Dr. Kanizsai Viktor*

Adatvédelem titkosítással

Bevezetés

A biztonsági rendszereknek mindig nyerniük kell, de a támadónak elég csak egyszer győznie. A számítógépek, rendszerek és informatikai hálózatok korszakában élünk. Az információs technológiák fejlődése szinte exponenciális görbét ír. Az egyének hétköznapjai, valamint a modern üzletelés egyszerűen elképzelhetetlen számítógépes adatfeldolgozás nélkül. A modern társadalom nélkülözhetetlen összetevője az informatikai hálózatok és rendszerek összessége, szinte minden ennek az alárendeltje. Legyen szó otthoni kikapcsolódásról: internetes böngészés, közösségi oldalak, a kapcsolattartás különféle formái, stb.; vagy pedig üzleti folyamatokról: vegyesbolt áru–nyilvántartása, pénztárgép, bankolás, stb., mind – mind számítógépes rendszerek használatát igényli.

Az információs technológiák gyors fejlődésével viszont párhuzamosan a visszaélések újabb és újabb módszerei is mind inkább megmutatkoznak. Az adat, az információ kulcsfontosságú értékké vált, hiszen ezek bizalmasságának, sérthetetlenségének vagy rendelkezésre állásának megsértésével közvetlen anyagi károk is érhetik az egyént, vagy szervezetet. Egyrészt ma már nem kell feltétlenül minőségi szakembernek lenni ahhoz, hogy egy csúcstechnológiás bűncselekményt végrehajtsunk, ehhez csak akarat és minimális tőke kell, másrészt pedig gyorsan és többszörösen visszakaphatjuk a befektetett összeget – a Trustwave cég kutatásai szerint akár 1500%-os is lehet a visszatérülési arány Ransomware[1] vírusok készíttetése és terjesztése esetén[3]. A McAffee cég tanulmányai szerint évente a csúcstechnológiai bűnözés 400 milliárd dollárjába kerül a világnak[8].

Mindemellett, a jól ismert államszintű adatszivárgásos esetek mellett (Wikileaks és Edward Snowden), tanúi vagyunk a vállalatok (pl. JP Morgan[6], Citigroup[2]), a közösségi hálózatok (pl. Facebook[4]), online szolgáltatások (pl. iCloud[1]) adatszivárgásaiknak is.

* *Dr. Kanizsai Viktor, osztályvezető, Információ Biztonsági Osztály, OTP banka Srbija a.d. Novi Sad, Újvidék*

[1] Rosszindulatú szoftver, mely titkosítja a felhasználó állományait és megköveteli tőle, hogy fizessen az állományok újra olvashatóvá tételéért.

Ugyanakkor kétségtelen, hogy az adatvédelmi megoldások nem maradhatnak figyelmen kívűl. Nem elég ma már egy informatikai rendszer funkcionalitására gondolni csak, meg kell tervezni annak biztonságát is, még akkor is ha nem rendszerről van szó, hanem egyéni felhasználóról. Az alábbiakban az adatvédelem megelőző formájának egy módszrere kerül bemutatásra, a titkosítás.

A titkosításról általában

A titkosítás vagy rejtjelezés a kriptográfiának az az eljárása, amellyel az információt (nyílt szöveg) egy algoritmus (titkosító eljárás) segítségével olyan szöveggé alakítjuk, ami olvashatatlan olyan ember számára, aki nem rendelkezik az olvasáshoz szükséges speciális tudással, amit általában kulcsnak nevezünk. Az eredmény a titkosított információ (titkosított szöveg). A titkosított szöveg újra olvashatóvá alakítását visszafejtésnek nevezzük. A titkosítás elsősorban az információ bizalmasságát védi.

Titkosítás hiányában a kommunikáció során az információ a csatornán keresztül jut el a forrástól a célállomásig (lsd: 1. ábra). A csatornát gyakran többen használják, így egymást zavarhatják, illetve „lehallgathatják”.

1. ábra
Titkosítatlan kommunikáció

A titkosítás során az információt úgy alakítjuk át, hogy az csak a megfelelő állomás(ok) számára legyen értelmezhető. A visszafejtés pedig a titkosított információ visszaalakítását jelenti (lsd: 2. ábra).

A titkosító algoritmusok két csoportra oszthatók:

• A titkos algoritmusok: az algoritmus titkossága szolgál biztonsági alapul (csak történelmileg érdekes).

• Kulcs alapú algoritmusok: a biztonság alapját a kulcsok képezik, nem az algoritmus részletei, amelyek akár nyilvánosan is közzé tehetők. Itt az algoritmus leginkább nyilvánosan ismert, és a kulcsot tartják titokban.

2. ábra
Titkosított kommunikáció

Ma a legszélesebb körben használt titkosító algoritmusok a kulcs alapúak, és ezeket három csoportba lehet sorolni:

- Szimmetrikus, amelyeknél egy kulcs használandó,
- Aszimmetrikus, ahol két kulcs van és
- Hibrid, az előző kettő kombinációja.

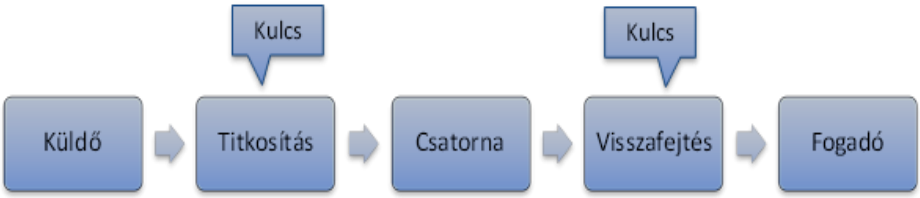
Annak érdekében, hogy az adatvédelem a legmegfelelőbb legyen, a titkosítási algoritmusnak a következő követelményeknek kell eleget tennie:

- Az algoritmus „áttörésének" ára magasabb legyen a titkosított adatok értékétől;
- Az algoritmus „áttöréséhez" szükséges idő hosszabb legyen, mint a titkos adatok bizalmasságának megőrzésére szánt időszakasz;
- Az egy kulccsal titkosított adatok száma kevesebb legyen, mint amennyi arra szükséges, hogy az adott algoritmust „áttörjék".

Szimmetrikus titkosítás

A szimmetrikus kulcsú titkosítás az információk titkosításának a legrégebben ismert és legegyszerűbb módja. Lényege, hogy mind a küldő mind a fogadó ugyanazzal a kulccsal végzi a titkosítást és a megfejtést. Az alapelve egyszerű: a titkosítandó szöveget a közös titkosítási kulcsot felhasználva átalakítjuk, az így kapott információt továbbítjuk, majd a fogadó fél ugyanazt a közös titkosító kulcsot használva fejti azt meg.

A visszafejtés a titkosítás inverz művelete, pl.: ha a titkosítás összeadás, akkor a visszafejtés a kivonás.



3. ábra
Szimmetrikus titkosítás

A legismertebb szimmetrikus kulcsú titkosítási algoritmusokhoz a következők sorolhatóak: DES, 3DES, AES, stb.

DES

Egészen a 2000-es évekig a kriptográfiában leginkább használatos algoritmus a DES (Data Encryption Standard) volt. Az IBM az 1960-as évek végén indított el egy kutatási projektet egy szimmetrikus, titkos kulcsos titkosítási rendszer fejlesztésére. Horst Feistal vezetésével 1971-re kifejlesztették az akkor LUCIFER-nek nevezett algoritmust, amely 128 bites blokkokra osztotta a nyílt szöveget és 128 bites kulcsot alkalmazott a titkosításhoz.

A LUCIFER-t eladták a londoni Lloyd's biztosítónak, amely egy szintén az IBM által fejlesztett készpénz-elosztó rendszerben alkalmazta. Carl Meyer és Walter Tuchman egyetlen chipen akarta implementálni a LUCIFER algoritmust végrehajtó célhardvert, amelyhez némi változtatást is végrehajtott az algoritmusban.

A 70-es évek közepe táján hirdetett pályázatot az NSA (National Security Agency) egy olyan titkosítási eljárásra, amely szabványosítható. Erre a pályázatra nyújtotta be az IBM Carl Meyer és Walter Tuchman az általuk kitalált eljárást, amely messze a legjobb volt az összes benyújtott pályázat között, amit aztán 1977-ben DES néven szabványosítottak is.

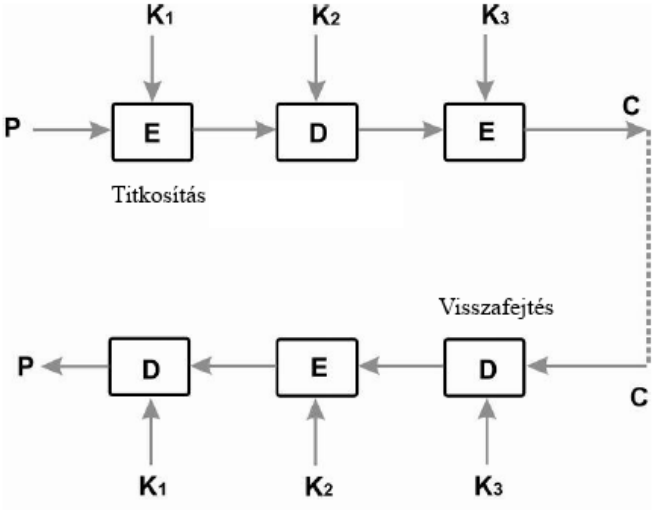
A módszer kiválóan illeszkedett a rohamosan fejlődő elektronikus adatfeldolgozás lehetőségeihez. Magas szintű biztonságot nyújtott, amelyet egyszerű felépítéssel valósított meg. A hardver megoldások jóval hatékonyabbak, mint a szoftveresek, hiszen a DES rengeteg bitszintű műveletet végez.

A DES kulcsmérete 64 bit, azonban minden nyolcadikat kihagyjuk a felhasználásból. Az elhagyott biteket ellenőrzési célokra használják. Így a valódi kulcsméret 56 bit lesz csak.

Az első lépésben a bemenet bitjeit jól összekeverjük, még utolsó lépésben ennek pont az inverzét alkalmazzuk. A DES titkosításban ezt inicializációs permutációnak (IP) nevezzük. Ezután a 16 körös Festel kódolást alkalmazzuk a permutált nyílt szövegre. Végül a titkosított szöveget az IP inverzével kapjuk.

Mivel a kulcstér nem túl nagy, a mai számítási kapacitások mellett az úgy nevezett „brute force" támadásokkal szemben tehetetlen a rendszer. Ezekben az esetekben „egyszerűen" végig nézzük a összes

lehetséges kulcsot a megfejtés érdekében. Nehezíthetjük a feltörést a DES módszer többszöri, egymás utáni alkalmazásával, az így kapott módszerek a TripleDES, illetve 3DES neveket viselik. Az elsőnél három különböző kulcsot alkalmaznak egymás után, még a másodiknál a három alkalmazott kulcsból kettő megegyezik.



4. ábra
TripleDES: P – nyílt, C – titkosított szöveg, E – titkosító, D – visszafejtő algoritmus, K – kulcs

AES

A DES algoritmus 1976-ban való bejelentése óta nagyot változott az informatika világa. Egyre növekedett a hálózati adatforgalom, javult a számítógépek gyorsasága és a szakemberek számára egyre nyilvánvalóbbá vált, hogy DES már nem nyújtja azt a biztonságot, amit az előző évtizedekben nyújtott.

Az AES helyettesítő és lineáris transzformációkat ötvöző módszer. Az ismétlődő körfüggvények négy egymástól független transzformációból állnak:

- SubBytes( ): elemek (bájtok) cseréje az S-box lookup táblázat segítségével,
- ShiftRows( ): elemek elmozdítása meghatározott számú pozícióval,
- MixColumns( ): lineáris transzformáció az oszlopok felett,
- AddRoundKey( ): XOR művelet eredménye.

A transzformációk sorrendje és száma a konkrét kivitelezéstől függ.

A szimmetrikus algoritmusoknál a kulcsokat meg kell osztani a résztvevő felekkel, amely nem mindig olyan egyszerű dolog. Könnyen kimutatható, hogy n számú kommunikáló partner esetén n x ((n-1)/2) kulcsra van szükség, ha minden lehetséges párnak adni akarunk egy közös kulcsot. Ez nagy számú partner esetén elég sok kulcs generálását teszi szükségessé és szimmetrikus módszer használatakor mindenkinek mindenkivel meg kell állapodnia.

A kettő hátránya mellett előnye a gyorsaság, ugyanis rövid kulcsokat alkalmaz, melyeknek köszönhetően nagy a hatékonysága. Ezért a szimmetrikus titkosítást leginkább nagyobb üzenetek titkosítására/visszafejtésére alkalmazzuk.

Aszimmetrikus titkosítás

A nyílt/nyilvános kulcsú rejtjelezés vagy titkosítás, más néven aszimmetrikus kulcsú titkosítás egy olyan kriptográfiai eljárás neve, ahol a felhasználó egy kulcspárral – egy nyilvános és egy titkos kulccsal rendelkezik. A titkos kulcs titokban tartandó, míg a nyilvános kulcs széles körben terjeszthető. A kulcsok matematikailag összefüggnek, ám a titkos kulcsot gyakorlatilag nem lehet meghatározni a nyilvános kulcs ismeretében. Egy, a nyilvános kulccsal kódolt üzenetet csak a kulcspár másik darabjával, a titkos kulccsal lehet visszafejteni.

5. ábra
Aszimmetrikus titkosítás

1975-ben Diffie és Hellman egy forradalmian új titkosítási eljárást hoztak nyilvánosságra. Ebben a titkosításban a titkosító (T) és a megfejtő (M) kulcsok – melyek egy-egy függvényt takarnak s egymás inverzei – közül T-t nyilvánosságra hozzuk, M-et pedig titokban tartjuk, ráadásul minden félnek saját T és M „függvényei” vannak.

Minden szereplő elkészít magának egy T,M kulcspárt, melyek egymás inverzei. A T kulcsot nyilvánosságra hozza, az M kulcsot viszont titokban tartja. Diffie és Hellman rendszerének megvalósításához tehát olyan T,M kulcspárokra van szükség, melyeknél T ismeretében M visszafejtése nagyon bonyolult, ideális esetben lehetetlen.

1976-ban Rivest, Shamir és Adleman a nyílt kulcsú titkosítás elvéhez fejlesztette ki az azóta is népszerű, s elterjedt RSA titkosítási módszert.

RSA

Az RSA-titkosításhoz egy nyílt és egy titkos kulcs tartozik. A nyílt kulcs mindenki számára ismert, s ennek segítségével kódolhatják mások nekünk szánt üzeneteiket. A nyílt kulccsal kódolt üzenetet csak a titkos kulccsal tudjuk „megfejteni”. Az RSA-eljáráshoz a következő módon generáljuk a kulcsokat:

1. Véletlenszerűen válasszunk két nagy prímet, p-t és q-t
2. Számoljuk ki N = pq –t.
   N lesz a modulusa mind a nyilvános, mind a titkos kulcsnak is.
3. Számoljuk ki az Euler-féle φ függvény értékét N-re: φ(N)=(p-1)(q-1).
4. Válasszunk egy olyan egész számot, e-t melyre teljesül 1 <e<φ(N), és e és φ(N) legnagyobb közös osztója 1.
   Az e-t nyilvánosságra hozzuk, mint a nyilvános kulcs kitevőjét.
5. Számítsuk ki d-t, hogy a következő kongruencia teljesüljön, de≡1(modφ(N)). Azaz de=1+kφ(N) bármely k pozitív egészre.
   d-t titokban tartjuk, mint a titkos kulcs kitevőjét.

A nyilvános kulcs az N modulusból és a nyilvános e kitevőből áll, (N,e).

A titkos kulcs az N modulusból és a titkos d kitevőből áll, melyeket természetesen nem osztunk meg mással, (N,d).

A küldő a következő egyenlet segítségével végzi a titkosítást:

C = Pe mod N,

ahol: P, az eredeti szöveg, szám formájában, C, a kódolt szövegnek megfelelő szám; e és N számok és a nyilvános kulcs komponensei. A tikosított üzenetet a következő egyenlettel kell dekódolni:

P = Cd mod N,

ahol a P és C, mint az előző képletben, az N és d viszont a titkos kulcs komponensei.

Gyakorlati alkalmazásra jelenleg az 1024 - 3072 bites modulusokat tekintjük biztonságosnak. Ha az RSA kulcsainak hosszáról beszélünk, akkor ez alatt mindig n hosszát értjük. A biztonság érdekében ajánlott közel azonos méretű prímszámokból előállítani a kulcsot.

Lényeges megjegyezni, hogy az RSA feltörhető, amennyiben az n számot faktoraira tudjuk bontani. Ezt természetesen meg is tudjuk tenni, csak elegendő idő és számítási kapacitás kell hozzá, ami a jelenlegi matematikai ismereteink és számítási kapacitásaink mellett olyan óriási igény, ami nem teszi lehetővé ésszerű időkorlátok mellett a fejtést.

Az aszimmetrikus titkosításnak/visszafejtésnek két előnye van: először is, elhárítja a hiányosságokat a szimmetrikus algoritmus kulcsmegosztásával kapcsolatban két ember kommunikációja során. A szimmetrikus titkosításnál a kulcsot két személy között kell megosztani, és nem felhasználható, ha a két személy közül az egyik egy harmadikkal szeretne kommunikálni. Az aszimmetrikus titkosításnál minden személy két kulcsot hoz létre, egyik titkos, és a tulajdonosa magánál tartja, a másik pedig nyilvános és megosztható másokkal. A másik előnye, hogy a szükséges kulcsok száma (2) jóval kisebb mint a szimmetrikus titkosítás esetén (n*(n-1)/2).

Az asszimetrikus titkosítás legnagyobb hátránya a bonyolult algoritmusok alkalmazása. Hatékony titkosítás esetén nagy kulcsokat kell alkalmazni, ami viszont nagy működési időt igényel. Ezért nem ajánlott az aszimmetrikus algoritmusok alkalmazása nagy forrásadatok esetére. Az aszimmetrikus algoritmusok sokkal hatékonyabbak rövid üzenetek kezelésében.

PGP – Hibrid titkosítás

A PGP (ang: Pretty Good Privacy) működése a két titkosítási módszer kombinációjaként létrejött úgynevezett hibrid titkosításon alapul. A módszer egyesíti a szimmetrikus titkosítás gyorsaságát az aszimmetrikus titkosítás biztonságával. A PGP a titkosítási eljárás során tömöríti a titkosítani kívánt adatot ZIP algoritmussal, majd azt egy véletlen generálású kulccsal (session key) titkosítja.

Ez a folyamat még nagy méretű adatfolyam esetében is gyorsnak tekinthető, hiszen a hibrid titkosítás ezen részében szimmetrikus algoritmussal történik a kódolás. Következő lépésként a session kulcs kerül titkosításra, ez azonban már az aszimmetrikus titkosításból ismert publikus kulccsal lesz titkosítva. Így létrejön egy olyan csomag, amely tar-

talmazza a titkosított adatot és a visszafejtéshez szükséges kulcsot – titkosítva.

Az üzenet titkosításának lépései:

1. Tömörítés.
2. Szimmetrikus titkosítás egy véletlen generálású kulccsal (session key).
3. A véletlen generálású kulcs (session key) titkosítása a címzett nyilvános kulcsával (aszimmetrikus titkosítás) – mivel a session kulcs kis méretű, a titkosítás gyorsan megtörténik.
4. Küldés.

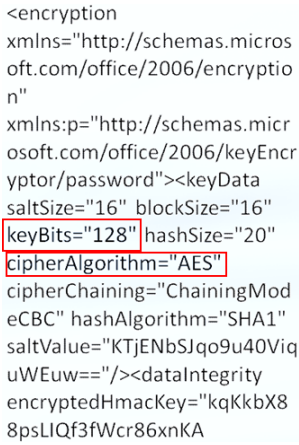
A titkosított üzenet visszafejtése a címzettnél fordított sorrendben történik:

1. Üzenet fogadása.
2. A véletlen generálású kulcs (session key) visszafejtése a címzett titkos kulcsával (aszimmetrikus eljárás).
3. Az üzenet visszafejtése a véletlen generálású kulcs (session key) segítségével.
4. Megjelenítés.

A titkosítás gyakorlati alkalmazása egyszerű felhasználóknál

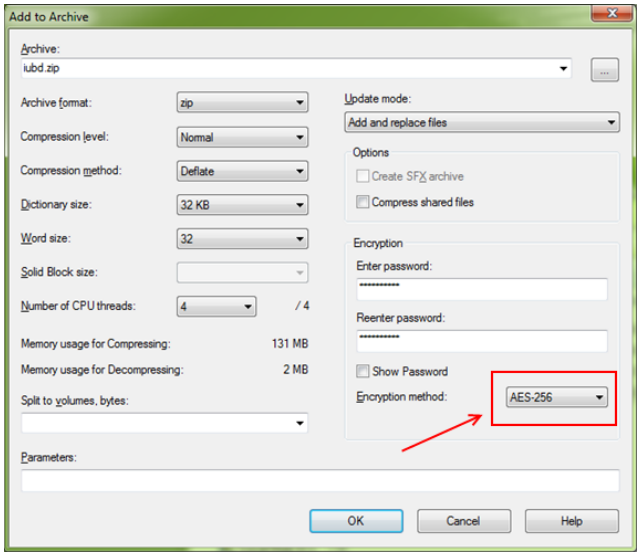
A „Microsoft Word 2010” szimmetrikus, 128-bites kulcsú, AES titkosítást alkalmaz a dokumentum jelszó-védettsége esetén. Ezen utóbbi a 6-os ábrán is látható, egy jelszóval védett dokumentum elemzése során.

A „7-zip” tömörítő alkalmazás is AES titkosítást alkalmaz, méghozzá 256-bites kulccsal (lsd.: 7. ábra). Ez a mai viszonyokhoz mérten megbízhatónak mondható.



6. ábra
Microsoft Word 2010 titkosított dokumentum

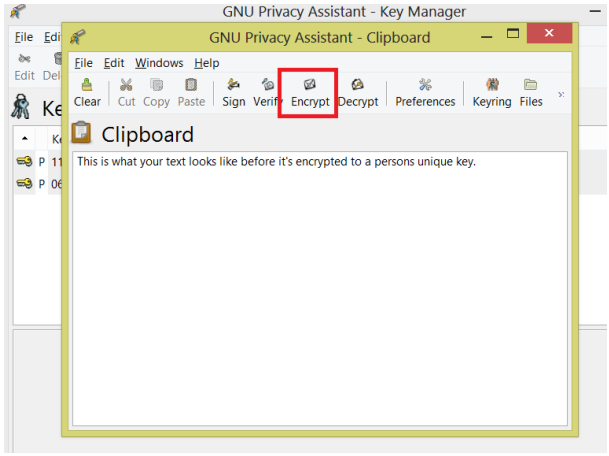
A fent említett állomány – titkosítás esetek a szimmetrikus titkosítás példái, s mint korábban elhangzott, a szimmetrikus titkosítás, gyorsasága miatt, a legalkalmasabb az állományok, illetve merevlemezek (BitLocker és TrueCrypt is AES alapú) hatékony titkosítására.



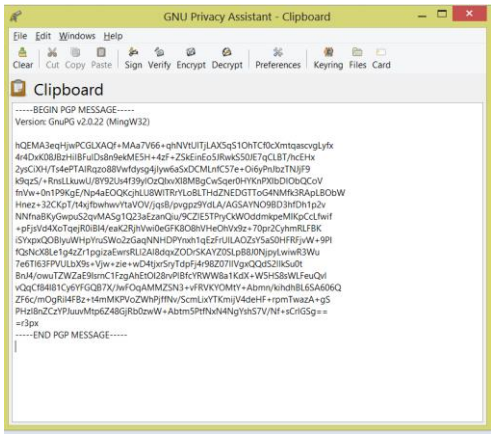
7. ábra
Titkosítás 7-zippel

A „gpg4win“ alkalmazás PGP titkosítást használ. Jelenleg ez számít a legbiztonságosabb módszernek, ha titkosan szeretnénk kommunikálni valakivel.

8. ábra
Titkosítás gpg4win-nel

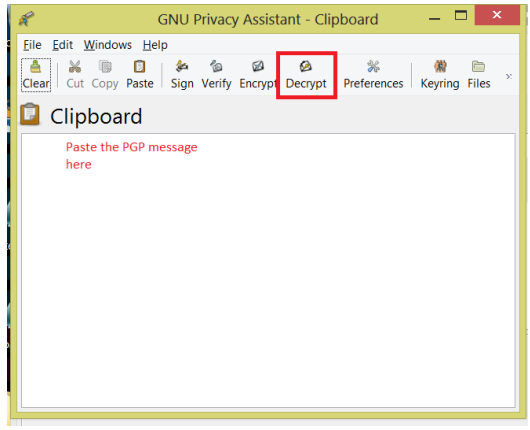


Használata igen egyszerű, a megfelelő kulcsok létrehozása és beolvasása után a küldendő szöveget bemásoljuk az alkalmazás ablakába, elvégezzük a titkosítást és a kívánt csatornán (e-mail, Facebook üzenet, stb.) megküldjük a titkosított szöveget (lsd: 8. - 9. ábra).



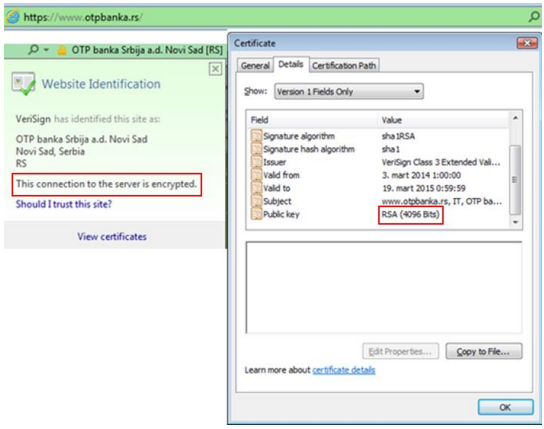
9. ábra
Titkosított szöveg gpg4win-nel

A fogadó a titkosított üzenetet bemásolja az alkalmazás saját ablakába majd visszafejti azt olvasható szöveggé (lsd: 10. ábra).



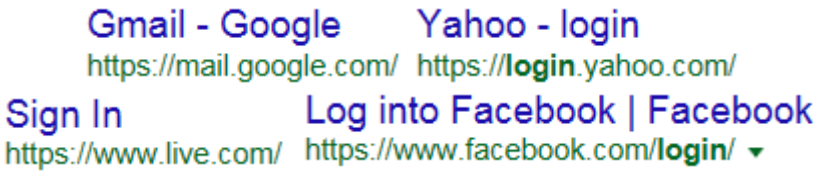
10. ábra
Visszafejtés gpg4win-nel

Az SSL/TLS protokoll hibrid titkosítást alkalmaz. Az alábbi képen látható, hogy a kiválasztott példán az asszimetrikus titkosítás 4096-bites kulcsú RSA titkosítással történik.



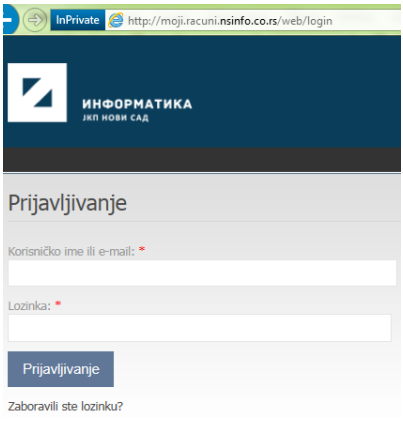
11. ábra
SSL/TLS alkalmazása egy internetes oldalon

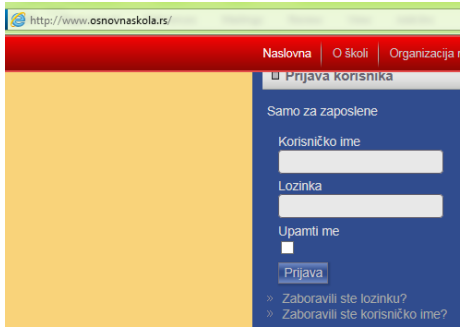
Alábbiakban, néhány példa látható a titkosítást alkalmazó olyan internetes oldalak közül, amelyek bejelentkezést igényelnek (felhasználói név és jelszó így titkosítva kerül továbbításra). Az SSL/TLS alkalmazására a „https” utal.



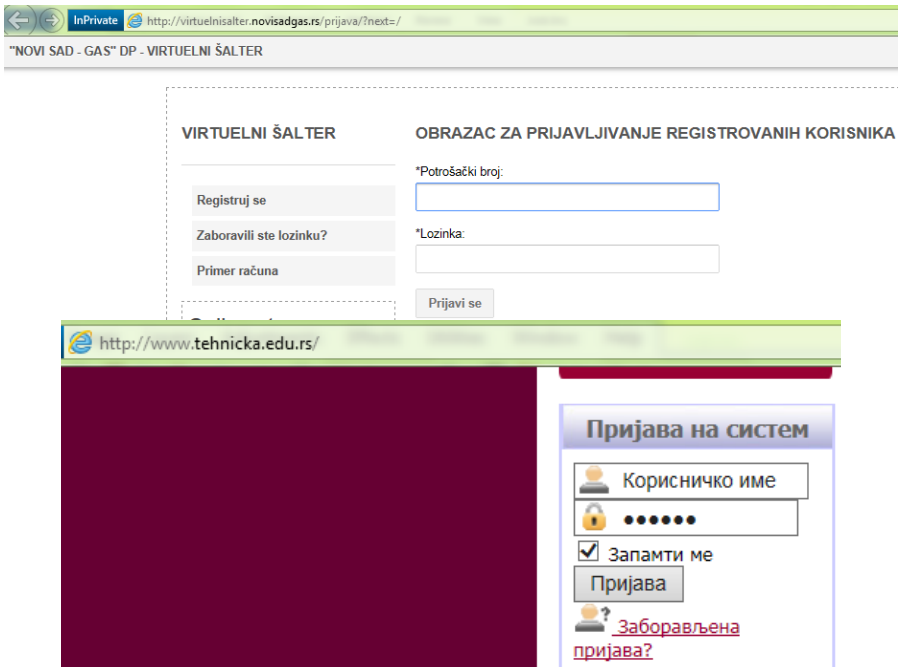
12. ábra
Titkosított bejelentkezést biztosító internetes oldalak példái, utolsó hozzáférés 2015. szeptember 30-án

Végezetül, olyan internetes oldalak példái láthatók, amelyek nem alkalmaznak titkosítást a felhasználó bejelentkezése során.

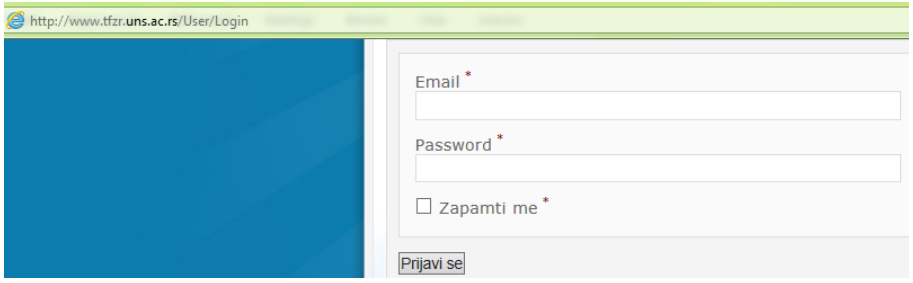




13. ábra
Titkosítatlan bejelentkezések példái, utolsó hozzáférés 2015. szeptember 30-án



14. ábra
Titkosítatlan bejelentkezések példái, utolsó hozzáférés 2015. szeptember 30-án



15. ábra
Titkosítatlan bejelentkezés, utolsó hozzáférés 2015. szeptember 30-án

Összegzés

Az adat, az információ kulcsfontosságú értékké vált, hiszen ezek bizalmasságának, sérthetetlenségének vagy rendelkezésre állásának megsértésével közvetlen anyagi károk is érhetik az egyént, vagy szervezetet. Adataink jogosulatlan megszerzésével és feldolgozásával a csúcs-

technológiai bűnözés újabb áldozataivá válhatunk, mely nem csak anyagi, hanem reputációs kárral is járhat, illetve becsületi sértéssel.

Az adatokat védeni szükséges, ennek pedig egyik módszere a titkosítás. A céltól függően alkalmazható szimmetrikus vagy asszimetrikus kulcsú, illetve hibrid titkosítás.

A gyakorlatban sajnos nem elég mértékben közterjedt a tikosítás alkalmazása, sem egyszerű felhasználók, sem szervezetek körében. A legnagyobb veszély pedig akkor fenyeget, ha sem a szolgáltatást nyújtó, sem az azt igénybe vevő felhasználó nem fordít kellő figyelmet az adatok bizalmasságának megőrzésére.

Ezzel a tanulmánnyal a szerző hozzájárulni szeretne a titkosítás mind gyakoribb alkalmaztatására mint az egyéni felhasználók, úgy a szervezetek körében is.

Felhasznált irodalom:

[1] 2014 celebrity photo hack, http://en.wikipedia.org/wiki/2014_celebrity_photo_hack, hozzáférve 2015. szeptember 21-én.

[2] Citigroup Suffers Massive Data Breach In Japan, http://www.huffingtonpost.com/2011/08/08/citigroup-suffers-another_n_920862.html, hozzáférve 2015. szeptember 24-én.

[3] Cyber-thieves cash in from malware, http://www.bbc.com/news/technology-33048949, hozzáférve 2015. szeptember 25-én.

[4] Facebook Data-Leaking Bug Exposes 6 Million Users' Data, http://www.infosecurity-magazine.com/news/facebook-data-leaking-bug-exposes-6-million-users/, hozzáférve 2015. szeptember 25-én.

[5] Fuszenecker Róbert, A nyílt kulcsú titkosítás és a digitális aláírás, Budapest Műszaki Főiskola, Kandó Kálmán Műszaki Főiskolai Kar, Műszertechnikai és Automatizálási Intézet, 2006.

[6] JP Morgan suffers data breach affecting 76 million customers, http://www.itgovernanceusa.com/blog/jp-morgan-suffers-data-breach-affecting-76-million-customers/, hozzáférve 2015. szeptember 24-én.

[7] Liptai Kálmán, Kriptográfia, Eszterházy Károly Foiskola, Matematikai és Informatikai Intézet Eger, 2011.

[8] Net Losses: Estimating the Global Cost of Cybercrime, http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf, hozzáférve 2015. szeptember 24-én.

[9] Nyilvános kulcsú rejtjelezés, https://hu.wikipedia.org/wiki/Nyilv%C3%A1nos_kulcs%C3%BA_rejtjelez%C3%A9s, hozzáférve 2015. szeptember 21-én.
[10] PGP aláírás levélküldéskor, illetve a kulcs ellenőrzése levél fogadásakor, http://wiki.math.bme.hu/view/PGP_al%C3%A1%C3%ADr%C3%A1s_lev%C3%A9lk%C3%BCld%C3%A9skor,_illetve_a_kulcs_ellen%C5%91rz%C3%A9se_lev%C3%A9l_fogad%C3%A1sakor, hozzáférve 2015. szeptember 24-én.
[11] Szimmetrikus kulcsú rejtjelezés, https://hu.wikipedia.org/wiki/Szimmetrikus_kulcs%C3%BA_rejtjelez%C3%A9s, hozzáférve 2015. szeptember 24-én.
[12] Titkosítás, http://www.jpte.hu/~uhi/kurzus/informatika/titok.htm, hozzáférve 2015. szeptember 21-én.
[13] Titkosítás, https://hu.wikipedia.org/wiki/Titkos%C3%ADt%C3%A1s, hozzáférve 2015. szeptember 21-én.