Kriptográfia

Első előadás
A kriptográfiáról általában

Dr. Németh L. Zoltán
SZTE, Számítástudomány Alapjai Tanszék
2008 ősz

Mi a kriptográfia?

Kriptográfia: a szó görög eredetű

(kriptos = eltitkolt, elrejtett + graphein= írni)

A 70-es évekig csak a üzenetek titkosításának módszereit értették alatta.

Mára jelentése kibővült:

Az információvédelem algoritmikus (nem fizikai, ügyviteli stb.) oldala

,, A kriptográfia azoknak a matematikai eljárásoknak, algoritmusoknak, biztonsági rendszabályoknak kutatását, alkalmazását jelenti, amelyek elsődleges célja az információnak illetéktelenek előli elrejtése."

/IT **biztonsági fogalomtár: ld.** www.fogalomtar.hu /

Kriptoanalízis, kriptológia

Kriptoanalízis: kriptográfiai rendszerek elemzése, és feltörésének kutatása.

/Hagyományosan a titkosított üzenet megfejtése a kulcs ismerete nélkül./

Kriptológia: kriptográfia + kriptoanalízis

Más besorolás szerint:

Kriptográfia : inform. védelmi alkalmazások

Kriptológia : az elmélet amin alapszik.

Információ biztonság

Az információnak illetéktelenek előli elrejtése jelenti az

- az információ titkos továbbítását
- az információ titkos tárolását

Védelmet kell biztosítani

- a megsemmisüléstől
- az eltulajdonítástól

Ez a két védelmi szempont egymással ellentétes:

egy példányban – sok példányban

tároljuk az adataikat?

Kriptográfia - szteganográfia

Szteganográfia(adatrejtés, data hiding)
,,A szteganográfia üzenetek elrejtése, tipikusan az üzenetnél nagyobb adathalmazban úgy, hogy az **üzenetátadás ténye is rejtve marad** a külső megfigyelő számára." /fogalomtár/

- láthatatlan tintával
- rabszolga fejbőrére írva *(hátránya meg kell várni, míg kinő a haja)*
- képben a színeket leíró bájtok alacsony helyiértékű bitjeiben *(szemre nem látható)*
- szórt spektrumú adásban
(fehér zajként észleli a külső megfigyelő)

Biztonsági célok / szolgáltatások (security services)

1. **bizalmasság** (confidentiality, privacy, secrecy)
   Csak azok érhessék el az információt, akik arra jogosultak.
2. **sértetlenség** (data integrity)
   Védelem az adatok jogosulatlan módosítása ellen pl. beszúrás, törlés, helyettesítés.
3. **hitelesség** (authenticity)
   - a kommunikáció szereplőinek hitelesítése (partner authentication)
   - az üzenetek hitelesítése (eredet, tartalom, küldési idő, stb., message authentication)
     /Ez implicit módon magába foglalja a sértetlenséget is:
     Ha az üzenet a küldőtől származik, nem módosíthatták./

Biztonsági célok / szolgáltatáson (security services) II

4. **letagadhatatlanság** (non-repudiation)
   Annak elérése, hogy valamelyik fél letagadhassa korábbi kötelezettségvállalását vagy cselekedetét, mert a letagadhatatlanság alkalmazásakor az ilyen vitákat egy megbízható harmadik fél (trusted third party) helyesen el tudja dönteni.
   Pl. "elektronikus aláírás = az üzenet hitelesítése + letagadhatatlansága"

A kriptográfia alapvető feladatai

- **rejtjelezés/megfejtés** (encryption/decryption)
- **elektronikus aláírások, időpecsétek** (digital signature, time stamp)
- **hitelesítés** (certification)
- **partnerazonosítás – identifikáció** (identification)
- **azonosító hitelesítése – autentikáció** (authentication)
- **jogosultságok kiosztása – autorizálás, tulajdonság birtoklás** (authorization, attribute ownership)
- **hozzáférés szabályozás** (access-control)
- **titokmegosztás, titokszétvágás** (secret sharing/spitting)

Alkalmazási területek

- **titkosított üzenetküldés** (encryption)
  ez a klasszikus kriptográfia
- **hozzáférés szabályozás** (acess control)
  pl. szoftverek, adatbázisok védelme,
  pay per view TV csatornák
- **banki tranzakciók**
- **elektronikus kereskedelem**
  vevő+bank+bolt, mindenki csak a rá tartozó információkat lássa
- **elektronikus pénztárca**
- **elektronikus szavazás** *(anonimitás is kell !)*
- **elektronikus publikáció**

"A kriptográfia önmagában nem védelem" (Virrasztó Tamás)

A kriptográfia csak a védelem algoritmikus oldala.

Nem tartoznak ide:

- az implementáció részletei
- az ügyviteli rendszabályok
- a fizikai védelem

stb.

A védelem erőssége mindig a leggyengébb láncszemen múlik. (Az emberi tényező?)

Szintén nem lesz szó ...

- általános üzemeltetési és biztonságtechnikáról
- kockázatelemzésről
- vírusvédelemről, tűzfalakról
- biztonsági résekről és kihasználásukról
- hackelési és crackelési technikákról

=> computer security, network security
(Persze ezek is használják a kriptográfiát.)

A kriptográfia rendszerek hierarchiája

- **kriptográfiai primitívek** (algoritmusok)
  - kulcsnélküli (egyirányú fgv, hash fgv., véletlenszám generátorok)
  - titkos kulcsú (egyirányú fgv, blokk- és folyamtitkosítók)
  - nyilvános kulcsú (PKI titkosítók, kulcsegyeztetők, aláíró alg.)
- **kriptográfiai sémák** (ezek vezérlik a primitívek összekapcsolását, azok kriptográfiai alkalmazásait)
- **kriptográfiai protokollok**

  = több résztvevős algoritmusok, melyben a a részvevők számításai és üzenetküldései egyértelműen meghatározottak.
- **kriptográfiai alkalmazások**
  (pl. a GSM kriptográfiai alrendszere, SET elektronikus fizetés védelmére kidolgozott rendszer)

Titkosítási alapfogalmak I

- **nyílt szöveg** (plaintext): az eredeti érthető üzenet, melyet védeni szeretnénk

- **titkosított (rejtjelezett) szöveg** (ciphertext): a titkosítással átalakított üzenet

- **kulcs** (key) a titkosításhoz/megfejtéshez használt kritikus információ.

  (A szimmetrikus kulcsú titkosítás biztonsága azon alapszik, hogy a kulcsot csak a feladó és a címzett ismeri).

Titkosítási alapfogalmak II

- **titkosítás** (enciphering, encryption): a nyílt szöveg "olvashatatlanná tétele" a kulcs segítségével.

  titkosító algoritmus (cipher)

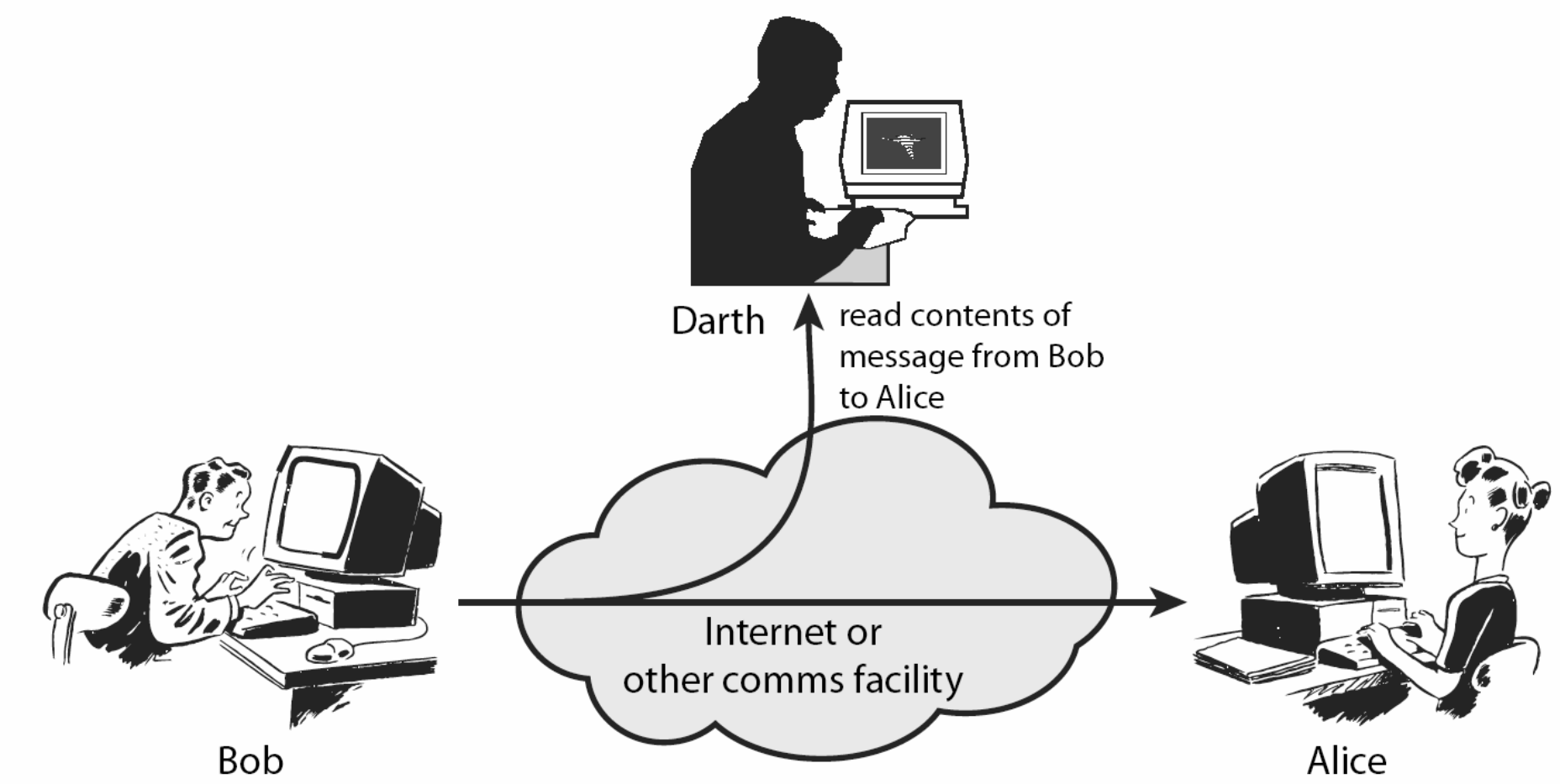
- **megfejtés** (deciphering, description): a títkosított szöveg visszaalakítása nyílt szöveggé a kulcs segítségével.

- **feltörés** (break): /első közelítésben/ a titkosított szövegből a nyílt szöveg rekonstruálása a kulcs ismerete nélkül (Részletesen lásd később a támadásfajták ismertetésénél.)

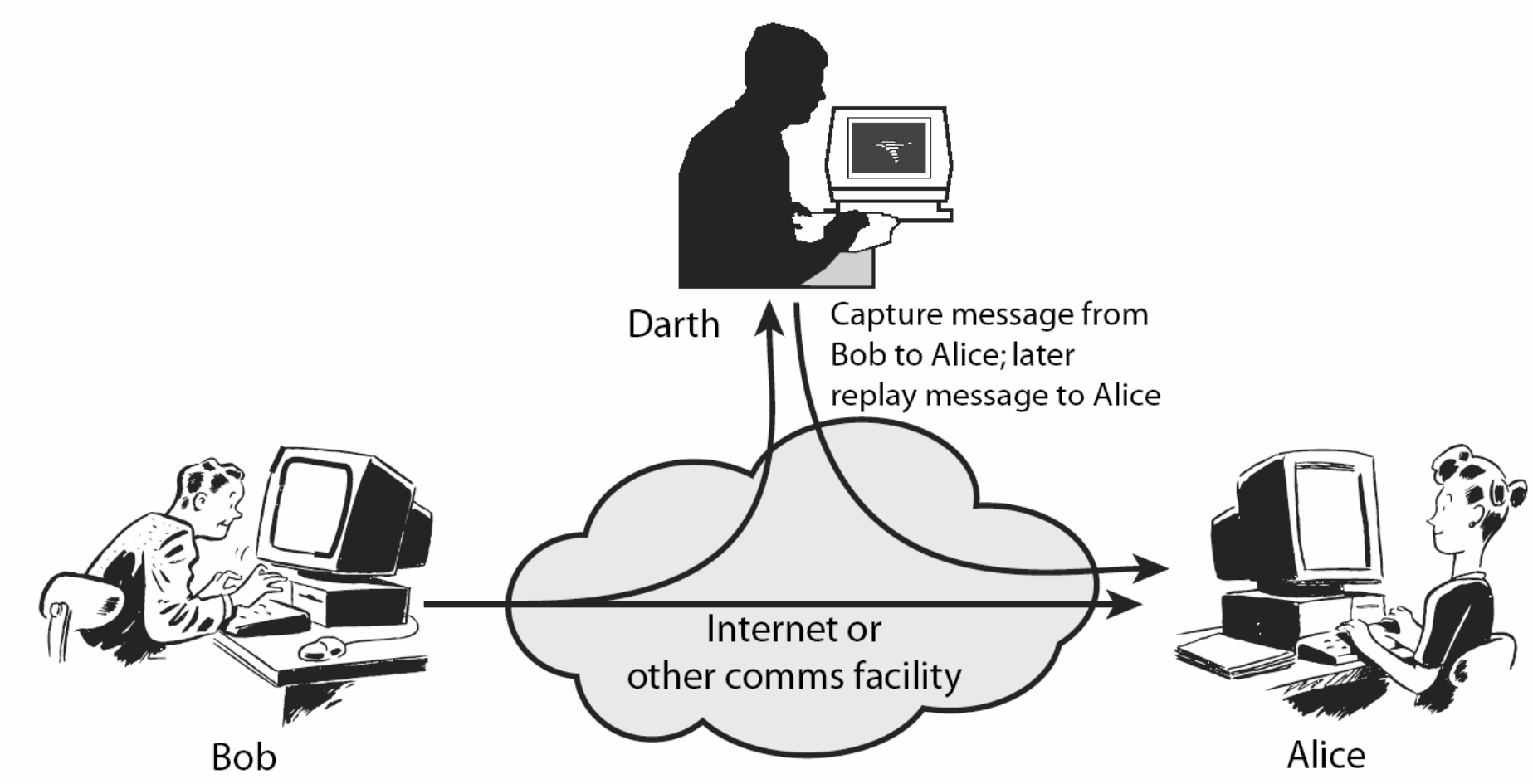
Résztvevők

- A: (Alíz, Alice) feladó (sender)
- B: (Bob, Béla) címzett (receiver)
  /estenként fordítva/
- C, D : (Carol, Dave)
  további kommunikáló felek
- E: (Éva, Eve) lehallgató (eavesdropper)
  /passív támadó/
- M: (Máté, Malory) aktív támadó (malicious active attacker)

Passzív támadás



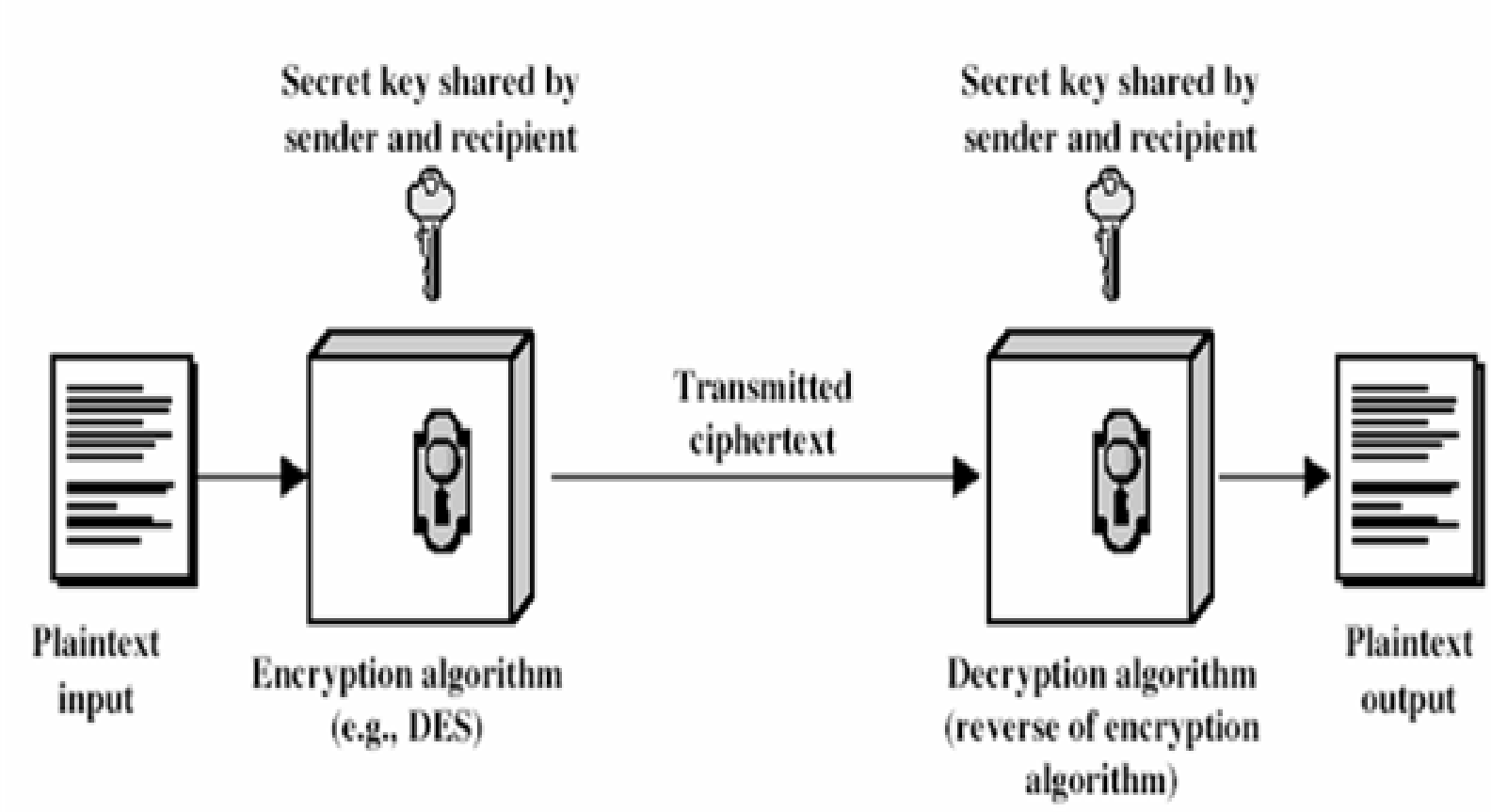
Aktív támadás



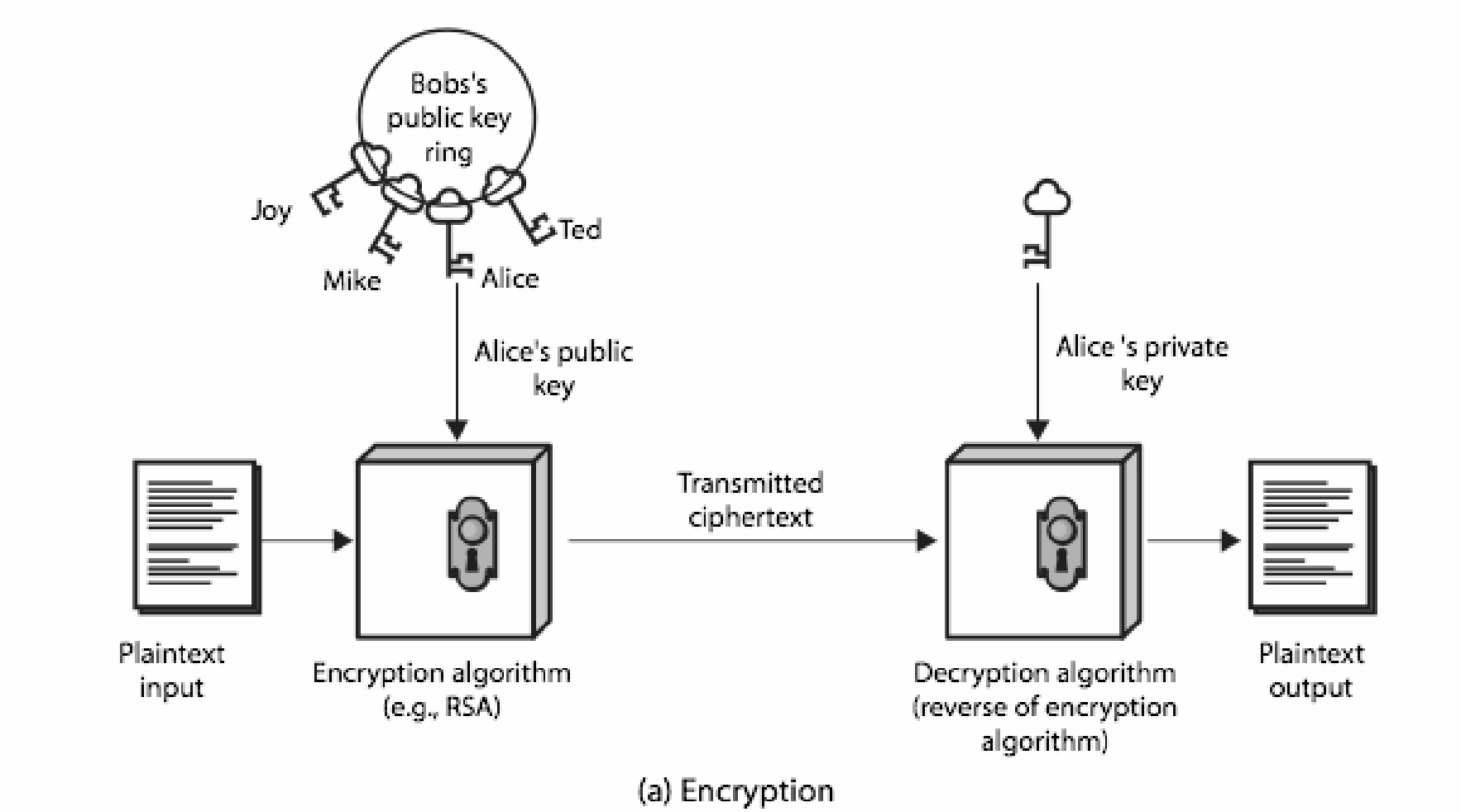
Titkosító rendszerek csoportosítása

- a kulcsok száma alapján:
  - szimmetrikus v. egykulcsú
  - aszimmetrikus v. két kulcsú v. nyilvános kulcsú
  - hibrid (a fenti kettőt ötvözi)
- a használt műveletek szerint
  - helyettesítő
  - keverő
  - produkciós (összetett v. kompozíciós)
- a nyílt szöveg feldolgozása szerint
  - blokktitkosítók
  - folyamtitkosítók

A szimmetrikus titkosítás modellje



A nyilvános kulcsú titkosítás modellje



Kriptoanalízis

- a cél a kulcs megtalálása, nem csak az üzenet megfejtése
- általános megközelítésben lehet:

  - **teljes kipróbálás**
    (exhaustive search, brute-force)
    az összes lehetséges kulcs kipróbálása
  - **kriptoanalízisen alapuló támadás**
    pl. betűgyakoriságra v. más statisztikai jellemzőkre támaszkodva

Kreckhoff követelmények

Auguste Kerchoffs von Nieuwelhof holland nyelvésztől (1883-ból!)

1. **Ha egy rendszer elméletileg nem feltörhetetlen, akkor a gyakorlatban legyen az**.

Egy rendszer

- *elméletileg biztonságos*, ha feltörésének valószínűsége független a támadó számítási kapacitásától és a támadásra szánt időtől.
- *gyakorlatilag biztonságos*, ha a feltöréséhez szükséges legjobb (ismert!) algoritmus idő vagy tárkorlátja annak alkalmazását lehetetlenné teszi.
- *nem biztonságos*, ha ismert feltöréséhez kielégítő tár és időkorlátos algoritmus.

A teljes kipróbálás lehetősége miatt legtöbbször csak a "gyakorlatilag biztonságos" szint elérésére törekedhetünk.

Kreckhoff követelmények II

2. A rendszer egy részének (tipikusan a használt titkosító algoritmusnak) a kompromittálódása (kitudódása), ne okozza a rendszer egészének kompromittálódását.

Azaz a biztonság **egyedül a kulcsnak**, és ne magának az algoritmusnak a titkosságán lapuljon.

Kriptoanalízisben feltesszük, hogy a támadó a rendszert ismeri. Mert:

- tömeges méretű alkalmazásoknál úgy sem lehetne az algoritmust titokban tartani
- az algoritmus az implementációkból visszafejthető
- a kriptográfia története mind ezt igazolja
- egy nyilvános, tesztelt módszer nagyobb bizalmat érdemel mint egy soha nem látott ,,szupertitkos”

Ez a Kerckhoff-elv.

Kreckhoff követelmények III

3. Az alkalmazott kulcsnak – feljegyzések nélkül – is könnyen megjegyezhetőnek és megváltoztathatónak kell lennie.
4. A titkosított szöveg táviratban is továbbítható legyen.
5. A titkosító rendszer legyen hordozható és egy személy által is üzemeltethető.
6. A rendszer legyen egyszerű, könnyen kezelhető, ne igényelje listányi szabályok betartását.

Kriptoanalízis

- a cél a kulcs megtalálása, nem csak az üzenet megfejtése
- általános megközelítésben lehet:

  - **teljes kipróbálás**
    (exhaustive search, brute-force)
    az összes lehetséges kulcs kipróbálása
  - **kriptoanalízisen alapuló támadás**
    pl. betűgyakoriságra v. más statisztikai jellemzőkre támaszkodva

Titkosítás elleni támadások

- csak titkosított szöveg alapú (cipertext only)
- ismert nyílt szöveg alapó (known plaintext)
- választott nyílt szöveg alapú (choosen plaintext)
- választott titkos szöveg alapú (choosen cipertext)

Kriptorendszerek értékelési szempontjai

- a titkosság mértéke (level of security)
- funkcionalitás (functionality)
- működési módok (modes of operation)
- teljesítmény (performance)
- a megvalósíthatóság könnyűsége (ease of implementation)

A biztonság fogalma

- **Feltétlen biztonság**

(unconditional security, perfect secrecy)

  - Függetlenül a rendelkezésre álló titkos szöveg mennyiségétől, időtől és számítási kapacitástól a titkosítás nem törhető fel, mert a titkosított szöveg a kulcs ismerete nélkül nem hordoz elég információt a nyílt szöveg rekonstruálásához. (Csak az egyszeri hozzáadásos módszer /one-time pad/ ilyen.)

- **Kalkulációs biztonság (computational security)**

  - Adott korlátos számítási kapacitás mellett (pl. a szükséges idő több mint az univerzum életkora) a titkosítás nem törhető fel a **ma ismert(!)** algoritmusokkal (pl. teljes kipróbálással (Brute Force), vagy ismert faktorizációs algoritmussal)

Mennyire biztonságos?

A kriptográfiai algoritmus biztonsága függ

- a választott algoritmus erősségétől
- a kulcs hosszától

Jó algoritmus esetén a kulcshossz növelésével a biztonság növelhető.

Például ha egy algoritmus csak teljes kipróbálással (Brute Force) törhető, akkor plusz egy bit kétszeres biztonságnövelést jelent.

Mennyire biztonságos? II

- Alapkérdés: Mit, ki ellen, mennyi ideig kell védeni?

magántitok / üzleti titok / állam titok
szomszéd / vállalt / állambiztonsági szervek
10 perc / 1 év / 30 év

- A jövőbeli hardver fejlődés és a feltörő algoritmusok (pl. faktorizálásra) fejlődése jósolható.
- Bizonyos kockázat persze mindig marad.
- Azért ne lőjünk verébre ágyúval (a sebesség jelentősen lassulhat a biztonság pedig egy határon túl már kérdéses, hogy növelhető-e).
- Érdemes követni a kriptográfusok ajánlásait.

A teljes kipróbálás (brute force) a gyakorlatban megvalósíthatatlan lehet

- Számoljunk egy kicsit! 128 bites kulcs esetén
- 2^{128} =340 282 366 920 938 463 463 374 607 431 768 211 456 lehetőséget kell kipróbálni
- Ha másodpercenként milliárdszor milliárd, azaz 10^{18} kulcsot próbálunk is ki, az
- kb. 10^{13} évet igényel
- ami több mint az egész univerzum becsült életkora ($1.3 \cdot 10^{10}$ év)
- és egy 256 bites kulcs brute force feltörése ennél 2^{128}-szor több időbe kerül!
- fizikai korlátok miatt nagyon valószínűtlen, hogy a brute force ilyen kulcsméretek esetén kivitelezhető!

A hamis biztonság csapdája

- Ha egy magas kilátó tetején egy erősnek látszó, ám valójában korhadt korlát áll, akkor ott nagyobb veszélyben vagyunk, mintha nem lenne ott korlát.
- Ha a saját magunk által kitalált és/vagy implementált "szuper" titkosítást erősebbnek gondoljuk, mint amilyen az valójában, akkor szintén veszélyes tévedésben élünk.
- A kriptográfia nem kezdő programozók játékterepe.
- Válasszunk inkább megbízható implementáci-ókat, *cryptoAPI*-kat. /pl. CAPICOM.DLL/

Bizalmasság ↔ biztonság ?

Tény: A kriptográfia ellenséges hatalmak, bűnözők, terroristák, crackerek stb. kezében veszélyt jelent.

Erre hivatkozva a hatóságok (főleg USA) korlátozták

- a maximális kulcshosszt (pl. szimmetrikusnál 40 bit)
- a kriptográfiai termékek exportját

Illetve kikötötték, hogy csak az exportálhat titkosító technológiát, aki a kulcsokat letétbe helyezte az államnál (key escrow)
Pl. 1993: Clipper chip minden chip egyedi kulcsáról volt egy "biztonsági" másolat az államnál.

Bizalmasság ↔ biztonság ? II

Polgárjogi mozgalmak a ,,Nagy testvér érzés" ellen.

A privát kommunikációt védi az alkotmány is
=> Erős kriptográfiát magánszemélyeknek is.

- 1991: Philip Zimmermann (Pretty Good Privacy, PGP) 128 bites kulcsokkal is !
- a fegyverexport törvény miatt három évig zaklatták
- 96-98 óta a korlátozások folyamatosan gyengültek
- ma már lehet 128 bites titkosítást is exportálni az USA-ból

Bizalmasság ↔ biztonság ? III

De ugyanez a helyzet "kicsiben" is:

Engedélyezik-e egy cégnél mindenkinek a titkosított levelezés használatát?

A központi vírusirtó, tűzfal, spam-szűrés működését (általában a tartalomfigyelést) ez lehetetlenné teszi.

A rendszergazda pedig felelős a biztonságért ...

A nyilvános kulcsunkat ezért ne adjuk oda mindenkinek.

Felhasznált irodalom

- Virrasztó Tamás: Titkosítás és adatrejtés: Biztonságos kommunikáció és algoritmikus adatvédelem, NetAcademia Kft., Budapest, 2004. Online elérhető: http://www.netacademia.net/book.aspx?id=1#
  (1. fejezet, 6.4, 6.5 és 14.1 függelék)
- Papp Pál, Szabó Tamás: A kriptográfiai biztonság megközelítési módjai, *Alk. Mat. Lapok*, **23**(2006) 207-294
- William Stallings: Cryptography and Network Security, 4th Edition, Prentice Hall, 2006. (Chapter 1)
- Lawrie Brown előadás fóliái (Chapter 1, Chapter 2)
- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone : Handbook of Applied Cryptography, CRC Press, 1996, online elérhető: http://www.cacr.math.uwaterloo.ca/hac/ (Chapter 1)
- **KIKERES Fogalomtár** 3.0 www.fogalomtar.hu