ADATBIZTONSÁG: TITKOSÍTÁS, HITELESÍTÉS, DIGITÁLIS ALÁÍRÁS

Buttyán Levente
PhD, egyetemi adjunktus, BME Híradástechnikai Tanszék
buttyan@hit.bme.hu

Györfi László
az MTA rendes tagja, egyetemi tanár
BME Számítástudományi és Információelméleti Tanszék
gyorfi@szit.bme.hu

Vajda István
a műszaki tudomány doktora, egyetemi tanár, BME Híradástechnikai Tanszék
vajda@hit.bme.hu

A kriptográfia alapvető céljai és története

Mindennapi életünkben gyakran találkozunk az információ elektronikus tárolásával, továbbításával és feldolgozásával kapcsolatos feladatokkal. A tárolt vagy továbbított információ gyakran érzékeny abban az értelemben, hogy annak illetéktelen megismerése, csalárd célú módosítása anyagi, erkölcsi kár okozására, jogosulatlan előnyszerzésre ad módot. Ezért a biztonság az információs és kommunikációs technológiák alkalmazhatóságának alapvető kritériumává vált.

Az információs és kommunikációs rendszerek biztonságát algoritmikus, fizikai, illetve rendszabályi technikák kombinálásával érhetjük el. Ebben a cikkben az algoritmikus módszerekről szeretnénk tömör áttekintést adni. Ezeket a módszereket más szóval *kriptográfiai* módszereknek is nevezik.

A kriptográfia alapvető céljai:

- *Titkosítás:* Célja a lehallgatás megakadályozása, pontosabban annak biztosítása, hogy egy lehallgatást végző támadó ne értse meg a lehallgatott üzenetek tartalmát.
- *Integritásvédelem:* Célja annak biztosítása, hogy egy üzenet vevője megbízhatóan meg tudja állapítani a vett üzenetről, hogy annak tartalma az átvitel során módosult-e vagy sem.
- *Hitelesítés:* Célja az üzenetfabrikálás és a megszemélyesítés detektálása. A hitelesítés folyamata során tehát a hitelesítést végző résztvevő megbízhatóan meggyőződik egy vett üzenet feladójának vagy egy párbeszédben részvevő másik félnek a kilétéről. Előbbit üzenethitelesítésnek, utóbbit partnerhitelesítésnek nevezzük.
- *Letagadás elleni védelem:* Célja annak elérése, hogy egy üzenet küldője ne tudja letagadni az üzenetküldés tényét, vagy más szavakkal, az üzenet vevője bizonyítani tudja, hogy ki az üzenet küldője.

A fenti célok elérése különböző kriptográfiai mechanizmusok (algoritmusok és protokollok) alkalmazásával lehetséges. E mechanizmusok közül tekintjük át a legfontosabbakat a következő fejezetekben.

A kriptográfia egyébként nem az újkor emberének találmánya, eredete visszanyúlik az ókori görögökhöz, rómaiakhoz, bár

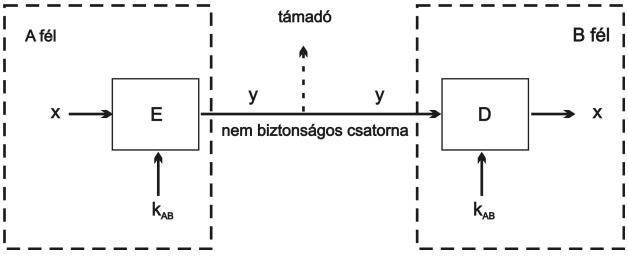
akkor még csak a titkosírás, rejtjelezés tudományát értették alatta. Az első rejtjelezések a nyílt üzenet betűinek felcserélésére vagy helyettesítésére épültek. A betűnkénti helyettesítés ötlete egészen a XIX. századig tovább élt, természetesen egyre összetettebb formában (például többábécés betűnkénti helyettesítés). A XX. század első évtizedeiben tökéletesedtek azok a módszerek, amelyek a matematikai statisztika eszköztárának felhasználásával alkalmasak voltak a gyakorlatban alkalmazott többábécés helyettesítők analízisére. *William Friedman* ilyen módon fejtette meg a japánok rejtjelezőjét az 1930-as évek végén. *Gilbert Vernam*, az AT&T mérnöke 1918-ban javasolta a klasszikus Vigenére-eljárás véletlen kulcsszöveggel történő alkalmazását. Ez a módszer – melyet *one-time pad*-nek (OTP) is hívnak – a ma ismert egyetlen, tökéletesen biztonságos eljárás, abban az értelemben, hogy ha valaki megszerzi (lehallgatja) a rejtett szöveget, bizonyíthatóan nincs módja a nyílt szöveggel kapcsolatosan az *a priori* ismereteinél többet megtudni. Vernam módszerének ezen tökéletességét *Claude Shannon* bizonyította. Shannon azt is megmutatta, hogy a tökéletes titkosságnak komoly ára van: a titkos kulcs hossza legalább akkora, mint az átküldendő üzenet. A tökéletes rejtjelező tehát a polgári gyakorlatban használhatatlan. Shannonnal vette kezdetét az információelmélet és a kriptográfia modern korszaka. Munkáiban lefektette mindazon matematikai alapokat, amelyek a konvencionális rejtjelezés tudományának és módszereinek évtizedekig vezérfonalul szolgáltak.

A következő fordulópontot *Whitfield Diffie* és *Martin Hellman* 1976-ban megjelent cikke jelentette, amelyben a gyakorlati titkosság fogalma alapján megvetették a nyilvános kulcsú kriptográfia alapjait. Ez számos új, korábban ismeretlen biztonsági megoldásnak nyitott teret, mint például a digitális aláírásnak. Diffie és Hellman ötletét követve, az első praktikusan is jól használható nyilvános kulcsú algoritmust *Ronald Rivest, Adi Shamir* és *Leonard Adleman* találta ki 1977-ben, melyet a szerzők nevének kezdőbetűi alapján RSA algoritmusnak hívnak.

Szimmetrikus és aszimmetrikus kulcsú rejtjelezés

Tegyük fel, hogy egy *A* üzenetküldő szeretné átküldeni üzenetét *B*-nek egy olyan kommunikációs csatornán, amelyről feltételezhető: nem biztonságos abban az értelemben, hogy egy, a csatornán „hallgatózó” támadó képes a csatornán áthaladó biteket megfigyelni. Az üzenetet küldő szeretné megakadályozni, hogy a támadó illetéktelenül visszafejtse az üzenetét, azaz szeretné az üzenetet rejtjelezni.

A konvencionális, más néven szimmetrikus kulcsú rejtjelezés modelljét az *1. ábrán* vázoltuk. Jelöljük az átküldendő üzenetet x-szel. A rejtjelezés az *x* nyílt üzenetből az $y = E(k_{AB}, x)$ rejtett üzenetet állítja elő, ahol *E* egy k_{AB} paraméterű rejtjelező (kódoló)



1. ábra • A szimmetrikus kulcsú rejtjelezés modellje

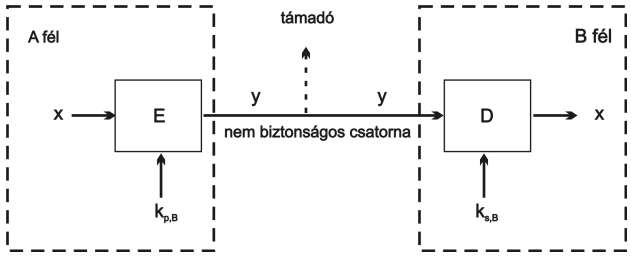
transzformáció. A k_{AB} paramétert a rejtjelezés kulcsának nevezzük, amely meghatározza (kiválasztja) az aktuális rejtjelező transzformációt. A k_{AB} kulcs tetszőleges rögzített értéke mellett, az E kódoló transzformáció egy kölcsönösen egyértelmű leképezés. A kódoló transzformáció inverze a D dekódoló transzformáció, amely az y rejtett üzenetet egyértelműen leképezi, visszafejti az $x = D(k_{AB}, y)$ üzenetbe. A k_{AB} kulcsot csak a két kommunikáló fél, A és B ismeri (erre utal az index), s így csak ők tudják végrehajtani a kódolást és a dekódolást. Természetesen A-nak és B-nek a rejtjelezést megelőzően biztonságosan meg kell állapodnia a k_{AB} kulcs értékében, általában az egyik fél egy védett, titkos csatornán juttatja el a k_{AB} kulcsot a másikhoz.

Az aszimmetrikus kulcsú rejtjelezés modellje a *2. ábra* mutatja. A szimmetrikus kulcsú rejtjelezéshez képest annyi a különbség, hogy a kódoló és a dekódoló kulcs nem azonos, sőt a dekódoló kulcsot a kódoló kulcsból kiszámítani „nehéz” feladat. Egy aszimmetrikus kulcsú rendszerben minden rendszerbeli B résztvevőhöz tartozik egy kulcspár, mely a $k_{p,B}$ kódoló kulcsból és a $k_{s,B}$ dekódoló kulcsból áll, ahol a kódoló kulcs nyilvános (ezért nevezik ezt a rejtjelezési módszert nyilvános kulcsú rejtjelezésnek is), míg a dekódoló kulcs titkos, azt csak B ismeri. Egy több résztvevőt tartalmazó rendszerben a nyilvános kulcsokat egy nyilvános kulcstárba teszik le, amelyet bárki olvashat. Ha A szeretne egy x üzenetet rejtjelezetten küldeni B-nek, akkor kiolvassa a nyilvános kulcsok tárából a $k_{p,B}$ kódoló kulcsot, és az $y=E(k_{p,B}, x)$ rejtett üzenetet küldi B-nek. Ezen y rejtett üzenetből $x = D(k_{s,B}, y)$ dekódolással nyeri ki B az x üzenetet. A kódolás a nyilvános kulcs ismeretében „könnyű” feladat, míg a dekódolás a rejtett kulcs ismeretének hiányában gyakorlatilag nem végrehajtható, „nehéz” feladat. „Nehéz” feladatra példa egy nagy összetett szám prímtényezőkre bontása.

Az aszimmetrikus kulcsú rejtjelezés előnye tehát, hogy a titkos kommunikáció megvalósításához nincsen szükség egy közös titkos kulcs előzetes létrehozására (cseréjére) a küldő és a vevő között; elegendő a rejteni kívánt üzenetet a vevő nyilvános kódoló kulcsával rejtjelezni. Megjegyezzük azonban: a küldőnek meg kell tudnia győződni arról, hogy a használni kívánt nyilvános kulcs valóban a vevő nyilvános kulcsa, és nem egy harmadik, feltehetően rossz szándékú félé. A nyilvános kulcsú kriptográfia tehát oly módon egyszerűsíti a kulcscsere-problémát, hogy titkos csatorna helyett hiteles csatorna létezését követeli meg a vevő és a küldő között, melyen a vevő eljuttathatja nyilvános kulcsát a küldőnek.

Üzenethitelesítő kódok

Az üzenethitelesítés feladata a kommunikációs csatornán átküldött üzenetek hitelességének és integritásának biztosítása. Pontosabban, az üzenethitelesítés lehetővé teszi az üze-



2. ábra • Az aszimmetrikus kulcsú rejtjelezés modellje

net vevője számára a küldő identitásának ellenőrzését és az átvitel során az üzenetben bekövetkezett változások (melyek származhatnak véletlen hibából vagy szándékos módosításból) detektálását.

Az üzenethitelesítést leggyakrabban üzenethitelesítő kódok alkalmazásával valósítják meg. Egy üzenethitelesítő kódra gondolhatunk úgy, mint egy kriptográfiai ellenőrző összegre, amit a küldő az üzenet elküldése előtt kiszámít, és az üzenethez csatol. A csatornán átvitelre kerül az üzenet és az üzenet ellenőrző összege is. A vevő mindkettőt veszi, majd ellenőrzi az ellenőrző összeget. Fontos megjegyezni, hogy az üzenethitelesítő kód értéke nemcsak magától az üzenettől függ, hanem egy a küldő és a vevő által megosztott titkos kulcstól is. A támadó ezen titok hiányában nem tud fabrikált vagy módosított üzenetekhez érvényes üzenethitelesítő kódot előállítani. A vevő tehát meg lehet győződve arról, hogy minden helyes üzenethitelesítő kóddal vett (és nem saját magától származó) üzenet csakis a vélt (például az üzenetben megjelölt) küldőtől származhat, és annak integritása sértetlen.

Digitális aláírás

Az üzenethitelesítő kód lehetővé teszi a csatornán átküldött üzenetek (véletlen és szándékos) módosításának detektálását és az üzenetek küldőjének hitelesítését. Ezeket a szolgáltatásokat azonban csak a vevő számára biztosítja. A vevő egy kívülálló harmadik felet már nem tud meggyőzni arról, hogy egy vett üzenet sértetlen, és a küldőtől származik, hiszen az üzenethitelesítő kód értéke egy olyan kulcstól függ, melyet a vevő is ismer. A harmadik fél tehát nem tudja biztosan eldönteni, hogy az adott üzenethitelesítő kódot a küldő vagy a vevő generálta. Ez azt jelenti, hogy a küldő bármikor *letagadhatja,* hogy egy üzenetet küldött a vevőnek, és a vevő nem tudja bebizonyítani, hogy a küldő hazudik. Más szóval, az üzenethitelesítő kódok nem biztosítanak (eredet) letagadhatatlanságszolgáltatást.

A letagadhatatlanság-szolgáltatás megvalósítására olyan aszimmetrikus mechanizmusra van szükség, melynek segítségével csakis az üzenet küldője állíthatja elő az üzenet eredetére vonatkozó bizonyítékot (így azt hamisítani nem lehet), de a rendszer bármely résztvevője (köztük a vevő is) ellenőrizni tudja azt. Ezt a mechanizmust digitális aláírásnak nevezik, mivel tulajdonságai nagymértékben hasonlítanak a hagyományos aláírás tulajdonságaihoz. Egy fontos különbség a digitális és a hagyományos aláírás között az, hogy a digitális aláírás nem az üzenet anyagi hordozójához (például papír) kötődik, hanem magához az üzenethez. Így nemcsak az üzenet eredetére vonatkozóan nyújt garanciát, hanem segítségével az üzenet tartalmában az aláírás generálása után bekövetkezett módosításokat is detektálni lehet. Összefoglalva tehát: a digitális aláírás olyan mechanizmus, mely biztosítja az üzenetek integritását és hitelességét, valamint az üzenetek eredetének letagadhatatlanságát.

A digitális aláírás fent említett aszimmetrikus tulajdonsága miatt a jól ismert digitális aláírássémák mind nyilvános kulcsú technikákra épülnek. Egy digitális aláírásséma két komponensből áll: egy aláírásgeneráló algoritmusból és egy aláírásellenőrző algoritmusból. Az aláírásgeneráló algoritmus az aláíró fél titkos aláíró kulcsával van paraméterezve, míg az ellenőrző algoritmus az aláíró fél nyilvános aláírásellenőrző kulcsát használja paraméterként. Az aláírásgeneráló algoritmus bemenete az aláírni kívánt m üzenet, kimenete pedig egy σ digitális aláírás. Az aláírásellenőrző algoritmus bemenete egy m üzenet és egy σ aláírás, kimenete pedig 1, ha σ az aláíró fél érvényes aláírása m-en, és 0 egyébként. Értelemszerűen, az ellenőrzést végző fél akkor fogadja el az aláírást hitelesnek, ha az ellenőrző algoritmus kimenete 1. Természetesen az ellenőrzés végrehajtásához

az ellenőrző félnek ismernie kell az aláíró fél nyilvános kulcsát, mert ez szükséges az ellenőrző algoritmus helyes paraméterezéséhez. Az aszimmetrikus kulcsú rejtjelezéshez hasonlóan, itt is biztosítani kell tehát a nyilvános kulcsok hitelesítését.

Megjegyezzük, hogy ha egy nyilvános kulcsú rejtjelező rendszerben, minden m üzenetre teljesül az $E(k_{p,A},D(k_{s,A},m)) = m$ egyenlőség, vagyis a kommutativitás (például az RSA titkosító rendszer esetén), akkor a rejtjelező rendszerből digitális aláírásséma készíthető a dekódoló transzformáció aláírásgeneráló algoritmusként, és a rejtjelező transzformáció aláírásellenőrző algoritmusként történő használatával.

Gyakorlati okokból célszerű, ha a digitális aláírás mérete nem függ az aláírt üzenet méretétől. Ezt úgy érhetjük el, hogy nem magát az üzenetet írjuk alá, hanem annak egy rögzített hosszúságú ún. lenyomatát, amely praktikus értelemben megbízhatóan reprezentálja magát az üzenetet. Ehhez egy kriptográfiai lenyomatképző függvényt, vagy más néven *hash* függvényt használunk, amely tetszőleges hosszúságú bináris sorozatot rögzített hosszúságú (rövidebb) bináris sorozatba képez le. Annak érdekében, hogy a lenyomat valóban megbízhatóan reprezentálja az üzenetet, egy kriptográfiai hash függvénytől megköveteljük, hogy az egyirányú és ütközésellenálló legyen.

Kriptográfiai mechanizmusok minősítése

Egy kriptográfiai algoritmusnak egy támadó korlátlan számítási erőforrásával szemben mutatott védettségét információelméleti (tökéletes) biztonságnak *vagy feltétel nélküli biztonságnak,* míg a korlátos erőforrású esetet *algoritmikus (gyakorlati) biztonságnak* vagy feltételes biztonságnak nevezzük. Rejtjelező algoritmusok közül egyetlen algoritmust ismerünk csak, amely feltétel nélkül biztonságos: a one-time pad (OTP) rejtjelezőt. Tudjuk azonban, hogy a feltétel nélküli biztonság ára nagy: a rejtjelező kulcsának hossza legalább akkora, mint a tömörített nyílt üzenet mérete. A legtöbb alkalmazásban tehát az OTP rejtjelező nem praktikus, és kénytelenek vagyunk feltételes biztonságú algoritmusokkal megelégedni.

De hogyan lehetünk biztosak abban, hogy kriptográfiai algoritmusunk (feltételesen) biztonságos? A tradicionális (nem bizonyított biztonságú) megközelítésben úgy, hogy megkísérlünk egy támadást találni. Ha sikerrel járunk, akkor azt mondjuk, hogy nem biztonságos az algoritmusunk. Ha nem találunk támadást, akkor semmi megbízhatót nem tudunk mondani az algoritmus biztonságáról. Ha kiderül, hogy nem biztonságos az algoritmusunk, akkor – a támadás erejétől, jellegétől függően – vagy véglegesen elvetjük a konstrukciót, vagy megpróbáljuk megerősíteni a támadás jellegének megfelelően (azaz foltozunk).

Ezzel szemben létezik a minősítésnek egy megalapozottabb módszere is, amely azonban nem mindig vezet a gyakorlatban is jól használható konstrukciókhoz. Ezt a *bizonyított biztonság* elméletének nevezik. Ebben a megközelítésben először definiálunk egy biztonságfogalmat (ahol a különböző fogalmak különböző támadási környezetek modellezését jelentik), azaz megmondjuk, mit értünk pontosan a biztonságon (definíció). Kriptográfiai algoritmusunkat valamely biztonságosnak feltételezett elemre (például egy „nehéznek” hitt matematikai problémára) építjük (feltételezés). Az algoritmusunk biztonságosságát ezek után indirekt módon bizonyítjuk: feltesszük, hogy egy Z támadó sikerrel fel tudja törni (az alkalmazott biztonságfogalomnak megfelelő értelemben) a kriptográfiai algoritmusunkat, majd megmutatjuk, hogy Z támadási algoritmusát felhasználva egy Z' támadó sikerrel fel tudja törni a biztonságosnak vélt elemet (például hatékony algoritmust ad a „nehéznek” hitt problémára). Ezzel ellentmondásba

kerülünk eredeti feltételezésünkkel. A szó igazi értelmében tehát nem bebizonyítjuk a biztonságot, hanem visszavezetést végzünk a feltételezésre. Ezt redukciónak nevezzük.

A bizonyítható biztonság modern elméletének klasszikus korszaka az 1980-as évekre tehető. Ezen elmélet kiindulópontja az egyirányú függvény, s az annak létezésével kapcsolatos sejtés. Egyirányú függvényeken alapszik a bizonyíthatóan biztonságos álvéletlengenerátor. Ezen álvéletlengenerátor felhasználásával definiálták az álvéletlen függvényt, majd arra építve az álvéletlen permutációt. Ugyanezen sorrendben épülnek egymásra a kapcsolódó konstrukciók is. Mindezen elemek a szimmetrikus kulcsú rejtjelezés komplexitáselméleti megalapozását adják. Az egyirányú függvények speciális esetei az úgynevezett csapda típusú egyirányú permutációk; ezekre épülnek az aszimmetrikus kulcsú rejtjelezők első bizonyított biztonságú konstrukciói.

Alkalmazások

A fent bemutatott kriptográfiai mechanizmusok számos alkalmazásával találkozhatunk a mindennapi életben, még ha az átlagos felhasználó ennek nincs is mindig tudatában. Kriptográfiai módszerekkel történik például a híváskezdeményező hitelesítése a GSM rendszerben, a bankkártyák mágnescsíkján tárolt adatok védelme az illetéktelen módosítások ellen, és a fizetős műholdas adások kódolása. Itt most a web biztonságát szolgáló protokollról, az SSL-ről (Secure Socket Layer) szólunk röviden. Az SSL protokoll hitelesített és titkos kommunikációt tesz lehetővé a böngésző és a webszerver között. Mikor a felhasználó a böngészőben egy https://... kezdetű linkre kattint, akkor a böngésző és a linkben megnevezett webszerver az SSL protokollt kezdi el futtatni. Ezt általában a böngészőablak alján megjelenő kis kulcs vagy zárt lakat jelzi. Az SSL protokoll elején a böngésző és a szerver először egy kulcscserét hajt végre, mely során aszimmetrikus kulcsú kriptográfiai módszereket (nevezetesen az RSA-t vagy a Diffie–Hellman-algoritmust) használva létrehoznak egy közös titkos kulcsot, melyet az SSL terminológiában mestertitoknak neveznek. A mestertitokból a böngésző és a szerver előállítja a kapcsolat során használandó szimmetrikus kapcsolatkulcsokat. Ezután minden egymásnak küldött adatot (kérést és weblapot) ezen kapcsolatkulcsokkal védenek, ahol a védelem üzenethitelesítő kód és szimmetrikus kulcsú rejtjelezés alkalmazását jelenti. Az SSL protokoll használata esetén tehát egy támadó nem látja a böngésző és a szerver között átküldött adatokat, és nem tudja azokat észrevétlenül módosítani sem. Az SSL protokollt ezért gyakran alkalmazzák, amikor valamilyen bizalmas információt (például jelszót vagy hitelkártyaszámot) kell megadnia a felhasználónak egy adott weboldal vagy szolgáltatás eléréséhez.

A kriptográfia és a hálózatbiztonság oktatása a BME Villamosmérnöki és Informatikai Kar műszaki informatika szakán az *Információelmélet* és a *Kódelmélet* alaptárgyak után, az *Adatbiztonság* alaptárgy, valamint az *Infokommunikációs rendszerek biztonsága* szakirány keretében történik. A szakirány három féléve alatt öt tárgyat (Számítógépes biztonságtechnológia, Hálózatbiztonsági protokollok, Infokommunikációs szolgáltatások biztonsága, Hibatűrő hálózati architektúrák és modellezésük, A biztonságos elektronikus kereskedelem alapjai) hallgatnak a hallgatók, tizennyolc mérési gyakorlaton szereznek kézzelfogható, praktikus, készségszintű ismereteket, és minden félévben önálló projekteken keresztül mélyíthetik el tudásukat egy-egy speciális témában. Az oktatás mellett nemzetközi szinten is elismert kutatás folyik a Budapesti Műszaki és Gazdaságtudományi Egyetemen, az információs és kommunikációs rendszerek biztonsága területén. A kriptográfia oktatásában és kutatásában meghatározó

szerepet tölt be a Híradástechnikai Tanszék CrySyS Adatbiztonsági Laboratóriuma (www.crysys.hu).

Kulcsszavak: *adatvédelem, adatbiztonság, rejtjelzés, titkosítás, algoritmusok, protokollok, hitelesítés, digitális aláírás*

IRODALOM

Buttyán Levente – Vajda István (2004): *Kriptográfia és alkalmazásai*. TypoTeX, Budapest

Györfi László – Győri S. – Vajda I. (2000): *Információ- és kódelmélet*. TypoTeX, Budapest

Lovász László (2004): *Mit kívánnak a számítógépek a matematikától, és mit adnak neki? Mindentudás Egyeteme 2*. Kossuth, Budapest, 357–370.

Mao, Wenbo (2003): *Modern Cryptography: Theory and Practice*. Prentice Hall PTR

Nemetz Tibor – Vajda István (1991): *Algoritmusos adatvédelem*. Akadémiai, Budapest

Rónyai Lajos – Ivanyos G. – Szabó R. (2002): *Algoritmusok*. Typotex, Budapest

Stinson, Douglas (2002): *Cryptography: Theory and Practice*. CRCPress, Boca Raton