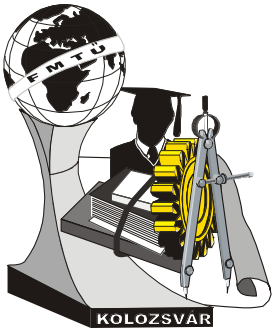
DOI: 10.36243/fmtu-2005.71



X. FIATAL MŰSZAKIAK TUDOMÁNYOS ÜLÉSSZAKA

Kolozsvár, 2005. március 18-19.

AZ *RSA* ALKALMAZÁSÁNAK EGY LEHETŐSÉGÉRŐL

Máthé Zsolt, Görög Levente K.

Abstract
When a consumer walks in to a store to buy goods, she presents herself, her identity, and a payment method. But on the Internet, both the buyer and the seller have difficulties proving each other's identity. How can the buyer convince herself to transmit sensitive information to the seller? How does the seller know about a legitimate purchase order? How do both parties become aware if an uninvited third party copies or modifies transaction information? These questions and many others describe the issues affecting commercial transactions over the Internet.

Összefoglaló
Mikor egy fogyasztó belep az üzletbe bizonyos javakat vásárolni, bizonyítja személyazonosságát, és egy fizetési módszert. De az interneten, mindketten, mint a vevő mint az eladó nehézségekkel bír azonosságának bizonyításakor. Hogyan tudja a vevő meggyőzni magát arra, hogy átadjon fontos információkat az eladónak? Hogyan tudja biztosítani magát az eladó egy valódi rendelésről? Hogyan jut tudatára mint a szolgáltatónak mint az igénylőnek hogy egy hívatlan harmadik lemásolja vagy módosítja az üzlet lebonyolításához szükséges információkat? Ezek a kérdések és meg sok más ehhez hasonló kérdés képezi az interneten való kereskedelem problémait.

Bevezetés

Annak érdekében, hogy biztonságos e-kereskedelmi applikációkat tudjunk építhetni, szükségünk van a biztonsági igények meghatározására. Szükség van az alábbi négy nagy követelmény teljesítésére, egy biztonságos e-kereskedelem váza eseten[4,7]:

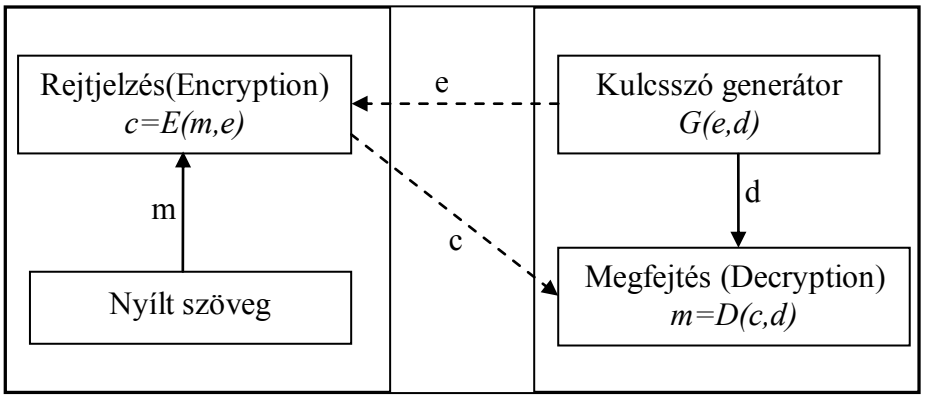
- **Bizalmasság (Confidentiality):** az információk megvédése mindenki elől, a címzetten kívül.
- **Jogosultság vizsgálat (Authentication), Hitelesség (Certification)**: lehetőség bizonyos személy bizonyítására.
- **Sértetlenség (Integrity):** gondoskodni a jogosulatlan információ változtatás lehetetlenségére.
- **(Le)Tagadhatatlanság (Non-repudiation):** megakadályozni egy entitást hogy előző elkötelezettségét vagy tettét letagadja.

Az általánosan használt módszer az adatok bizalmasságának megőrzése érdekében a kriptográfia. De ahogy ezt az elkövetkezőkben meglátjuk, a hagyományos kriptográfiával a hitelességet, sértetlenséget es letagadhatatlanságot lehetetlen kivitelezni, biztosítani. Nyilvános kulcsú kriptográfia az első igazából forradalmi előrelépés ezen elvárások teljesítése végett. A tanulmány ezen fajta kriptográfiát fogja tárgyalni, illetve ezen fajta kriptográfia felhasználását az e-kereskedelemben.

Az alapvető szerepe a kriptográfiának az információk elrejtése. Üzemeltetésének általában két folyamata van: a **rejtjelezés** (encryption), amely az információt átalakítja úgy hogy egy külső személy

érthetetlennek találja, és a **megoldás** vagy **megfejtés** vagy **titkosítás feloldása** (decryption) amely visszaalakítja az érthetetlen szöveget ismét érthetővé. Az információt eredetileg **nyílt szövegnek** (plain text, clear text), a rejtjelezett szöveget pedig **titkosított szövegnek** (cipher text) nevezzük. Ez a folyamat az 1. ábrán látható.[7]

Bruce Schneier vezette be a beszédes, szerepkörhöz kötődő névhasználatot, amely azóta az angol szakirodalomban szinte "szabvánnyá" vált[7,8]. Feltételezzük hogy Alice es Bob akarnak egy



biztonságos kommunikációt. Első lépésben kiválasztanak, vagy kicserélnek egy **(e,d)** kulcs-part. Egy későbbi pillanatban, ha Alice akar egy titkos m információt átküldeni Bobnak, akkor egy **E** matematikai függvényt alkalmaz az m-re, felhasználva az **e** kulcsot, hogy kiszámolja a titkosított szöveget ***c***-t: ***c=E(m,e).*** Mikor Bob megkapja a ***c***-t, o a ***D*** inverz függvényt alkalmazza a ***c***-re a ***d*** kulccsal, hogy visszakapja az ***m***-et: ***m=D(c,d)***. A biztonság abban rejlik hogy a matematikai függvény és a kulcs csak a küldő illetve a fogadó tulajdonában áll.

Egy alapvető kérdés merül fel, hogy miért van szükségünk kulcsokra. Miért nem lehet kiválasztani egy titkosító, és egy annak megfelelő megfejtő függvényt? Hogyha a függvényekhez hozzárendelünk kulcsokat akkor abban az esetben ha a függvények nyilvánosságra kerülnek(az adott kulcsokkal együtt), akkor nem kell új függvényt választanunk csupán a kulcsokat kell megcseréljük. Valójában a kulcsok kritikus fontosságúak és a gyakorlatban gyakori (nem túl költséges) cserélésük továbbá növeli a rendszerek biztonságát.[4]

Nyilvános Kulcsu Kriptografia indoklása

A hagyományos kriptorendszerek (szokás szerint szimmetrikus rendszerek, vagy titkos kulcsú rendszerek) igényelik hogy a feladó (küldő) és a fogadó megosszanak egy kulcsot amelyet csak ok ketten tudnak. Ennek a kulcsnak az ismerete lehetővé teszi a rejtjelezett üzenet megfejtését. Az 1. ábrán ez az eset áll fent amikor ***e=d***. A rejtett kulcsú kriptográfia hosszú történelemre tekint vissza, a legelterjedtebb algoritmus ezen fajta rejtjelezésre a **DEA** (Data Encryption Algorithm) amely a DES (Data Encryption Standard) által van meghatározva, más ilyen algoritmus[8] a **Triple DES**, **IDEA**, **RC4** (Rivest Chiper 4), **RC6** (Rivest Chiper 6), Blowfish es Twofish. Annak ellenére hogy ezek erős biztonságot nyújtanak, több hátrányuk van, mint például:

- **Kulcs kiosztás/csere**: Egy kétszemélyes kommunikáción belül a kulcs titkos kell maradjon, mindketten kell ismerjek, az információ csere előtt, tehát a két fel nagyméretű figyelmet kell áldozzon a kulcsszó cserekor hogy egy hallgatódzó ne kaphassa meg.
- **Kulcs kezelés**: Egy nagy hálózaton belül több kulcsot kell kezelni. Továbbá, hogy a biztonság garantálható legyen gyakran, akar minden kommunikáció eseten kulcsot kell cserélni.

Tehát a klasszikus titkos kulcsú kriptográfia biztonsági problémákat kelt. Azonkívül a hitelesség, sértetlenség és letagadhatatlanságot lehetetlen megoldani ilyen rendszereken keresztül. Az

áttörés 1976-ban történt, amikor Diffie es Hellmann[2] feltalálta a nyilvános kulcsú kriptográfiát. Amellett hogy megoldottak a kulcs csere és kulcs kezelés problémáit, a nyilvános kulcsú kriptorendszerek több más előnnyel is rendelkeznek. Emellett teljesítik a fentebb említett négy elvárást is.

A titkos kulcsú kriptográfiával ellentétben a nyilvános kulcsú kriptorendszerek két kulcsot igényelnek minden ***A*** felhasználótól: egy nyilvános kulcsot, $K_{pub}(A)$ amely nyilvánosságra van hozva és egy másik, magán kulcsot $K_{pri}(A)$ amely titokban van tartva. Egy üzenetet amelyet az ***E*** függvénnyel kódolunk felhasználva az **egyik kulcsot**, a ***D*** függvénnyel lehet kikódolni és **csak** a **másik kulcs** felhasználásával. Hogyha Alice akar küldeni egy üzenetet, valamilyen információt Bobnak, használja Bob nyilvános kulcsát, hogy kódolja az üzenetet (jelölés: $\mathbf{E_{Kpub(Bob)}(m)}$). Bob miután megkapja a rejtjelezett információt az ő saját kulcsát használva megfejti az üzenetet (jelölés: $\mathbf{D_{Kpri(Bob)}(c)}$).

Elméletileg a nyilvános kulcsú kriptográfia megvalósítható egy speciális egy-irányú (one-way) függvénnyel [6], a trapdoor one-way függvénnyel [8]. Matematikailag az f egy-irányú függvény egy olyan függvény amely eseten ***f(x)*** kiszámítása könnyű bármely ***x*** bemenetre, viszont f^{-1} kiszámítása nagyon nehéz. (i.e. nehéz megoldani az ***f(x)=y*** egyenletet, ahol y ismert). Egy trapdoor one-way függvény egy olyan függvény amelyben az ***f(x)=y*** egyenlet megoldása egyszerűvé válik egy kiegészítő információ segítségével.

A következő két probléma a legvalószínűbb hogy biztosíthatja egy ezt a fentebb említett tulajdonságot:

- **Egész számok faktorizálásának problémája**: egy összetett hatalmas egész ***n***, amely nagy prím, ***p*** és ***q*** szorzata. Míg találni nagy prím számokat relatív könnyű, addig két nagy prím szorzatának faktorizálása komputacionálisan nagyon alkalmatlan. Ebben az esetben a trapdoor one-way függvény elv teljesedik, hogyha ismerjük a ***phi(n)***-t (lásd alább) akkor a faktorizálás mar egyszerű.
- **Diszkrét logaritmus problémája**: adott egy ***p*** prím, egy ***g*** generátor($\mathbf{Z_p^*}$), és egy ***a*** elem a $\mathbf{Z_p^*}$-ből. A feladat abban áll hogy úgy határozzuk meg az egyedi ***i*** egészet, ***0<=i<p-1***, úgy hogy $a \equiv g^i \pmod p$. A diszkrét logaritmus hasznossága abban rejlik hogy nagyon nehéz diszkrét logaritmusokat találni. A brute force eljárás $g^j \pmod p$, ***0<=j<p-1,*** egyáltalán nem járható út nagy p eseten.

Nagy része a nyilvános kulcsú kriptorendszereknek az előbbi két probléma nehézségre alapozódik. A következő részek a leggyakrabban elterjedt publikus kulcsú kriptorendszereket tárgyalják.

RSA Kriptorendszerek

Az RSA az egyik legismertebb nyilvános kulcsú kriptorendszer. R.L.Rivest, A. Shamir és L.M.Adleman publikálta 1978-ban [1]. A rendszer az egész számok faktorizációjának nehézségen alapszik, a Z_n-csoportban. Az RSA két lépésben irható le:

1. RSA, beállítások: cél egy nyilvános/titkos kulcs generálása.

- Bob generál két óriásprímet, ***p***-t és ***q***-t
- Kiszámolja ***n = pq***-t és ***phi(n) = (p-1)(q-1) mod n***-et
- Választ egy véletlenszerű ***e*** számot (***0 < e < phi(n)***), úgy, hogy ***e*** és ***phi(n)*** relatív prímek legyenek. A továbbiakban ***e***-t nyilvános hatványnak, exponensnek nevezünk. Kiszámolja ***d***-t, mint az ***e*** modulo ***phi(n)*** inverze, vagyis megoldja az ***ed ≡ 1 (mod phi(n))*** lineáris egyenletet. ***d*** lesz a titkos hatvány.
- Bob nyilvánosságra hozza az ***(e,n)***-párt, mint nyilvános kulcsot és megtartja ***(n,d)***-t, mint titkos kulcsot. ***p*** és ***q*** feltétlenül titkos kell maradjon, nem art megsemmisíteni őket.

2.ábra: nyilvános/titkos kulcs generálása az RSA-ban

A fenti eljárásban alapvető elvárás, hogy ***e*** és ***phi(n)*** relatív prímek legyenek. Ellenkező esetben nem lehetne megoldani a moduláris lineáris egyenletet amelyből kapjuk ***d***-t, másszóval nem lenne ***e***-nek inverze a ***phi(n)*** moduláris osztályban.

2. RSA, az algoritmus: adatok rejtjelezése és megfejtése

KÉRELEM: Adottak: Z_n csoport és az ***(n,e,d)*** halmaz: ***n = pq***, ***p*** és ***q*** primek, ***ed ≡ 1 (mod phi(n))***.
FELTÉTEL: Alice ismeri Bob ***(n,e)*** nyilvános kulcsát, de nem ismeri Bob titkos kulcsát ***(n,d)***.

ALGORITMUS:
1. Alice rejtjelezi az ***m*** üzenetet kiszámolva $c = m^e \bmod n$-et.
2. Alice elküldi ***c***-t Bobnak
3. Bob megfejti ***c***-t kiszámolva $c^d \bmod n$-et és visszakapja ***m***-et.

Ahogy a fenti leírásból látható, az egyetlen matematikai művelet, amelyre szükségünk van az adataink rejtjelezésére és megfejtésére, a moduláris hatványozás, vagyis egy xy mod n formájú függvény kiszámítása. Ennek kiszámítására több olyan ismeretes eljárás van, amelyek polinomiális komplexitásúak, az x bináris alakjában levő bitjeinek számától függ [5]. Észrevehető, hogy a rejtjelezés és a megfejtés egymással inverz műveletek. RSA 3. lépésének bizonyítása a 4-es ábra

ADOTTAK: $ed \equiv 1 \pmod{phi(n)}$ => $ed = k * phi(n) + 1$ egy bizonyos **k**-ra.

$$
\begin{aligned}
c^d \bmod n &\equiv (m^d)^e \bmod n \\
&\equiv m^{ed} \bmod n \\
&\equiv m^{k * phi(n)+1} \bmod n \\
&\equiv (m^{phi(n)})^k m \bmod n \\
&\equiv 1^k m \bmod n \\
&\equiv m \bmod n
\end{aligned}
$$

Az eljárásnak a biztonsága azon a tényen alapszik, hogy a $c = m^e \bmod n$ rejtjelező függvény egyirányú, vagyis matematikailag lehetetlen lesz egy ellenség számára a ***c*** megfejtése. Ahhoz, hogy ez

sikerüljön neki, szüksége van ***d***-re, mivel ki kell számolja $m = c^d \bmod n$-et. A fentebb már emlitettük, hogy ***e***-t és ***d***-t az $ed \equiv 1 \pmod{phi(n)}$ lineáris egyenlet kapcsolja össze, vagyis az ellenseg kiszámolhatja ***d***-t ha ismeri ***phi(n)***-et. Továbbá az ***n=pq***-ra, ahol ***p*** és ***q*** prímek, a ***phi(n)=(p-1)(q-1)*** képlet áll fenn, vagyis észrevehető, hogy az RSA feltörése a ***p*** és ***q*** ismeretét feltételezi, vagyis ***n*** faktorizációját [4].

Hivatkozások

[1] Rivest, R.L., Shamir, A., and Adleman, A. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM.* 21 (1978), pp. 120-126.

[2] Diffie, W. and Hellman, M.E. New Directions in Cryptography. *IEEE Transactions in Information Theory*. IT-22(1976), pp. 644-654.

[3] Menezes, A., Oorschot, P.V., and Vanstone, S. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL, USA, 1996.

[4] Mao, W., *Modern Cryptography, Theory and Practice*, Hewlett Packard Books, Prentice Hall, NJ, USA, 2004

[5] Cormen, T.H., Leiserson, C.E., Rivest, R.L., and Stein, C., Introduction to Algorithms (Second Edition). MIT Press, Cambridge, MA, 2001.

[6] Public Key Cryptography, Mohapatra, P. K., *ACM Crossroads Fall 2000-7.1,* 2000.

[7] Virasztó, T., *Titkositás és adatrejtés*, NetAcademia Oktatoközpont, 2004.

[8] Schneier, B. *Applied Cryptography. 2nd Edition*, John Wiley & Sons, New York, 1996.

Mathe E. Zsolt/ egyetemista III. év
Kolozsvari Műszaki Egyetem, Számítástechnika szak / Marosvasarhely, Cornesti utca 42. szam
Tel., email: 0740351000, mathezsolt@yahoo.com

Görög Levente-Károly / egyetemista III. év
Sapientia Egyetem / Icland 68, MS 547218
Tel., email: 0742606039, goroglev@yahoo.com