A Caesar-kódtól az SSH-ig – a rejtjelezés rövid története

Bodnár Csaba, bocs@missioncriticallinux.hu

2002.10.01.

Kivonat

A történelem során mindig voltak olyan társadalmi csoportok, akik szerették volna üzeneteik ill. jegyzeteik tartalmát titokban tartani: az uralkodók, politikusok és a katonai vezetők részéről már az ókorban jelentkezett ennek igénye.
Adataink biztonsága mára meghatározó jelentőségűvé vált – különösen, ha napi rendszerességgel az interneten dolgozunk: távoli kiszolgálóra ssh-val lépünk be, fontosabb adatainkat scp-vel másoljuk, cégünk telephelyei között titkosított VPN-csatornákat építünk ki és félve adjuk meg bankkártyánk adatait akkor is, ha tudjuk, hogy https protokollal kommunikál böngészőnk a kiszolgálóval.
Korunkat az információ korának nevezik, de nevezhetnénk ugyanígy az információbiztonság korának is, hiszen ha az információ a legfőbb érték, akkor annak védelme elsődleges fontosságú. Úgy gondolom, érdemes áttekinteni, hogyan jutottunk el eddig, hogyan fejlődött a titkosítás – amit főleg katonai körökben rejtjelezésnek is neveznek – az elmúlt évezredek során, illetve mi várható a jövőben.

Tartalomjegyzék

1. Szteganográfia – az üzenet elrejtése

Már az ókorban is tudták, hogy annak legegyszerűbb módja, hogy az ellenség ne tudja meg az üzenetet, az üzenet elrejtése. Míg a szteganográfia az üzenet létezését palástolja, addig a kriptográfia az üzenet tartalmát. Gyakran a kettő kombinációját használták: ha a futárnál meg is találták az elrejtett üzenetet, a tartalmát akkor sem tudták meg. Példák szteganográfiára:

- Hérodotosz: Demaratosz üres viasz írótábla deszkájára írja, majd viasszal fedi el üzenetét.
- Hisztaiaszeusz a küldönce fejét leborotváltatta, ráírta az üzenetet, majd megvárta, míg a haja kinő. Akkoriban még erre is volt idő...
- Kínaiak: selyemre, azt labdaccsá gyúrták, viasszal borították, majd lenyelte az üzenetvivő.
- kemény tojásban üzenet: timsó és ecet elegyével írtak rá, a fehérjén kirajzolódik az írás.
- láthatatlan tinta: növény (pl. pitypang) nedvével.
- Második világháború, Dél-Amerika: német ügynökök, mikropont módszer: fényképészeti eljárással egy oldalnyi szöveget pöttyé zsugorítottak.

2. Kriptográfia – az üzenet titkosítása

A kriptográfia két ága az átrendezés és a behelyettesítés.

2.1. Átrendezés

Gyakorlatilag anagrammát készítünk a szövegből. A kódoláshoz/dekódoláshoz egyértelmű módszerre van szükség. Rövid szöveg esetén könnyen megfejthető, hosszú esetén nehéz megfelelő könnyen használható módszert találni. Példák átrendezésre:

- az iskolások fésűs módszere, rácsos módszere.
- a világ első katonai rejtjelező eszköze a spártai szkütalé: a szkütalé egy sokszögletű bot, amelyre szíjat tekertek és úgy írták rá a szöveget. i.e. 404-ben Lüszandrosz szkütalé segítségével kapott hírt, hogy a perzsák támadást akarnak indítani ellene.
- A II. világháború alatt a németek által használt Enigma rejtjelezőgép az átrendezést és a behelyettesítést egyaránt alkalmazta.

2.2. Behelyettesítés

2.3. Monoalfabetikus behelyettesítés

A monoalfabetikus legrégebbi legrégibb leírása a Káma-Szútrában (!) található, ahol 64 művészet tanulmányozását írja elő a nők számára, ezek egyike a titkosírás művészete. Itt az egyik ajánlott módszer az ábécé betűinek találomra történő párosítása.

Julius Caesar gyakran használt behelyettesítéses kódot: minden betű helyett az ábécében utána következő harmadikat írta le. Ezt Caesar eltolásos ábécéjének vagy egyszerűen Caesar-kódnak nevezzük. A monoalfabetikus behelyettesítéses kódábécé egyszerűséget és megbízhatóságot jelentett évszázadokon keresztül.

2.4. A monoalfabetikus kód megfejtése: Gyakoriságelemzés

Időszámításunk szerint 750-től az iszlám kultúra aranykorát éli, felvirágzott a tudomány és a művészet, a titkosírásokat napi rendszerességgel használták a közhivatalokban. Így nem csoda, hogy elsőként az arabok ismerték fel a monoalfabetikus behelyettesítéses kód megfejthetőségét gyakoriságelemzéssel.
Minden nyelvre jellemző, hogy az adott nyelven leírt szövegben a betűk milyen gyakorisággal fordulnak elő. Így kellően nagy mennyiségű szöveget gyakoriság szempontjából elemezve ki tudjuk következtetni, hogy a kódszöveg valamely jele az ábécé mely betűjének felel meg. Ezt a reneszánsz-kori Európában is ismerték, az olasz városállamok, a Vatikán, és az egyes uralkodók diplomáciai levelezésében (És azok megfejtésére is). Mária skót királynő titkos levelezését is ezzel a módszerrel fejtették meg, így fény derült Erzsébet királynő ellen szőtt összeesküvésükre, Máriát pedig kivégezték.

Összegzésül elmondhatjuk, hogy a gyakoriságelemzés meggyengítette a monoalfabetikus kódolás nyújtotta biztonságot.

2.5. Homofonikus behelyettesítéses kód

A homofonikus kód olyan monoalfabetikus kód, melyben az egyes betűknek (általában a gyakran használtaknak) több sifréje (helyettesítése, kódja) is lehet, amelyek száma az adott betű gyakoriságához igazodik. Ha az a gyakorisága 8%, akkor akár 8 jelet is rendelhetünk hozzá.

Sokáig megfejthetetlennek tűnt XIV. Lajos, a Napkirály grand chiffre-je, „nagy kódja”. Ezzel titkosították legfontosabb üzeneteit, haditerveit, politikai „húzásait”. Csak évszázadokkal később, 1890-ben fejtette meg Étien Bazeries őrnagy három év alatt. Itt is homofonikus kódról volt szó, de nem a betűk, hanem a szótagok voltak kódolva.

2.6. Polialfabetikus behelyettesítés (Vigenére-sifre)

Az ötlet: ne egy, hanem több kódábécét használjunk. Alberti, Trithemius és Porta munkáit Blaise de Vigenere kovácsolta új, egységes és erős kódrendszerré az 1560-as években. Nem 1, hanem 26-féle kódábécé, amelyek mindegyikét egy hellyel eltolják az előzőhöz képest. A titkosítás módja:

- Vigenére-tábla elkészítése,
- Nyílt szöveg minden betűjét társítjuk a kulcsszó megfelelő betűjéhez (pl. fölé írjuk),
- Táblából kikeressük a megfelelő kódot.

Előnye, hogy gyakoriságelemzéssel megfejthetetlen. Rengeteg kulccsal alkalmazható. Hátránya, hogy sokkal bonyolultabb használni, ezért kétszáz évre feledésbe merült, helyette inkább homofonikus kódolást használtak.

2.7. A polialfabetikus kód megfejtése: Babbage

Charles Babbage angol matematikus sokféle dologgal foglalkozott, sebességmérő, „bölényhárító”, statisztika, mortalitási táblázatok, stb. a számológépével a mai számítógépek alapjait rakta le. Babbage egy bristoli fogorvos hatására kezdett el foglalkozni a Vigenére-sifre megfejtésével: Rájött, hogy a kódolt szövegben ismétlődések vannak, ezek segítségével – megfelelően hosszú szöveg esetén – meg tudta állapítani a kulcs hosszát. Ha a kulcs pl. 5 betűből áll, akkor a feladat visszavezethető 5 monoalfabetikus szöveg elemzésére, ami gyakoriságelemzéssel megoldható.

3. Az I. és a II. világháború kriptográfiája

3.1. A rádió megjelenése

A rádió előnye a kommunikáció felgyorsítása, hátránya a lehallgathatóság. Megjelenésével megnőtt a titkosításra való igény. A rejtjelfejtők legnagyobb problémájává a kódszövegek hatalmas mennyisége vált. Korábban az elfogott üzenet ritka volt, a rádió megjelenésével a rejtjelfejtőkre a kódszövegek valóságos áradata zúdult.

3.2. Az ADFGVX

Az első világháborús német ADFGVX-kód egy monoalfabetikus behelyettesítéses és egy átrendezéses módszer együttes alkalmazását jelentette. A francia Georges Painvinnek sikerült feltörnie.

A világháború idején Zimmermann német külügyminiszter a mexikói elnöknek küldött rejtjelezett táviratot, melyben arra próbálja rávenni, hogy támadja meg az Egyesült Államokat és erre beszélje rá Japánt is. Az angolok a táviratot elfogták és megfejtették, majd publikálták. Ennek hatására lépett be az Egyesült Államok a háborúba.

3.3. Egyszeri kulcsos módszer

A Vigenére-sifre alapvető gyöngesége az, hogy ciklikus jellegű, segítségével azonban egy sokkalta erősebb módszer készíthető:

- Legyen a kulcs egyenlő hosszú a kódolandó szöveggel. Ez kivédi a ciklikusságból adódó gyengeséget. A rejtjelfejtő továbbra is megpróbálhat gyakran használt szavakat a nyílt szövegbe beilleszteni és így értelmes részeket találni a kulcsban (vagy fordítva), ami akár a teljes szöveg megfejtéséhez is vezethet!
- Ennek megoldására legyen a kulcs teljesen véletlenszerű (random).

Matematikailag igazolható, hogy az egyszeri kulcsos módszer valóban abszolút megbízható. A gyakorlati alkalmazásával azonban vannak problémák, ugyanis rengeteg kulcsra van szükség (nem „reciklálható”): Nehézkes volt a random kulcsok előállítása, a kulcsok szétosztása (kódkönyvek) pedig sokszor áthidalhatatlan nehézséget okozott. Emiatt alig-alig használták az egyszeri kulcsos módszert.

3.4. A titkosítás gépesítése

Kódtárcsa: Leon Alberti találta fel a XV. században. Két korong, egyik valamivel nagyobb, mint a másik. A kisebbet a nagyobbra helyezzük, közös tengellyel összefogjuk

és ráírjuk mindkettőre szélére körben az ábécét. Segítségével egyszerű Caesar-kódú üzeneteket sifírozhatunk. Ha mindegyik betű kódolása után elfordítjuk a tárcsát egy megfelelő kulcs szerint, akkor polialfabetikus kódot is generálhatunk. A kódtárcsa megkönnyítette a kódolást.

3.5. Az Enigma

A II. világháború alatt mind a központi hatalmak (a német Enigma ill. Lorenz SZ40 vagy a japán Purple), mind a szövetségesek (a brit Typex ill. az amerikai SIGABA) használtak retjelezőgépeket. A németek által a második világháború előtt és alatt használt Enigma-rejtjelezőgép (Arthur Scherbius találmánya) a fenti kódtárcsa elektromos változatán alapul:

- Az eredeti modellbe három, fix huzalozású tárcsát építettek be, a tárcsák kivehetők és egymással is felcserélhetők voltak (polialfabetikus kód).
- Kapcsolótábla, mellyel betűket lehet felcserélni (hat betűpárt) (átrendezéses módszer).
- Gyűrű, amely szintén befolyásolja a sifírozást.

A kulcs a tárcsák „alapbeállítása” és a kapcsolótábla beállítása volt, ezeket kódkönyvekben négy hetente kapták meg és naponta változtatták.

3.6. Az Enigma-kód feltörése

Lengyelország már a harmincas években tartott egy esetleges német lerohanástól, így megalakították a Biuro Szyfrów-t, a kódirodát. Ciezki százados vezetésével sikerült feltörniük az Enigma kódját: rendelkezésükre állt egy kereskedelmi verziójú Enigma (a katonaitól különböző huzalozással) és megszereztek olyan dokumentumokat, amelyből előállíthatták a katonai verziót. A németek a kódkönyv kódjait „fő kódkulcsként” használták, amellyel az egyes üzenetek egyedi kulcsait kódolták. Az egyedi kulcsokat kétszer egymás után írták be – elkerülendő a tévedéseket és a rádióinterferencia okozta hibákat és ez vált a rendszer gyenge pontjává. Az egyik kódfejtő, Marian Rejewski, ebből olyan összefüggéseket állapított meg, amelyből kiindulva egy évnyi munka eredményeképpen meg tudták fejteni a kódot és évekig dekódolni tudták az üzeneteket. Kódfejtő-gépet is konstruáltak hozzá (Rejewski-bomba). A németek egy idő után változtattak az Enigmán, ezt még tudták követni a lengyelek, de amikor elkezdtek három helyett öt tárcsát használni, majd a kapcsolótáblákon hat betűpár helyett tízzel kellett számolni, akkor feladták a dolgot. Néhány héttel Lengyelország lerohanása előtt átadták a megszerzett információkat, tervrajzokat és egy Enigma-másolatot a franciáknak és az angoloknak.

Az angolok a Bletchley Parkban a lengyel módszerekkel és jóval több pénzzel, így technikával meg tudták fejteni a nehezebb német kódot is, így rendszeresen értékes hadi értesülésekhez jutottak. A csoport tagja, Alan Turing matematikus (ld. Turing-gép) közben olyan összefüggéseket tárt fel a kódszövegben, amelynek segítségével – ha van az embernek némi támpontja – több Enigmát hurokba kötve záros határidőn belül megfejthető volt a keverőtárcsák aktuális beállítása, vagyis maga a kulcs. Ezen az elven alapuló komplett dekódoló gépeket (Turing-bombákat) építettek, így amikor a németek újra „csavartak egyet” az Enigma kezelésén (nem duplikálták többé a kulcsokat), követni tudták a változást. Sokak szerint a Bletchley Park tevékenysége nagyban

hozzásegítette a szövetségeseket a háború megnyeréséhez, de legalábbis lerövidítéséhez.

3.7. A navaho-titkosítás

A II. világháború legtrükkösebb kódolási módszerét az amerikaiak találták ki és használták a csendes-óceáni térségben: navaho indiánokat alkalmaztak rádiósként, akik anyanyelvükön tartották a kapcsolatot egymással. A navaho nyelv egyetlen ismert nyelvcsaládba sem tartozik bele, korábban nagyon kevesen tanulmányozták, így ideálisnak tűnt a feladatra. A „navaho-titkosítást” a japánok soha nem tudták megfejteni.

4. Számítógépes kriptográfia

4.1. Az első szabvány (DES)

Horst Feistelt – amerikai német emigráns lévén – a háború alatt, majd később sem hagyta az NSA érvényesülni, pedig ő mindig is kriptográfiai kutatásokkal akart foglalkozni. Végül a hetvenes évek elején megalkothatta az IBM-nél a Lucifer rendszert. A titkosítás egy igen képletes leírás szerint a következőképpen néz ki:

„A sifrírozási eljárás kicsit a dagasztáshoz hasonlít. Képzeljünk el egy hosszúra nyújtott tésztamasszát, amelyre valamilyen üzenetet írtak. A tésztát először 64 centiméteres darabokra vágják, ezt fölszabdalják, összegyúrják, hozzácsapják a következő darabhoz, és megint összegyúrják. Ezt a műveletet ismétlik újra meg újra, míg az üzenet teljesen össze nem gabajodik. 16 dagasztás után elküldik a kódszöveget, a címzett pedig a művelet fordított irányú végrehajtásával kibogarássza a tartalmát.”

A titkosításhoz tartozik egy kulcs is, az üzenet a választott kulcstól függően milliárdnyi módon sifrírozható. 1976-ban a Lucifer vált a DES-szabvánnyá.

4.2. Az aszimmetrikus kulcs

Továbbra is komoly probléma volt azonban a titkos kulcsok eljuttatása a túloldalra. A rendszeresen titkosított adatokkal dolgozó szervezetek költségvetésében komoly pénzügyi tételekként jelentek meg az ezzel kapcsolatos kiadások. A hetvenes években Diffie, Hellman és Merkle a Stanfordon talált egy módszert arra, hogyan lehet nyilvánosan kulcsot cserélni. Nem sokkal később Diffie kitalálta az ún. aszimmetrikus kulcsot. Itt tulajdonképpen két kulcsról van szó: az egyikkel sifrírozni lehet, a másikkal desifrírozni. A desifrírozó kulcsot hívjuk ma privát kulcsnak, a sifrírozó pedig a nyilvános kulcs. A nyilvános kulccsal kódolva bárkinek küldhetünk titkos üzenetet, azt csak ő maga, a privát kulcsával tudja majd elolvasni.

4.3. RSA

Diffie csak magát az elvet találta ki, a gyakorlati megoldásra az RSA-hármas (Rivest, Shamir, Adleman) jött rá 1977-ben. Módszerük szerint a nyilvános kulcs két elég nagy prímszám szorzata, a privát kulcs pedig maga a két prímszám. Mivel a prímtényezős felbontás – kellően nagy számok esetén – hosszadalmas, időigényes feladat, ez garanciát jelent az adatok biztonságára nézve.

Nemrég kiderült, hogy ugyanezt a dolgot a brit biztonsági szolgálatnál már néhány évvel korábban kitalálták: az elvet James Ellis, a gyakorlati megvalósítást pedig Clifford Cocks és Malcolm Williamson dolgozta ki.

4.4. PGP és GPG

A nyolcvanas években Phil Zimmermann – aki azon a véleményen volt, hogy mindenkinek joga van a saját személyes adatai védelmére – kifejlesztett egy könnyen kezelhető, gyors titkosító szoftvercsomagot, melyet PGP-nek (Pretty Good Privacy) nevezett el. A PGP az RSA-t és egy IDEA nevű szimmetrikus kódolást egyaránt tartalmazott: a sebesség érdekében az RSA-t csak az IDEA kulcsának kódolására használta. A szoftver emellett digitális aláírás készítésére is használható volt.

A programot freeware-ként felrakta egy publikus helyre, ahonnan rengetegen letöltötték és kezdték el használni. Emiatt először a szabadalom jogtalan felhasználásával, majd illegális fegyverexporttal vádolták. Végül nem ítélték el és – miután az RSA Security-val megállapodott – a PGP azóta is terjed, nem kereskedelmi célokra szabadon letölthető. Maga az alapkérdés azonban még mindig nyitott, mi a fontosabb, a kriptográfia szabadság és az egyéni jogok védelme, vagy a bűnüldöző szervek lehetősége a betekintésre. A döntő tényező valószínűleg mindig az lesz, mitől fél jobban a közvélemény: a bűnözéstől vagy az államtól.

Bár a PGP magán használatra ingyenes, üzleti célúra azonban nem. Ezt az „apró problémát” küszöböli ki a GPG vagy GnuPG (Gnu Privacy Guard), ami az OpenPGP szabvány (RFC 2440) nyílt forráskódú megvalósítása. Mivel az eredeti PGP-ben lévő IDEA algoritmus licensszel védett, helyette válogathatunk az ingyenes algoritmusok bő választékából (ElGamal, DSA, AES, 3DES, Blowfish, Twofish, CASTS, MD5, SHA-1, RIPE-MD-160 és TIGER).

4.5. TripleDES

A kilencvenes évek elejére az 56-bites DES algoritmus már nem volt elég biztonságos. Számítani lehetett arra, hogy egyszerre akár több ezer számítógépből álló cluster próbálja feltörni titkos kódunkat. Ekkor jött a TripleDES, amely 3 egymástól független kulcsot használ, így megháromszorozza a lehetséges kulcsok számát $(5.2 \cdot 10^{33})$, így a feltöréshez szükséges erőfeszítéseket is. Az évtized közepére ez sem volt elég jó, bár a biztonsága megfelelő volt, más problémák voltak vele: túl lassú volt, a sávszélességek megnövekedtek, így egyszerre a korábbinál jóval nagyobb mennyiségű adatot kellett megfelelő sebességgel titkosítani. Az NSA/NIST így pályázatot írt ki az új szabvány (Advanced Encryption Standard, AES) megtervezésére.

4.6. Az új titkosítási szabvány (EAS)

A pályázat első körébe 15 fejlesztői csapat jutott be, köztük egészen nagy (RSA Labs) és egészen kis (a puerto ricoi illetőségű Georgoudis FROG nevű algoritmusával, mely első ilyen jellegű próbálkozása volt) nevekkel. A második körbe öten jutottak be, közülük az ismertebbek:

- Az RSA Laboratories egy mindössze néhány soros, nagyon erőteljes algoritmussal, amely azonban túlságosan processzorigényes volt.
- TwoFish algoritmus az ismert BlowFish algoritmus fejlesztőitől.

A győztes a Rijndael algoritmus lett, két flamand kriptográfus, Daeman és Rijman tervezésében. Hogy lehet, hogy egy belga algoritmus lett az új amerikai titkosítási szabvány? Előnyös tulajdonságai miatt, úgymint: könnyű szoftveres implementálhatóság, a komponensek általános áttekintehetősége, alacsony erőforrásigényű hardverimplementációs tapasztalatok.

5. Alkalmazások

Az internet használatával megnőtt az igény a biztonságos kommunikációt lehetővé tevő programokra. Most ejtünk néhány szót a legelterjedtebb alkalmazási módokról. A PGP-ről korábban – Phil Zimmermann tevékenysége kapcsán – volt már szó.

5.1. SSH és OpenSSH

Tatu Ylönen finn diák 1995-ben kifejlesztette az SSH első verzióját, megnyugtató biztonságú alternatívaként az addig előszeretettel használt telnet helyett, a telnet protokoll ugyanis nemhogy a kommunikációs csatornát, hanem magát a felhasználói nevet és jelszót sem titkosította. Mindenki SSH-t kezdett használni, mindaddig mígnem Tatu megalapította az ssh.com nevű biztonságtechnikai céget, az ssh forrásának licenszelését pedig úgy módosította, hogy azt már nem igazán lehetett „nyílt forrásúnak” nevezni. Mint sok más fejlesztőt, az OpenBSD fejlesztői csapatot is nagyon zavarta ez a dolog, hiszen az OpenBSD-ben szerverként és kliensként egyaránt használták már az ssh-t. Fogták hát a legutolsó szabad forrású verziót és azt fejlesztették tovább OpenSSH néven. 2000 májusára az OpenSSH már az új, SSH2 szabványt is támogatta. Csak „licenszmentes” titkosítási algoritmust használ, úgymint 3DES, Blowfish, CAST128, Arcfour and AES. A kezdeti kulcscsere RSA-val vagy DSA-val történhet.

5.2. SSL

Az SSL (Secure Sockets Layer) a web-alapú kommunikáció titkosítására szolgáló szabványos módszer, melyet a Netscape fejlesztett ki. Az SSL a következő szolgáltatásokat nyújtja egy TCP/IP kapcsolat esetén: adattitkosítás, szerver authentikáció, üzenet integritásellenőrzés, opcionális kliens authentikáció. Az SSL-t az összes ismert web kiszolgáló és böngésző szoftver ismeri és támogatja, de SSL-be mi magunk is becsomagolhatunk bármit, pl. IMAP-et vagy POP3-at. Az SSL a következő algoritmusokat támogatja: DES, DSA, KEA, MD5, RC2, RC4, RSA, SHA-1, SKIPJACK, Triple-DES.

Érdemes külön szót ejteni a szerver authentikációról. Ennek segítségével a böngészőnk megbizonyosodhat arról, hogy az elérni kívánt szerver valóban az-e, akinek mondja magát, egy erre feljogosított független állami vagy magán hatóság (certification authority, CA) szerverének segítségével. Ugyanez lehetséges a másik irányba is, vagyis hogy a kliens igazolja magát (opcionális kliens authentikáció), de ezt ritkán használják.

5.3. IPSEC

Míg az SSL az átviteli szinten (transport layer), addig az IPSEC a hálózati szinten (network layer) dolgozik. Az SSL két alkalmazás, az IPSEC pedig két számítógéphálózat között biztosít biztonságos kommunikációs csatornát. Az IPSEC-et protokollt az IETF (Internet Engineering Task Force) fejlesztette ki, része lesz az a TCP/IP következő generációjának, az IPV6-nak, de a jelenlegi IPV4 alatt is széles körben használják. Az IPSEC-re alapozva virtuális magánhálózatok építhetők ki az interneten keresztül pl. cégünk telephelyei között. Egyik legelterjedtebb nyílt forráskódú implementációja a freeswan.

6. A jövő a kvantumkriptográfia?

Az RSA nagyon erős kód, nagyméretű kulcsok esetén feltörésére csak a prím-faktorizáció valamilyen új matematikai módszerrel történő felgyorsításával lenne lehetséges, erre azonban nincs sok esély. A kódtörők újabban a kvantumfizikában reménykednek, jóllehet, a kvantumszámítógép elve „dacol a józan ésszel”. Ennek elméletét David Deutsch brit fizikus dolgozta ki. A kvantumszámítógép egyszerre hihetetlen mennyiségű számítás elvégzésére lesz képes, megépítéséig azonban még jónéhány elméleti és gyakorlati akadályt le kell győzni. A kutatók között sincs egyetértés abban, megépíthető-e belátható időn belül vagy sem. Peter Shor és Lov Grover a Bell Laboratóriumban már programot is írtak – kvantumkomputeren történő futtatásra. Ha a kvantumszámítógép egyszer elkészül, újra a kódfeltörők lesznek előnyben, hiszen azzal az RSA pillanatok alatt feltörhető lesz.

Ők azonban már dolgoznak a kvantumelméleten alapuló titkosítási módszeren: Stephen Wiesner ötlete alapján Charles Bennett és Gilles Brassard a fény polarizációján alapuló módszert dolgozott ki és túl van több sikeres teszten, vagyis fénykábelen ill. a levegőben sikerül átjuttatni polarizált fénnyel kódolt adatokat biztonságosan.

7. Hivatkozások

Simon Singh: Kódkönyv, A rejtjelezés és a rejtjelfejtés története
Bruce Scneier: Applied Cryptography
David Kahn: The codebreakers
Daniel J. Barrett, Ph. D. and Richard E. Silverman: SSH: The Secure Shell
www.rsa.com
www.pgp.com
www.gnupg.org
www.openssh.org
www.ssh.com
www.freeswan.org
csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
www.nist.gov/aes