KERESKEDELEM A SZÁMÍTÓGÉPES HÁLÓZATOKON

Sasvári Péter
Számítástechnikai munkatárs
Miskolci Egyetem, Vállalatgazdaságtani Tanszék

BEVEZETÉS

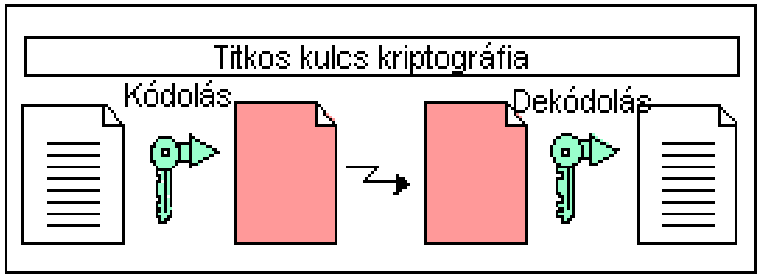
A banki szolgáltatások köre az egész világon gyors ütemben bővül és fejlődik. Mára létrejött az első olyan bank, amely mögött nincs háttérintézmény, nincs anyavállalat; a bank működéséhez csupán néhány számítógépre van szükség.
Ez a bank az Internet világhálózatának segítségével működik, ezáltal a szolgáltatás a világ bármely pontján, sőt a fejlett országokban az otthonokban is elérhetővé vált. Az Eurocard és a Visa már kidolgozta azt a közösen használható szabványt, amelylyel az Internet-átutalásokat, adatokat titkosítani tervezik, a szabványukhoz való csatlakozást viszont még nem tették publikussá.

AZ ELEKTRONIKUS KERESKEDELEM KEZDETE

Az Internet felhasználói korábban igen aktívan használták a hálózatot. Kiválasztották a árut, kitöltöttek egy adatlapot, aztán - bankkártyájuk és azonosítóik számait begépelve- várták, mikor érkezik a megrendelt pizza, vagy könyv. Ezt az idilli folyamatot törte ketté az a pillanat, amelyben - egy ilyen átutalás alkalmával- valakik először szippantottak le minden pénzt a számláról, elcsípve a hálózaton kódorgó adatokat, és maguk számára is kihasználva más kártyájának hitelképességét. A szoftvercégek ekkor különböző bonyolultságú titkosító kódok beépítéséhez fogtak, amely rendszereket átlagosan egy hét alatt törték fel a szoftvertesztelők. Így aztán az Interneten keresztül -Visa-Mastercard szabvány elterjedéséig- csak saját felelősségre adhatja meg a kuncsaft bankkártyája adatait.
Napjainkban az Interneten több szempontból is kulcskérdéssé vált a megfelelő szintű titkosítás, amelyik ma még beláthatatlan távlatokat nyithat az elektronikus kereskedelemben, de sértheti is a világhatalmak nemzetbiztonsági érdekeit.
A kriptográfia ősidők óta állami monopólium, módszerei a digitális médium megjelenése előtt ritkán kerültek ki a civil szférába. Az Egyesült Államok exporttörvényei a kriptográfiai technológiát nemzetbiztonsági fontosságúnak minősítik, és a kriptográfiai rendszerek fejlesztőit arra kötelezik, hogy termékeiket a szövetségi hatóságoknál regisztráltassák. A privát, vagy kódolt telefonvonalakat kínáló telefontársaságok kötelesek olyan kiskaput beépíteni a rendszerbe, amelyikkel a hatóságok le tudják hallgatni a kódolt vonalakat is. A nemzet biztonsága fölött őrködő szervezetek, pl. az NSA, az FBI és a CIA ennek az elvnek a kiterjesztését szorgalmazza a számítógépes világhálózatra. Az Interneten számos lehetőség van az információ kódolt továbbítására, és több módszer olyan szintű titkosítást biztosít, amelyik a most legkorszerűbb számítógépekkel sem törhető fel.

A KRIPTOGRÁFIA

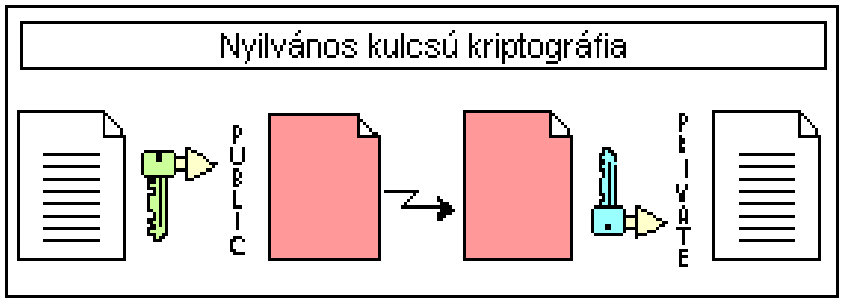
A kriptográfia legkorszerűbbnek számító válfaja a nyilvános kulcsú kriptográfia, amelyik kiküszöböli az összes eddigi titkosítási rendszer klasszikus gyengeségét, az üzenetek megfejtéséhez szükséges kulcs eljuttatását a másik félhez. A prímszámokon alapuló public key, vagyis nyilvános kulcsú szisztémák lényege, hogy mindenkinek két azonosító van a birtokában: a nyilvános kulcs kódolt üzenetek küldését, a titkos kulcs pedig a kapott üzenetek dekódolását teszi lehetővé.



1. ábra
Hagyományos titkosítás

Tekintsük a titkosító módszert széfeknek. Hagyományos algoritmusok (a fenti ábra alapján) esetében van egy kulcs, amelyiknek birtokában ki tudjuk nyitni a széfet. A kulcs másolható és a másolattal is ki lehet nyitni a széfet.

Az új rendszerben minden széfhez két kulcs jár: az egyik a nyilvános kulcs (public key), amiről mindenkinek lehet másolata, a másik a privát kulcs (private key), amit a széf tulajdonosa megtart magának. Ha az egyik kulccsal bezárjuk a széfet, akkor csak a másikkal lehet kinyitni. Ilyen módon akárki bezárhat egy üzenetet a széfbe a nyilvános kulccsal, amit csak a széf tulajdonosa tud kinyitni a privát kulccsal, illetve a széf tulajdonosa bezárhat egy üzenetet a privát kulcsával és mindenki, aki a nyilvános kulccsal kinyitja azt, biztos lehet abban, hogy valóban a széf tulajdonosa hagyta az üzenetet a széfben.



2. ábra
Nyilvános kulcsú titkosítás

A nyilvános kulcsú titkosításnál tehát nincsen szükség bizalmas információk előzetes cseréjére. Az Internet világában nagy szükség van erre a módszerre, hiszen a

nyílt rendszerek működésmechanizmusa számos visszaélésre ad lehetőséget: a kommunikációs csatorna decentralizált és nyitott, az oda-vissza áramló információkhoz bárki hozzáférhet és manipulálhatja azokat, tehát megfelelő szintű kriptográfia alkalmazása nélkül semmilyen információ nem tekinthető hitelesnek.
Ez a tény lehetetlenné teszi a privátszférához való jog érvényesülését az elektronikus világban, és a legnagyobb korlátja az on-line világ kommercializációdásának is. Addig nem lehet üzleti tevékenységet folytatni az Interneten, amíg a részt vevő felek nem győződhetnek meg arról, hogy a hálózaton forgalmazott bizalmas információk (pl. megrendelések) nem kerülnek illetéktelen kezekbe, tartalmuk nem változik meg, illetve nem tudnak meggyőződni partnereik személyazonosságáról. A nyilvános kulcsú kriptográfia megoldást kínál erre a problémára, a legnagyobb szoftvercégek használják olyan biztonságos alkalmazások kifejlesztéséhez, amelyek kódolt kommunikációt, digitális aláírást, sőt elektronikus pénzmozgást tesznek lehetővé a nyilvános hálózaton.
Az USA-ban a titkosítás tudományát a kilencvenes évek elejéig az amerikai nemzetbiztonsági szervezet, az NSA (National Security Agency) birtokolta, és az általa kibocsátott titkosítási szabvány, a Digital Encyption Standard szerint kódolt dokumentumokat könnyedén meg tudta fejteni szuperszámítógépei segítségével. A növekvő piaci igény miatt több cég is elkezdett foglalkozni a kriptográfiával, például az RSA Data Security. A felfedezőiről (Rivest, Shamir és Adleman) RSA algoritmusnak nevezték el: nyilvános kulcsú titkosítás elvére épülő szisztéma, azonban olyan megbízható, hogy például a Netscape is ezt választotta a Navigator webböngésző program biztonsági funkcióinak ellátására.

A nyilvános kulcsú titkosítás tette lehetővé az elektronikus pénz létrejöttét is. Számos cég (például a DigiCash, a CyberCash vagy a VeriSign) kibocsátott digitális készpénzt: ez olyan anonim elektronikus fizetőeszköz, amelyikkel lehetséges a tisztán információ alapú pénzforgalom. A felhasználó bankszámlát nyit a kibocsátónál, ekkor kap egy olyan programot, amelyik egy RSA-kódolt adatsorral fizet az eladónak, amelyet az a kibocsátónál valódi pénzre vált. A rendszer fejlettebb, mint a hálózaton ma leginkább elterjedt hitelkártyás fizetési módszer, hiszen a digitális készpénz anonim, tehát kizárja az „adatbányászat" lehetőségét. Problémát okoz, hogy a különböző kisebb-nagyobb cégek eltérő szabványokkal jelentkeznek, így az ipar nagyágyúi (köztük a MasterCard, a Visa, az IBM és a Microsoft) idén megegyeztek egy új szabványban, amelyik a SET (Secure Electronic Transactions, vagyis biztonságos elektronikus tranzakciók) nevet kapta, és nyilvános kulcsú titkosítást használ az on-line hitelkártya-műveletek biztonságossá tételére.
A Microsoft bejelentette, hogy az on-line tranzakcióiba digitális aláírást épít be a Windowsba, az IBM és az RSA Data Security pedig együttműködési szerződést kötött hálózati titkosítási rendszerek fejlesztésére. Az IBM a következő néhány hónapban kriptográfiai rendszerek széles skáláját dobja piacra, a Secure Way elnevezésű termékcsalád az Internet-szolgáltatók, vállalatok és egyéni felhasználók biztonsági igényeit elégítik majd ki.
A kriptográfiai technológiák felértékelődését a szoftveriparban az okozza, hogy az elmúlt néhány évben óriási mértékben megnövekedett az Internet gazdasági jelentősége: a Forrester Research piackutató cég felmérése szerint az Interneten bonyolított

tranzakciók összes pénzforgalma már 1995-ben 30 millió dollár volt, és 2000-re a legmértéktartóbb becslések is több tízmilliárd dollárt prognosztizálnak.

AZ ELEKTRONIKUS KERESKEDELEM HATÁSA

Az Interneten történő kereskedelmi forgalom növekedés két alternatívát jelent.

Az egyik szerint az óriási növekedés az Internet összeomlását jelentheti. Ennek a valószínűsége igen kicsi, mert egyre több cég érdekelt a világháló normális működésében, egyre több pénz áramlik ennek a szektornak a fejlesztésére.

A másik alternatíva szerint, mint szoftveresen, mint hardveresen egyre fejlettebb lesz az Internet. Így egy állandóan változó, fejlődő új világméretű piac jelenik meg ami óriási kereskedelmi, marketing lehetőségeket tartogat.

IRODALOMJEGYZÉK

[1] **Secure Electronic Transaction Specification (SET)**, Book 1: Business Description, June 17, 1996, (http://www.mastercard.com)

[2] Népszabadság, **Világháló melléklet**, 1996. október 21.