Az RSA módszere

A választ két nagy prímszámot, p -t és q -t. Összeszorozza őket és ez lesz N . Ezután egy sem p -vel, sem q -val nem osztható x számot választ. Ezt követően közreadja egy listán x -et és N -t. B az üzenetet például ASCII-kódokkal vagy egyéb módszerrel számmá alakítja. Ez M lesz. A kódszöveg, K a következő lesz: $M^x \pmod{N}$, ezt B elküldi. A a következőképp deszifriroz: a deszifrirozó d kulcsot számolja először ki így: $x \cdot d = 1 \pmod{(p-1)(q-1)}$. A deszifrirozásra a következő módszert alkalmazza: $M = K^d \pmod{N}$.

PGP

A PGP-t Phil Zimmermann találta ki, heves viták voltak körülötte és az FBI is nyomozott. A szoftver célja az RSA felgyorsítása volt. A következőképp készítette ezt el: a DES-hez hasonló IDEA kulccsal kódolta az üzenetet a szoftver, csak az IDEA-kulcs lett RSA-val kódolva. A program emellett megfelelően nagy kulcsokat is tud generálni. Emellett digitális aláírásra is képes. A szoftver emellett automatikusan megkeresi a nyilvános kulcsot.

A programmal két probléma volt: a felhasznált RSA-t szabadalom védi. A másik egy törvény volt, ami az erős titkosítást tiltotta.

Kulcsokat kezelő, hitelesítő megoldások

A kódokat, üzeneteket a veszély miatt több módon is hitelesíteni kell.

Digitális aláírás

A digitális aláírás arra való, hogy a címzett megbizonyosodhasson arról, hogy valóban a látszólagos küldő küldte. Itt a küldő a privát kulcsával titkosítja az üzenetet, amit a nyilvános kulccsal bárki leellenőrizhet, hogy tényleg ő volt-e a küldő.

Hitelesítő szervezetek

A hitelesítő szervezetek (általában) az állam által jóváhagyott, engedélyezett és megbízhatónak ítélt szervezetek, amik a nyilvános kulcs hitelesítésére szakosodtak. Erre azért lehet szükség, mert egy hacker betörve a hálózatra meg tudja hamisítani az elküldött nyilvános kulcsokat. A hatóságok működése során az adott személy nyilvános kulcsát hitelesítik (ellenőrzik valóságát) akár személyes megjelenésre történő kötelezéssel is.

TTP-k

A TTP-k (trusted third party) a kulcsot elvesztő cégek kulcsának "megtalálására" szakosodott. Ezek a privát kulcsot tárolják. A társadalomban kétes a megítélésük, hiszen helyzetükkel visszaélhetnek a nem megfelelően ellenőrzött cégek.

Kvantumkriptográfia

A kvantumkriptográfia alapelve a kvantummechanika, azon belül is a szuperpozícióelmélet és a kétvilág-elmélet. Ez azt állítja, ha egy tárgyat elvesztünk szem elől, több állapotban is lehet. A gyorsulást a még nem létező, ám tervezett kvantumszámítógépekkel akarják megoldani.

Az üzenetek megfejtése

A kvantumkriptográfia használható kriptanalízis felgyorsítására. Ekkor a gépek, mivel az állapot ismeretlen, egyszerre sokkal több állapotot képesek megvizsgálni, így akár az RSA-t is könnyedén fel tudják törni. Ezek alapja a perdület is: egy részecske forgásának iránya alapján kap értéket. A következőképp akarják elérni a szuperpozíciót: a kezdeti forgási irány ismert. Ezután kap egy gyenge impulzust a részecske, ami után vagy másképp forog vagy megtartotta eredeti állapotát. A kvantumszámítógépre programokat is kidolgoztak, ami a DES illetve az RSA feltöréséhez szükséges.

Rejtjelezés

A rejtjelezők is elkezdtek a saját módszereiket kidolgozni. Ennek története a hatvanas évek végén kezdődött. Stephen Wiesner a hamisíthatatlan kvantumpénz fogalmát vetette fel, amin egy polarizációs szűrőn áthaladó fotonok a vibrálás irányától függően maradnak meg vagy nem. A pénzen húsz fonton polarizációs szűrőkön menne át, ezáltal hamisíthatatlan, hiszen rossz szűrő rossz eredményt eredményez, amivel nem lehet újra próbálkozni. Az ötlet kivitelezhetetlen és drága volta miatt csak egy Charles Bennett nevű ismerőse figyelt fel rá. Ő Giles Brassardnak, a Montreali Egyetem számítógéptudósának mutatta meg. Elkezdtek kidolgozni egy módszert. Kétféle továbbítás van: a *rektilineáris* (vízszintes és függőleges, a függőleges értéke 1) és *diagonális* (átlós, a jobb felső sarok és bal felső sarok közötti értéke 1). A lehallgató személy nem tudja megállapítani a polarizációs sémát, de a címzett sem. Ezért kulcsot kell cserélniük. Ekkor a küldő A elküld B -nek egy véletlenszerű bitsort a séma váltogatásával. B a saját szűrőjével véletlenszerűen megvizsgálja a polarizációt. Ezután A elmondja B -nek a polarizációs sémákat (csak azt). A

helyesen megvizsgált fotonok füzére lesz a kulcs. Ha lehallgatták az üzenetet, akkor néhány találmányra kiválasztott szám ellenőrzése elég. Ezeket később nem veszik figyelembe. Ezt a lapok leadták, de még be kellett bizonyítani a módszer működőképességét. Az 1988-ban kezdődő egyévnyi munka után (melybe bevontak egy John Smolin nevű kutatót), az első próbaüzenettel próbálkoztak. A küldést egy Alice, a fogadást egy Bob nevű számítógép irányította. Ha csak harminc centiméterre is volt a két számítógép egymástól, de a módszer működött. A hosszú távú küldés is elérhetőnek látszik, 1995-ben Genf és Nyon között huszonhárom kilométeren keresztül sikerült így továbbítani üzeneteket. A kvantumelmélet lehetetlenné teszi az így kódolt üzenetek megfejtését. Ha mégis így lenne, az univerzum elemi szintű működését kéne újragondolni.

Az RSA értékelése

Keveset tudunk a hivatásos rejtjelfejtők (pl. NSA) álláspontról. Az a kevés információ, amely nyilvánosságra került publikációkból nyerve arra mutat, hogy az NSA a DES-t részesíti előnybe a PKS-sel szemben. Ugyanakkor komoly erőfeszítéseket tesz, hogy a rejtjelzési kutatásokat ellenőrizni tudja. Már a hagyományos távközlő csatornán keresztüli rejtjelzésre is komoly nyomás nehezedik azért, hogy az úrtávközlés elterjedésével, üzleti okokból, a rejtjelzésre kerülő üzenetek mennyisége ugrásszerűen megnövekedjen.

Az úrtávközlés nem csak a klasszikus értelemben vett rejtjelzési problémákat veti fel, hanem az úgynevezett „titok megosztást” is.

A rejtjelzés ugrásszerű elterjedéséből és újszerűségéből adódó megnövekvő hatósági feladatok indították az USA kormányát új irányelvek kiadására. További nehézséget jelent, hogy a rejtjelzés híradástechnikai csatornán keresztüli módján kívül megjelentek a számítógépes háttértárakban (pl. mágneslemezen) levő adatok rejtjelzése, valamint a „smart card”-ok is ebbe a kategóriába tartoznak.

Prímszám tesztelő algoritmusok

Számos olyan kriptográfiai algoritmus létezik, amely működéséhez szükség van hosszú – akár több száz jegyű – prímszámra. A prímszámok előállítására azonban nem egyszerű feladat, nincsen például egyszerű, prímekeket generáló képlet. A gyakorlatban alkalmazott módszer az, hogy választunk egy véletlen számot, majd teszteljük, hogy príme-e.

A számok prímségének tesztelésére valószínűségi és determinisztikus tesz-

tek állnak a rendelkezésünkre.

A valószínűségi tesztek (pl. Miller-Rabin teszt, Lucas prímteszt, Solovay-Strassen prímteszt) gyorsak, de nem döntenek el teljes biztonsággal, hogy az input príme-e. Azonban a tévedés valószínűsége a teszt többszöri végrehajtásával – ha mindig pozitív a válasz – tetszőleges küszöbérték alá csökkenthető. Így ezek a módszerek kriptográfiai célokra – például RSA kulcsgenerálásra – megfelelőek.

A determinisztikus módszerek közül a legegyszerűbb eljárás, ha a számot sorban elosztjuk a gyökénél nem nagyobb természetes számokkal. Így biztos választ kapunk a szám prímségére vonatkozóan, azonban ez a módszer nagy számok esetében nagyon lassú (a szükséges lépésszám a szám hosszának exponenciális függvénye), ezért a gyakorlatban nem is alkalmazzák. Léteznek ennél jobb algoritmusok is erre a célra, a jelenleg (2003) ismert legjobb determinisztikus módszer az Atkin-Morain teszt.

Az RSA gyakorlati működése

A titkos kulcsot optimális esetben csak tulajdonosa ismerheti, viszont publikus kulcsát minél szélesebb körben ismertté kell tennie, hiszen így tudnak neki címzettnek titkosított üzenetet küldeni. A két kulcs egymást kiegészítve működik; a címzett nyilvános kulcsával titkosítjuk az üzenetet, amit rajta kívül más nem tud elolvasni, hiszen csak ő rendelkezik a dekódolást elvégző titkos kulccsal. A módszer erősségét, a szimmetrikus kulcsos titkosítás hátrányának megoldása szolgáltatja: azok is tudnak titkosított üzeneteket váltani, akik nem ismerik egymást (elég, ha előzőleg kicserélték nyilvános kulcsaikat). Ez a cseré történhet Interneten keresztül is, hiszen attól, hogy valaki megszerzi a nyilvános kulcsunkat még nem fér hozzá bizalmas információkhoz. További előnyös tulajdonsága, a digitális aláírás készítésének lehetősége, mely opciót a hitelességvizsgálat céljából érdemes kihasználni.

Megfejtése

A 40 bit hosszú kulcsok nem érnek semmit, simán feltörhetők, a 1024 bitnél rövidebb kulcs ma nem nevezhető biztonságosnak. A 40, 48, 56, 64 már fel van törve. (A 40-es RC5-öt 3 óra alatt törték fel.)

Ha lesz gyors módszer prímekeket számolni, akkor nagy gond lesz a jelenlegi kommunikációban. Ma azonban ilyen módszer még nem ismert.