Előszó

Az elmúlt 20 év alatt a kriptográfia terén végzett nyilvános kutatás robbanásszerű fejlődésen ment keresztül. Ennek a folyamatnak a hátterében alapvetően az áll, hogy az információs technológiák egyre mélyebben behatoltak a gazdaságokba, azok motorjaivá lettek, s ezeken keresztül az egyes egyén mindennapi életét is átszövik az információ elektronikus tárolásával, továbbításával és feldolgozásával kapcsolatos feladatok. Az információ gyakran érzékeny abban az értelemben, hogy annak illetéktelen megismerése, csalárd célú módosítása anyagi, erkölcsi kár okozására, jogosulatlan előnyszerzésre ad módot. A biztonság az információs technológiák alkalmazhatóságának alapvető kritériumává vált. Az információ biztonságát algoritmikus, fizikai, illetve rendszabályi technikák kombinálásával érhetjük el. A kriptográfia az algoritmikus biztonsági módszerek tudománya.

Tankönyvünk célja a kriptográfia legfontosabb módszereinek elméleti taglalása, s azok tipikus alkalmazásainak bemutatása olyan mélységben, amely – a tankönyv keretei és az adott feladatok önmagukban vett nehézsége mellett – eljuttatja az olvasót a tervezés és minősítés gyakran igen nehéz technikáihoz is. Mindezek alapos elsajátítását számos kidolgozott példa, s feladatok tára is támogatja. A cél – természetesen – nem kriptográfusok képzése, ugyanakkor a megoldások elméleti hátterének, feltételrendszerének alapos ismerete nélkül információs biztonsági területen bárminemű alkalmazásba fogni vagy létező alkalmazás biztonságát megítélni megalapozatlan, s nem tanácsos. Tankönyvünk törzsanyagának megcélzott olvasóközönsége elsősorban a felsőfokú informatikai oktatás hallgatósága. A könyv anyaga azonban ezen túlmutat, s néhány speciális elméleti terület (pl. a bizonyítható biz-

tonság elmélete vagy a kriptográfiai protokollok formális analízise), illetve a feladattár nehezebb problémái szakszemináriumok anyagát is alkothatják. Készséggel elismerjük, hogy nem volt – s nem is lehetett – célunk valamennyi élő, izgalmas területet lefedni a kriptográfia elmélete és alkalmazásai teljes spektrumában, s igyekeztünk lehetőleg olyan területeken maradni, amelyek valamennyire kötődnek oktatási és kutatási preferenciáinkhoz. A tankönyv alapvetően elméleti indíttatású, s így a biztonságos implementálás kérdéskört nem érinti, bár tudatában vagyunk annak a ténynek, hogy a napi biztonsági problémák nagyrészt implementációs hibákból származnak, s nem az elméleti építőelemek hibáiból. Ugyanakkor meg vagyunk győződve arról, hogy az elméleti háttér alapos megértése hosszabb távra érvényes, biztosabb fogódzót jelent az alkalmazónak az efféle hibák elkerülésére.

A tananyag gerincét a kriptográfiai algoritmusok elméleti taglalása képezi. A kriptográfiai algoritmusok építőelemei a kriptográfiai primitívek és protokollok. A tankönyvben nagy súllyal szerepel ezen építőelemek elméleti megalapozása, azok reprezentánsainak bemutatása, valamint a különböző kapcsolatos algoritmikus támadási módszerek taglalása. A támadások kérdésköre rendkívül fontos a kriptográfiában, hiszen a biztonságot a támadásokkal szembeni ellenállóképesség mértéke adja. A bizonyítható biztonság modern elmélete önálló részként szerepel a könyvben. Az elméleti részek megértését nagyszámú példával kívántuk segíteni. Ezen elméleti alapokra építve mélyebben megérthetők az alkalmazási példák, melyeket az internetes és a mobil hálózatokban használt biztonsági protokollok, illetve az elektronikus fizetési protokollok köréből vettük.

A könyv négy nagy részre tagolódik. Az I. rész a kriptográfiai primitíveket taglalja klasszikus felfogásban. Az alapfogalmak bevezetése után a szimmetrikus valamint az aszimmetrikus kulcsú rejtjelezők tervezési módszereit, legfontosabb képviselőit tárgyaljuk. Bemutatjuk a differenciális és a lineáris kriptanalízis alapjait, melyek a ma ismert legerősebb általános támadási módszerek szimmetrikus kulcsú rejtjelezők ellen. A leggyakrabban alkalmazott aszimmetrikus kulcsú rejtjelező, az RSA számos támadását is elemezzük. Az elliptikus görbéken alapuló tervezés elméleti hátterébe is betekintést adunk. Szintén az I. részben taglaljuk még a kriptográfiai tömörítő függvények tervezésének alapjait.

A II. részben a korábban bevezetett kriptográfiai primitívekre épülő legfontosabb kriptográfiai alapprotokollokat mutatjuk be, amelyek már önmagukban is használhatók bizonyos biztonsági szolgátatások megvalósítására, de sokszor más, komplexebb feladatot ellátó protokollok építőelemeiként ke-

rülnek alkalmazásra. Részletesen tárgyaljuk a blokkrejtjelezők gyakorlatban használt működési módjait, elemezve az egyes módok hátrányait és előnyeit. Bemutatjuk a kriptográfiai tömörítő függvényekre épülő üzenethitelesítési technikákat, az üzenethitelesítő kódok konstrukcióit. Ebben a részben tárgyaljuk a digitális aláírás protokollokat is, részletesen bemutatva azok biztonsági követelményeit és a gyakorlatban használt „tömörít és aláír" paradigma elvét. Végül, de nem utolsó sorban, a partner-hitelesítést és a kriptográfiai kulcsok gondozását támogató protokollok kerülnek bemutatásra, elsősorban a szimmetrikus kulcsok biztonságos cseréjére koncentrálva. Ezek már többszereplős, általában többlépéses üzenetcserét alkalmazó protokollok, s bár szerkezetük könnyen áttekinthető, tervezésük meglepően sok hibalehetőséget rejt magában. Az egyes protokollok elleni támadások részletes elemzésén keresztül így betekintést nyerhetünk ezen protokollok tervezésének elméleti hátterébe.

Könyvünk III. része kriptográfiai alkalmazásokkal foglalkozik. Természetesen igényes alapossággal a lehetséges alkalmazások teljes spektrumát nem lehet lefedni egy részben, de talán még egy teljes könyvben sem. Ugyanakkor úgy érezzük, hogy a valós alkalmazások tervezése, bevezetése és használata során nyert tapasztalatok igen hasznosak lehetnek a tankönyv által megcélzott olvasóközönség, az informatikus hallgatók számára, hiszen nagy valószínűséggel valamilyen szinten maguk is hamarosan kapcsolatba kerülnek kriptográfiai alkalmazásokkal. Ezért a III. rész a lehetséges alkalmazásoknak egy általunk érdekesnek és fontosnak tartott részét mutatja be. A bemutatott alkalmazások három témakörbe csoportosíthatók: internetes biztonsági protokollok, vezetéknélküli (mobil) távközlő hálózatokban alkalmazott biztonsági protokollok és az elektronikus kereskedelemben használt vagy tervezett kriptográfiai fizetési protokollok.

A IV. rész egyik fő célja a modern kriptográfia bizonyítható biztonság fogalmainak, főbb elméleti eredményeinek, konstrukcióinak megismertetése. Bonyolultság-elméleti megközelítésben kerül bevezetésre az egyirányú függvény, majd erre építve az álvéletlen bitgenerátor, az álvéletlen függvény és álvéletlen permutáció fogalma. Itt kerülnek bevezetésre azon biztonsági fogalmak és támadási modellek, amelyek mellett a bizonyítható biztonság elmélete és technikái bizonyítást adnak algoritmusok támadhatatlanságára. Bemutatjuk a véletlen orákulum modellben történő bizonyítási technikákat is.

A fejezetek túlnyomó többségének végén, a fejezet anyagához kapcsolódó feladatokat tűztünk ki. Igazából akkor sajátította el az olvasó az anyagot, ha megbirkózik a kitűzött feladatokkal is. A legtöbb feladat megoldását a könyv

végén, külön fejezetben közöljük. Azon feladatokat, melyek megoldása nem került bele a könyvbe, *-gal jelöltük meg.

Végül, szeretnénk megköszönni Ádám Zsolt, Árendás Csaba, Bacsárdi László, Debrei Gábor, Erős Tamás, Frajka Tamás, Holczer Tamás, Maschek Ádám, és Patakfalvi Tamás segítségét, akik drága idejüket feláldozva átolvasták a könyv kéziratának korábbi változatait, és megjegyzéseikkel, észrevételeikkel segítették a könyv színvonalának emelését. Külön köszönet jár Frajka Tamásnak, aki ezen túlmenően hasznos tanácsokkal segítette munkánkat, és odaadó segítséget nyújtott a kézirat szerkesztésében is. Hálásak vagyunk továbbá Szabó Istvánnak, a könyv lektorának hasznos észrevételeiért, melyeket igyekeztünk figyelembe venni a végső változat elkészítésénél.

Budapest, 2004. február 9. *Buttyán Levente és Vajda István*