Kriptográfia a gazdaságinformatikai képzésben
– Mit és hogyan? –

CSAJBÓK ZOLTÁN
Debreceni Egyetem Egészségügyi Főiskolai Kar
főiskolai adjunktus
csajzo@freemail.hu

ABSTRACT

The science of cryptography has a wide range of application in the modern electronic business life, even in every day's business. The present article deals with the educational aspects of the cryptography for the business information technology students in the higher education. First, it makes a survey known about the history of cryptography, then gives a short introduction to the essence of cryptography, and finally it summarizes the most relevant themes and its most current practices.

A titkosítás tudományát évszázadokig kisajátították az olyan tipikus és hagyományos alkalmazók, mint például a hadsereg és a diplomácia. A XX. század '70-es éveitől kezdődően azonban „a hírközlés robbanásszerű fejlődése azt az igényt is megteremtette, hogy akár *ismeretlen emberek* is biztonságos, mások számára érthetetlen levelezést folytathassanak egymással anélkül, hogy erre vonatkozóan korábban bármilyen közös megállapodást kellett volna tenniük" [10, 187. o.]. „Fontos, a problémakör titkosságát feloldó körülmény, hogy a rejtjelezési eljárások piacán új, hatalmas fogyasztó jelent meg: *az üzleti élet*" [1, 250. o.].

A jelen cikk alapját képező kutatást a B*M*K Audit-Konzulting Kft. és a Digitus-Pro Bt. támogatta.

Mit? Rövid történeti áttekintés

A kriptográfia oktatása hagyományosan a klasszikus titkosító eljárások bemutatásával indul. A klasszikus kriptográfiai rendszerek azon a kézenfekvő ötleten alapulnak, hogy a kódolandó szöveg betűit valamilyen szisztéma szerint ugyanazon ábécé más betűivel helyettesítik. E körbe három eljáráscsalád tartozik, az eltolásos titkosítás vagy Ceasar-kód, a helyettesítéses- és az affin-titkosítás [2,[15]: A Ceasar-kód lényege, hogy az eredeti szöveg betűit valamelyik rákövetkezőjével helyettesítik minden betű esetében ugyanolyan mértékű eltolást alkalmazva.

Mindhárom esetben mind a rejtés, mind a fejtés viszonylag egyszerű és látványos, didaktikailag pedig lehetőség nyílik a kriptográfia több fontos fogalmának, illetve eljárásának bemutatására és azok kritikai elemzésére (ez utóbbi önmagában is a kriptográfia jellemzője):

- eltolásos titkosítás: a *kulcstér* problematikája; a kis kulcstér kriptográfiai kockázata: a *teljes kipróbálás* (exhaustive search) vagy *nyers erő* (brute force) módszere
- helyettesítéses titkosítás: egyszerűen fejthető a nyelv betűinek gyakorisága alapján [12]
- affin-titkosítás: rejtés-fejtés, *moduláris aritmetika*].

Mária, skót királynő (XVI. század) titkosírása a hamis biztonságérzet tragikus példázata: „egy gyönge kód esetenként rosszabb, mint a nyílt szöveg" [20, 50. o.]. Mária merényletet szervezett unokatestvére, Erzsébet angol királynő ellen.

Biztonságosnak hitt „kommunikációs csatornája”, azaz futárja kettős ügynök volt, aki titkos levelezését kiszolgáltatta ellenségeinek. A viszonylag gyenge kódot sikerült megfejteni, és ezzel nemcsak a levelek tartalmához jutottak hozzá, hanem a válaszlevelek *meghamisításával* további adatok kiadására is rábírták. Végül a nyilvánvaló bizonyítékokat felhasználva Máriát és társait vérpadra küldték.

A Vigenère-eljárás

A Vigenère-eljárás 26 különböző kódábécét használ (B. DE VIGENÈRE XVI. századi francia diplomata, kriptográfus). Az első az egybetűs eltolással létrehozott Ceasar-kód, a második a kétbetűs stb. Az eredeti szöveg betűit más-más kódábécével kódolják. Természetesen a sikeres kommunikáció feltétele, hogy minkét fél ugyanabban a sorrendben használja a különböző kódábécét. Ez történhet úgy, hogy megállapodnak egy kulcsszóban, és a szöveg egyes betűinek kódolásához a kulcsszó egymást követő betűivel kezdődő kódábécét használják. A Vigenère-kód erőssége, hogy a betűk gyakorisági elemzésével feltörhetetlen és nagy a kulcstere. Előnyei ellenére két évszázadra feledésbe merült.

A Vigenère-kód a XIX. század közepe táján támadt fel ismét, mégpedig az elektronikus kommunikáció által támasztott igények miatt. Ez idő tájt terjedt el általánosan ugyanis a távíró és a morze. A morzeábécé nem jelent titkosítást, egyszerűen csak egy más ábécé, amit a távíró „ért”. Az üzenet tartalmának megóvása érdekében először kódolni kell, és csak azt követően adják át a távírókezelőnek, aki azt morzejelek formájában továbbítja. A történelem során az elektronikus kommunikáció ekkor igényelt először kriptográfiai eszközöket.

Akkoriban a Vigenère-eljárást feltörhetetlennek tartották, de a gondtalannak tetsző évek nem tartottak sokáig. C. BABBAGE 1854-ben megfejtette a Vigenère-kódot, de módszerét nem publikálta, és csak a XX. században, BABBAGE jegyzetanyagának átvizsgálása után derült fény eredményére. Egyik lehetséges magyarázat szerint a brit titkosszolgálat nyomására tartotta titokban felfedezését. Akárhogy is történt mindössze kilenc év után, 1863-ban F.W. KASISKI, a porosz hadsereg nyugállományú tisztje is megfejtette a Vigenère-eljárást. Korszakos felfedezését nyilvánosságra hozta. A fejtés alapja az, hogy a kulcs ismétlődik [11, [13, [20].

Verman-kód

A Vigenère-sztorinak azonban még koránt sincs vége: egy kis módosítással megfejthetetlen rendszerré alakítható. A módszer neve véletlen átkulcsolás vagy Vernam-kód, angolul one-time pad (magyarul nevezik még végtelen átkulcsolásnak vagy egyszeri kulcsos, egyszeri blokk módszernek). Lényege, hogy a kulcs véletlen (egyenletes eloszlású) betűk sorozata, amelynek hossza megegyezik az eredeti szöveg hosszával; maga a kódolás ezen a kulcs segítségével a Vigenère-eljárásnak megfelelően történik. Itt lényegében egy Vigenère-kódról van szó, azzal a cseppet sem elhanyagolható többlettel, hogy az eredeti üzenet minden betűjét véletlenszerűen kiválasztott külön-külön ábécével kódolják. Egzakt matematikai eszközökkel bebizonyítható, hogy a *Vernam-kód elméletileg is fejthetetlen*, feltéve, hogy egy véletlen kulcsot csak egyetlen egyszer használnak. Hiába próbálnánk ugyanis ki az összes lehetséges kulcsot, és állítanánk elő ezekkel az adott hosszú összes lehetséges üzenetet, *nincsen semmiféle támpont a helyes, azaz az eredeti illetve a helytelen üzenetek elkülönítésére*.

A Vernam-kódot J. MAUBORGNE őrnagy, az Amerikai Egyesült Államok hadseregének kriptográfiai osztályvezetője és G. VERNAM az AT&T munkatársa javasolta 1917-ben [18, 15. o.]. Fejthetetlenségét információelméleti eszközökkel C.E. SHANNON bizonyította be [19]; a bizonyítás magyarul a [5, 320. o.] könyvben található.

Azt gondolhatnánk, hogy ha megvan a megfejthetetlen kód, akkor vége a kriptográfia történetének, de távolról sem ez a helyzet. Mindenekelőtt a véletlen átkulcsolás gyakorlatilag alig, vagy csak nagyon különleges körülmények között alkalmazható. Ilyen különleges eset volt például a Moszkva és Washington közötti „forró drót", illetve SORGE 1935 és 1941 között Japánból küldött titkos jelentései [1, 251. o.]. A megvalósítás gyakorlati nehézségei röviden a következőkben foglalhatók össze: sok (valódi) véletlen számsort igényel, egy véletlen számsort csak egyszer szabad használni, abszolút megbízható módon kell a partnerhez eljuttatni és megőrizni (titokban tartani), végül a felhasználás után meg kell semmisíteni.

KAHN munkája a kriptográfia történetének kimerítő tárgyalását tartalmazza

[7], míg a magyar nyelvű kriptográfiai művek a rejtjelezés magyarországi történetéről adnak áttekintést [14[17]. GÁRDONYI Géza titkosírásának, amely közel öt évtizedig nyugtalanította-izgatta az irodalmár és nem irodalmár érdeklődők figyelmét, inkább irodalomtörténeti jelentősége van [4].

A kriptológia alapfogalmai

A számítógépes rendszerek védelme három, módszertanilag jól elkülöníthető területre osztható: *fizikai* (például beléptető rendszer, elektronikus eszközök árnyékolása stb.), *ügyviteli* (például jelenléti ív, gépnapló stb.) és *algoritmikus* védelem. A három terület csak együtt, egymást kiegészítve, egymásra épülve képes a megfelelő védelmet biztosítani. A kriptográfia az algoritmikus adatvédelem területéhez tartozik.

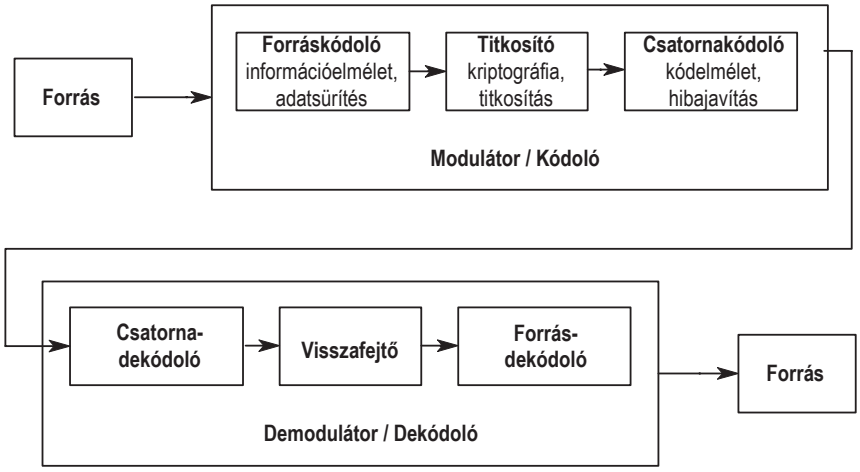
Definíció szerint a *kriptográfia* a titkosítás (rejtés) tudománya, amely nehéz matematikai problémák felhasználásával biztosítja az algoritmikus védelmi eszközök biztonságos megvalósítását. A kriptográfia eszközei a matematikai módszereket alkalmazó *algoritmusok*. Az algoritmusok használatának pontos leírását a *kriptográfiai protokollok* tartalmazzák. Míg a kriptográfia a rejtés, addig a *kriptoanalízis* a fejtés tudománya, amely a kriptorendszerek elemzésével, feltörésével, gyenge pontjainak feltérképezésével foglalkozik. A matematikának a kriptográfiát és a kriptoanalízist magában foglaló ágát pedig együttesen *kriptológiának* nevezzük.

A kriptográfia alapfogalmai

Hírközlési modellnek két főszereplője van, az *adó,* aki az eredeti üzenetet kibocsátja, és a *vevő,* akihez az eredeti üzenetet el kell juttatni. Az üzenet valamilyen csatornán keresztül juthat el a címzetthez, amely az informatikai és/vagy hírközlési napi gyakorlatban rendszerint bináris, azaz kétállapotú jeleket továbbító elektronikus eszköz, berendezés.

Általános esetben az üzenetet először időmegtakarítás és költségcsökkentés, sokszor egyszerűen „csak" a működőképesség céljából tömörítik. E kérdéssel foglalkozik többek között az *információelmélet*. A tömörített üzenetet tartalmának megóvása érdekében titkosítják, amely a *kriptográfia* témakörébe tartozik. Végül az átvitelre kész üzenetet le kell fordítani a csatorna nyelvére, azaz kódolni kell. A kódolás közben azonban fontos, hogy a csatornát ért zavaró hatások ellen is megóvjuk az átvitt tartalmat.

Fel kell hívni a figyelmet a *kódolás* szó *kettős* értelmére (homonima). Kriptográfiai értelemben az eredeti szöveg titkosítása; kódelméleti értelmezés szerint pedig azt jelenti, hogy a csatorna bemenetén lévő (eredeti vagy már titkosított) szöveget le kell fordítani a csatorna nyelvére, és ellenállóvá kell tenni a csatornát ért zavaró hatásokkal szemben (hibajavítás). A kriptográfiai értelmében vett kódolás fogalmára van egy másik szavunk a sifrírozás, de ennek használata a gyakorlatban kevéssé terjedt el. A szövegkörnyezetből általában egyértelműen kiderül, hogy a kódolás melyik jelentéséről van éppen szó. A kódolás és a hibajavítás a *kódelmélet* tárgya. Természetesen e három témakör szoros kölcsönhatásban áll egymással, de eszközrendszerük, módszertanuk külön-külön is tárgyalható.



20. ábra Hírközlési modell titkosítással

Titkosításkor az eredeti szöveget, szakszóval a nyílt szöveget, a *kulcs* segítségével valamilyen algoritmussal és egy kiegészítő információval kell kódolni. Minden kriptográfiai rendszer vizsgálható az algoritmusnak nevezett általános, és a kulcsnak nevezett konkrét módszer szerint. A kriptográfia modern felfogásában az *algoritmust nem kell titokban tartani*, lényeg az, hogy a *kulcs és az eredeti szöveg maradjon titokban*.

A *kulcs fontossága* a kriptográfia egyik legfőbb alapelve, amelyet már 1883-ban megfogalmazott A. KERCKHOFFS VON NIEUWENHOF holland nyelvész: „A kódolási rendszer megbízhatósága nem függhet a titkosítás algoritmusától, azt csak a kulcs titkának megőrzése garantálja.” [20, 21-22. o.] Az igazsághoz hozzátartozik, hogy a kulcs titokban tartása csak akkor ér valamit, ha a szóba jöhető kulcsok száma, szakszóval a kulcstér számossága meglehetősen nagy. Egyébként a teljes kipróbálás módszerével a titkos kulcs megismerhető. Hasonlóképpen fogalmaz J. A. BUCHMANN nemrég megjelent kriptográfia tankönyvében: „Modern cryptoanalysis assumes that an attacker knows which cryptosystem is used. Only the (private) keys and the plaintexts are assumed to be secret.”[6] [2].

[6] A modern kriptoanalízis azzal a feltételezéssel él, hogy a támadó ismeri az általa megtámadott kriptorendszert. Csak annyi a feltétel, hogy a (privát) kulcs és az eredeti szöveg titkos.

A kriptorendszer matematikai modellje

A kriptorendszer egzakt matematikai eszközökkel történő megfogalmazását az alábbiakban összegzem. A kriptorendszer matematikai modellje egy (P,C,K,E,D) ötös, ahol

- P: nyílt szövegek halmaza; formálisan: véges ábécé feletti véges szavak halmaza (plain text space).
- C: titkosított szövegek halmaz; formálisan: véges ábécé feletti véges szavak halmaza (ciphertext space).
- K: kulcstér (key space).
- E: titkosító (kódoló) függvények halmaza (encryption functions); formálisan:

  $$E=\{E_k \mid E_k : P\times K\rightarrow C, k\in K\}$$

- D: fejtő (dekódoló) függvények halmaza (decryption functions); formálisan:

  $$D=\{D_k \mid D_k : C\times K\rightarrow P, k\in K\}$$

Továbbá minden $e\in K$ (kódoló) kulcshoz létezik olyan $d\in K$ (dekódoló) kulcs, hogy:

$D_d(E_e(p)) = p$ minden $p\in P$ esetén.

Megjegyzés: A E_e függvény inverzének hagyományos jelölése a D_d.

Egy gyakorlatban is jól működő kriptorendszernek a következőket is teljesíteni kell:

– Az E_e kódoló függvény kiszámítása „könnyű” legyen: szakmai terminológiával: polinomiális (gyakorlatban: lineáris vagy kis kitevőjű polinomiális) időben kiszámítható legyen.

– Hasonlóképpen könnyű legyen a nyílt szövegből a titkosított szöveg kiszámítása is.

– A D_d dekódoló függvény kiszámítása a *d* titkos kulcs ismeret nélkül „nehéz” legyen: szakmai terminológiával exponenciális vagy nagy kitevőjű polinomiális időben kiszámítható legyen. Az olyan függvényt, melynek értékét könnyű, de inverzét nehéz kiszámítani *egyirányú függvénynek* (one way function) nevezzük. Jelenleg matematikai eszközökkel egzaktul bizonyítható módon nem tudjuk, hogy létezik-e egyirányú függvény. Vannak azonban a gyakorlatban jól bevált egyirányú függvény *jelöltek*.

– A kulcstér (a szóba jöhető/lehetséges kulcsok) számosságának megfelelően nagynak kell lennie. Ma az 1024 bitnél rövidebb kulcsok nem nevezhetők biztonságosnak. Ez esetben a kulcstér számossága 2^{1024}. Kisméretű kulcstér esetén ugyanis a titkosított üzenet az ún. teljes kipróbálás (exhaustive search) vagy más néven a nyers erő (brute force) módszerével visszafejthető: egyszerűen a szóba jöhető kulcsokkal szisztematikusan megpróbáljuk dekódolni a kódolt üzenetet mindaddig, amíg értelmes szöveget nem kapunk.

A kriptorendszerek számos szempont szerint csoportosíthatók. A gyakorlati alkalmazások szempontjából nagyon fontos a kódoló-dekódoló kulcsok viszonya szerinti megkülönböztetés. Eszerint beszélhetünk szimmetrikus vagy privát kulcsú konvencionális rendszerekről, illetve aszimmetrikus vagy nyilvános kulcsú kriptorendszerekről.

1. *Szimmetrikus kriptorendszer:* A kódoló k kulcs megegyezik a dekódoló d kulccsal $(k=d)$.

   Jellemzője: A közös kódoló-dekódoló kulcsot legalább két személy ismeri. Ezt a közös kulcsot egy biztonságos csatornán kell az érintett feleknek egymás között kicserélni. Ez a biztonságos kulcskiosztás (key distribution) vagy más néven kulcscsere (key exchange) problémája.

2. *Aszimmetrikus kriptorendszer*: A kódoló k kulcs *nem* egyezik meg a dekódoló d kulccsal $(k\neq d)$. A kódoló k kulcsot nyilvános, a dekódoló d kulcsot privát kulcsnak nevezik.

   Jellemzője: A k kódoló kulcs nyilvános lehet (mint egy telefonkönyvben a telefonszámok), csak a d dekódoló kulcsot kell titkosan megőrizni, azaz a kódoló kulcsot bárki megismerheti, míg a dekódoló kulcsot csak egy személy ismeri! Aszimmetrikus kriptorendszerben a kódoló-dekódoló függvények a következő jellemző viszonyban állnak egymással: az E_k kódoló függvény kiszámítása könnyű, de inverzét a D_d függvény d értékének ismerete nélkül *nehéz*, míg d ismeretében *könnyű* kiszámítani. Az ilyen E_k függvényeket *egyirányú csapóajtó függvényeknek* nevezzük (trap-door one-way function).

A kriptográfia elméleti alapjai

A kriptográfia több tudományterület alapvető ismereteit tételezi fel, illetve használja fel, így tisztában kell lenni matematikai és kriptográfiai fogalmakkal, kategóriákkal és módszerekkel:

Matematikai alapok

– Számelméleti alapfogalmak: prímszám; prímtényezőre bontás; oszthatóság; legnagyobb közös osztó, legkisebb közös többszörös; kongruencia; Euler-féle φ függvény; Euler kongruenciatétele; kis Fermat-tétel; elsőfokú kongruenciák megoldás; másodfokú kongruencák; kvadratikus maradék, kvadratikus nem maradék, Legendre-szimbólum;

- Euklideszi-algoritmus: két egész szám legnagyobb közös osztójának meghatározása;
- Kiterjesztett euklideszi algoritmus: két szám legnagyobb közös osztójának előállítása a két szám lineáris kombinációjaként.
- Kínai maradéktétel: több elsőfokú kongruencia együttes megoldása
- Intelligens hatványozás: hatványkifejezések értékének gyors meghatározására szolgáló algoritmus
- Moduláris aritmetika: maradékosztályok (maradékosztály-gyűrű); véges testek; számolás a moduláris aritmetikában (összeadás, szorzás); véges testek multiplikatív csoportja; rend, részcsoportok; moduloinverz fogalma, meghatározása a kiterjesztett euklideszi algoritmussal.
- Diszkrét logaritmus: a moduláris hatványozás egyik inverz művelete: az alap és a hatvány ismeretében a hatványkitevő meghatározása moduláris aritmetikában.
- Számítási bonyolultság elemei: az algoritmusok végrehajtáshoz szükséges idő és/vagy a számítógépes tárolókapacitás vizsgálata (becslése, meghatározása) a használt számítógépes rendszerektől függetlenül; konstans, lineáris, polinomiális, exponenciális bonyolultság.
- Véletlen és álvéletlen sorozatok; valódi véletlen sorozat; álvéletlen sorozat fogalma; statisztikai értelemben vett álvéletlen sorozat; kriptográfiailag erős álvéletlen sorozat.
- Prímtesztek: pozitív egész számok prímtulajdonságának valószínűsítésére, illetve megállapítására szolgáló algoritmusok (csak áttekintés).
- Faktorizációs eljárások: pozitív egész számok prímtényezőkre bontása (csak áttekintés).

Kriptográfiai protokollok

- Protokoll: előre meghatározott, egyértelmű lépések sorozatával definiált üzenetcsere-folyamat, amelyet kettő vagy több résztvevő között valósul meg valamely feladat közös végrehajtása céljából.
- Kriptográfiai protokoll: az algoritmikus védelem kriptográfiai eszközeit alkalmazó protokollok.
- Kriptográfiai protokoll – kriptográfiai algoritmus összefüggése.
- Protokollok leírásában szereplő személyek: Kriptográfiai protokollok leírásában az egyes résztvevőket jól meghatározott tulajdonságokkal rendelkező fiktív személyek:
  - Alice, Bob, Carol, Dave
  - Eve: lehallgató passzív betolakodó
  - Mallory: rosszindulatú aktív támadó
  - Trent abszolút megbízható döntőbíró
  - Walter: felügyelő, aki a többi résztvevőt segíti a protokoll végrehajtásában;
  - Peggy: bizonyító, aki a többieket szeretné meggyőzni valamiről;
  - Victor: verifikáló, aki ellenőrzi Peggy bizonyító eljárását
- Biztonsági modellek: direkt, hierarchikus és hálós biztonság.
- Protokollok csoportosítása működésük lényeges tulajdonságai alapján: döntőbírós, ítélkező és önműködő protokollok.
- Kommunikációs protokollok: kommunikáció szimmetrikus, nyilvános kulcsú kriptorendszer használatával, hibrid kommunikációs protokollok.
- Digitális aláírás és megvalósító protokolljai (hash függvény).
- További protokollok: kulcscsere; titok szétvágása; titok megosztása; átlátszó bizonyítás (zero knowledge proof); biztonságos választási rendszer; biztonságos közös számítások; digitális pénz.

További kriptográfiai témakörök

- Kriptográfiai algoritmusok: DES, IDEA, AES, RSA, DSA
- Az algoritmusok használati üzemmódjai: blokktitkosítás: elektronikus kódkönyv (ECB); blokkláncolás (CBC); titkosítás visszacsatolása (CFB); kimenet visszacsatolása (OFB), Folyamtitkosítás
- Nyilvános kulcsú infrastruktúra
- A kriptográfia-törvény lehetőségei, korlátai
- Társadalmi vonatkozások
- Informatikai rendszerek biztonsága, Informatikai Biztonsági Szabályzat
- Operációs rendszerek biztonsága
- Adatbázisok biztonsága
- Internetbiztonság: nyílt és zárt számítógépes hálózat; számítógépes alapfogalmak; tűzfalak; elektronikus üzlet; elektronikus levelezés biztonsága
- Smart kártyák

Hogyan?

A kriptográfia oktatását célszerű egy rövid történeti áttekintéssel kezdeni. Ez nemcsk a tárgy iránti érdeklődés felkeltését szolgálja, de lehetőséget nyújt arra is, hogy jól megválasztott példákon keresztül a hallgatók megismerjék a kriptográfia szemléletmódját, néhány jellemző sajátosságát.

A kriptográfia elméleti hátterének kimerítő tárgyalására gazdaságinformatika szakokon a szükséges matematikai ismeretek hiányában nem lehet szó. Az előzőekben vázolt elméleti témakörök a kriptográfia *gyakorlati alkalmazásának a megértését* segítik elő, amelyet a teljes oktatási folyamat során számos konkrét eszköz bemutatásával kell kiegészíteni. Tényleges kriptorendszerek használatának bemutatására kézenfekvő választás a PGP (Pretty Good Privacy). Ez a legismertebb és leggyakrabban használt freeware kriptorendszer, amelynek első változatát P. R. ZIMMERMANN készítette 1991-ben. Külön előny, hogy magyar nyelvű oktatási anyag is rendelkezésre áll. A titkosítási rendszerek információs folyamatainak a szemléltetésre két eszköz is szóba kerülhet az UML és az SDL [16, [21].

Az UML összetett rendszerek meghatározására, szemléltetésére, létrehozására és dokumentálására kifejlesztett egységes vizuális modellező nyelv. Elsősorban az objektumorientált szemléletre épülő szoftverfejlesztés elemzési és tervezési eszköze, de használható strukturált módszertannal készült modellek ábrázolására is. Az UML hangsúlyozottan modellező és nem vizuális programozási nyelv. Egy feladatról készült UML-modell a készülő számítógépes rendszer vázlatának, tervrajzának tekinthető. Az UML mint nyelv a problémamegoldásban együttműködő, ugyanakkor rendszerint eltérő ismeretekkel rendelkező szakemberek kommunikációs eszköze. Hasonló módon alkalmazható cégek, szoftverfejlesztés esetén például a megrendelő és a fejlesztő cég közötti információcsere eszközeként is [16].

Az SDL nyelvet (Specification and Description Language) az 1970-es években kezdték el kidolgozni távközlési rendszerek formális, matematikailag egzakt leírására. A nyelv első verzióját 1976-ban publikálta a CCITT Z.100 ajánlásában. Jelenleg a CCITT utódszervezete, az ITU (International Communication Union) fejleszti. Legutolsó változata az SDL-2000, amely teljes egészében objektumorientált nyelv. Az SDL a leírandó objektumot rendszernek, és mindazt, ami nem tartozik hozzá a rendszer környezetének tekinti. Az SDL szemlélete szerint a leírandó rendszer egymástól független kiterjesztett véges automatákból (az SDL szóhasználata szerint processzekből) áll, amelyek párhuzamosan működnek és egymással diszkrét jelekkel kommunikálnak. A kommunikáció lehetséges útvonalait csatornák és jelutak jelölik, amelyek FIFO-elven[7] működnek. A kommunikáció jelekkel történik. Minden processz egyetlen bemeneti sorral rendelkezik [21]. Az eszköz

[7] FIFO: First in First out, vagyis az először érkező jel kiszolgálása történik meg először, ez lesz az első kimenet is (a főszerkesztő megjegyzése).

sikerrel alkalmazható kriptográfiai rendszerek leírására, működésük szemléltetésére [3].

A kriptográfiai rendszerek megismeréséhez szükséges számítások végrehajtáshoz – különösen a nagy pontosságú számításokhoz, illetve a moduláris aritmetikához – ún. komputeralgebrai rendszerek javasolhatók, mint a Maple [6] vagy a Mathematica. Ezekkel a megoldásokkal, amelyek nélkülözhetetlenek a modern elméleti és alkalmazott tudományos kutatásokban, interaktív módon szimbolikus számítások végezhetők (például differenciálás, integrálás stb.). A Windows 2000-ben és a magasabb Windows-verziókban a kriptográfia számos eleme viszonylag könnyen hozzáférhető módon mutatható be [9]: a Windows alapértelmezett biztonsági protokollja, a Kerberos 5 titkosító fájlrendszer: nyilvános kulcsokra alapozott biztonsági rendszer (PKI), hitelesítő szervezetek (Certificate Authority, CA); intelligens kártyák használata (smart cards), valamint virtuális magánhálózat (VPN).

Hivatkozások

[1] Babai László: *Prímszámok és titkosírás*. Természet Világa. 1981/6. 250-253. o.

[2] Buchmann, Johannes A.: *Introduction to Cryptography*. Springer-Verlag, 2000.

[3] Csajbók, Zoltán: *SDL Modeling of Cryptographic Systems*. A Magyar Tudományos Akadémia Szabolcs-Szatmár-Bereg Megyei Tudományos Testülete Tudományos Ülésének Előadásai. Nyíregyháza, 2002. szeptember 28-29., I. kötet, pp. 263-268.

[4] Gárdonyi Géza: *Titkosnapló*. Szépirodalmi Könyvkiadó, Budapest, 1974.

[5] Györfi László – Győri Sándor – Vajda István: *Információ- és kódelmélet*. Typotex, 2000.

[6] Heck, André: *Bevezetés a Maple használatába*. Juhász Gyula Felsőoktatási Kiadó, Szeged, 1999.

[7] Kahn, D.: *The Codebreakers: The Story of Scret Writing*. New York: Macmillan Publishing Co., 1967.

[8] Ködmön József: *Kriptográfia*. ComputerBooks, Budapest, 1999/2000.

[9] McLean, Ian: *Windows 2000 biztonság*. Kiskapu Kft., Budapest, 2001.

[10] Nemetz Tibor: *Matematika a kriptográfiában*: ízelítő. a Közgyűlési előadásokban – 2000. november. 175 éves a MTA I. kötet. MTA 2002. 187-207. o.

[11] Nemetz Tibor: *A Springer rejtjeles levele*. Matematikai lapok, Új sorozat 1. évfolyam (1991), 3. szám, 7-18. o.

[12] Nemetz Tibor – Szászné Simon Judit: *Hiányos szövegek rekonstruálhatósága és a magyar nyelv entrópiája*. Magyar Nyelv, 1989. 427-438. o.

[13] Nemetz Tibor – Vajda István: *Bevezetés az algoritmikus adatvédelembe*. Akadémiai Kiadó, 1991.

[14] Németh József: *Adatvédelem a számítógépes és hírközlő rendszerekben*. Számítástechnika-alkalmazási Vállalat, 1984.

[15] Pethő Attila: *Kriptográfia*. Balogh János és Kiss József által készített előadás jegyzet.

[16] Raffai Mária, Ph.D.: *Egységesített megoldások a fejlesztésben. UML modellező nyelv. RUP módszertan. UML referencia kártya*. Novadat Kiadó, 2001.

[17] Révay Zoltán: *Titkosírások. Fejezetek a rejtjelezés történetéből*. Lazy Könyvkiadó, Szeged, 2001.

[18] Schneier, Bruce: *Applied Cryptography. Protocols, Algorithms, and Source Code in C*. Second Edition.John Wiley & Sons, Inc., 1996.

[19] Shannon, C. E.: *Communication theory of secrecy systems*. Bell System Technical Journal, 28:656-715, Oct, 1949.

[20] Singh, Simon: *Kódkönyv. A rejtjelezés és rejtjelfejtés története*. Park Könyvkiadó, 2001.

[21] Törő Mária, dr.: *SDL – Specification and Description Language*. Alaklamazott Informatika Nyári Egyetem, 1993. MTA Szabolcs--Szatmár-Bereg m.-i TT Közlemények 4.