Titkosítás, kulcsok

Számítástechnika tanár szak
Rendszertechnika II.
előadás

A titkosítás alapfogalmai

- Titkosítás, kriptográfia
- Rejtjelezés (encryption, decryption)
- Titokmegosztás (secret sharing)
- Hitelesítés (certification)
- Partnerazonosítás (identification)
- Hozzáférésvédelem (access control)
- jogosultság vizsgálat (authentication)
- Digitális aláírás (digital signature)

Titkosítási modell

Küldő {
Nyílt szöveg (plaintext)
⇩ kulcs (key)
Titkosított szöveg
}

⇩ nyílt csatorna

{
Titkosított szöveg
⇩ kulcs (key)
Nyílt szöveg (plaintext)
} **Fogadó**

Klasszikus rejtjelezések

- Caesar-féle rejtjelezés

  plaintext: `aábcdeéfghijklmnoöpqrstuüvwxyz`
  ciphertext: `deéfghijklmnoöpqrstuüvwxyzaábc`
- k-eltolás
- Általános egyábécés rejtjelezés
- Keverő kódok
- Egyszer használatos bitminta, a feltörhetetlen

Számítógépes titkosítások

- Tendenciák napjainkban és régen
- Két alapvető kriptográfiai elv
  - Redundancia
    - Aktív támadások elleni védelem
    - Passzív támadások elleni védelem
  - Frissesség
    - Ismétléses támadások

DES - Digital Encryption Standard

- 1977-ben az IBM fejlesztette ki.
- Szimmetrikus kulcsú algoritmus
  - 56 bites kulccsal kódol
- Blokk-kódolás
  - 64 bites blokkokat - 64 bites blokkokká
- 19 különálló lépés
- Ma már nem tekinthető biztonságosnak

3DES - Háromszoros DES

- Titkosítás
  - Nyílt szöveg kódolása K1 kulccsal
  - Az előző eredmény dekódolása K2 kulccsal
  - Az előző eredmény kódolása ismét K1 kulccsal
- Visszafejtés
  - Kódolt szöveg dekódolása K1 kulccsal
  - Az előző eredmény kódolása K2 kulccsal
  - Az előző eredmény dekódolása K1 kulccsal
- Két kulcs használata három helyett?
- EDE (kódol - dekódol - kódol) algoritmus vagy EEE?

Blowfish

- Változó kulcshosszúság
  - maximum 448 bites kulcsokkal képes kódolni
- Blokk-kódolás
  - 64 bites blokkokat titkosít
- Működése
  - Kulcs kiterjesztési fázis (kulcstömb előállítása)
  - Titkosítás a kulcstömb alapján

Nyilvános kulcsú titkosítás

- Szimmetrikus kulcsok szétosztási problémája
- Nyilvános kulcsú titkosítás
  - Nyilvános kulcs (N)
  - Titkos kulcs (T)
  - Kódolandó információ (x)
- Diffie és Hellmann követelményei:
  - **T(N(x)) = x** (N(T(x)) = x)
  - T előállítása N alapján rendkívül nehézkes legyen
  - T feltörthetetlen legyen választott nyílt szöveggel

Diffie-Hellmann kulcscsere

- Kommunikációban Alíz és Bob vesz részt
- Alíz választ két nagy prímszámot n-t és g-t
- Mindketten előállítanak egy (n-1)-nél kisebb számot, hasonló nagyságrendben. Legyen Alíz száma x és Bob száma y
- Alíz elküldi (g^x mod n)-t és (n,g)-t
- Bob (g^y mod n)-t küld vissza
- Alíz kiszámolja K=(g^y mod n)^x értékét
- Bob kiszámolja K=(g^x mod n)^y értékét
- A közös titkos kulcs: K = g^{xy} mod n

- Ezt a módszert használják például az **SSL (Secure Socket Layer**) esetében is

RSA (Rivest, Shamir, Adleman)

- 28 éve túlél minden támadási kísérletet
- Legalább 1024 bites kulcsot igényel
- Az algoritmus lépései
  - Válasszunk két nagy prímszámot, *p*-t és *q*-t
  - Számoljuk ki az $n=p*q$ és $z=(p-1)*(q-1)$ számokat
  - Válasszunk egy *z*-hez relatív prímet, ez legyen *d*
  - Keressünk olyan *e* számot, melyre $e*d \equiv 1 \bmod z$

RSA

- A nyílt szöveg bitsorozatát blokkokra osztjuk
  - a kódolandó szegmens (*P*) ahol $0 \le P < n$
- Kiszámítjuk $C = P^e \pmod n$ értéket
- C visszakódolása: $P = C^d \pmod n$ alapján
- Kódoláshoz: *e* és *n* számok (nyilvános kulcs)
- Dekódoláshoz: *d* és *n* számok (titkos kulcs)
- A módszer biztonsága a nagy számok faktorizálásának nehézségeiből adódik

RSA példa

- p=3 és q=11
- n=p*q azaz n=33; z=(p-1)*(q-1) azaz z=20
- d=7 (7-nek és 20-nak nincs közös osztója)
- e*d≡1 mod z alapján e*7≡1 (mod 20) → e=3
- Kódolás: $C = P^3$ (mod 33)
- Dekódolás: $P = C^7$ (mod 33)
- A példában P értékének alacsonynak kell maradni (P<33) így maximum egy karakteres blokkok kódolhatók

RSA példa

Szimbólum	Számérték	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Szimbólum
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E

Tannenbaum: Számítógép hálózatok

Digitális aláírások

- Az aláírt üzenetnek a következő feltételeket kell teljesíteni:
  - A fogadó ellenőrizhesse a feladó valódiságát
  - A küldő később ne tagadhassa le az üzenet tartalmát
  - A fogadó saját maga ne rakhassa össze az üzenetet (ne változtathassa meg a tartalmát)

Titkosítási algoritmusok összehasonlítása

- A szimmetrikus algoritmusok előnyei
  - gyors
  - viszonylag rövid (56-256 bit)
  - más kriptográfiai feladatokra is alkalmazhatók
  - produkciós kódolók
- A szimmetrikus algoritmusok hátrányai
  - a kulcsnak mindkét oldalon titokban kell maradni
  - nagy hálózatokban nehézkesen alkalmazható
  - kulcscsere szükségessége egy biztonságos csatornán
  - a rövid kulcsokat gyakran kell cserélni

Titkosítási algoritmusok összehasonlítása

- Az aszimmetrikus algoritmusok előnyei
  - mindenkinek csak a saját titkos kulcsára kell vigyázni
  - nagy létszám esetén sem gond a kulcsok kezelése
  - a kulcsokat csak ritkán kell cserélni
  - a titkosító és megoldó folyamatok felcserélhetők
- Az aszimmetrikus algoritmusok hátrányai
  - általában lassú algoritmusok
  - lényegesen hosszabb kulcsok
  - szükséges egy megbízható harmadik fél
  - ha új matematikai áttörés születik, az sok kulcsot érinthet

Szteganográfia

- Nem csak az üzenet tartalma hanem annak létezése is titkos
- Az üzenetet más (az üzenet szempontjából lényegtelen) adatok közé keverjük
- Üzenetek képekbe rejtése
- Üzenetek zenékbe rejtése
- Hátránya, hogy sok felesleges információt is át kell vinni

Jelszavak

- Mikor „jó” egy jelszó?
  - A felhasználó képes megjegyezni
  - Felhasználónként különböző egy adott rendszerben
  - Megfelelő hosszúságú (min. 8 karakter)
  - Vegyesen tartalmaz kis- és nagybetűket, számokat
  - Önmagában ne legyen értelmes szó, dátum, stb.
  - Jelszavak cseréje meghatározott időközönként

Felhasználók jelszavainak védelme

- Ismételt, folyamatos próbálkozások elleni védelem
  - Néhány hibás próbálkozás után a próbálkozó kizárása egy meghatározott időre
  - Helytelen próbálkozások közti várakozási idő folyamatos növelése
  - A rendszer nem árulja el, hogy a felhasználó név érvénytelen-e vagy a jelszó hibás
- Fontos a felhasználók képzése