

SzSzN 2006

# Titkosítás alkalmazásai szabad szoftverek alatt

Faragó János  
<farago.janos@andrews.hu>

# Mire fel ez a nagy titkolózás?

- bizalmasság (confidentiality)
- sértetlenség (integrity)
- letagadhatatlanság (non-repudiation)
- azonosítás (authentication)

# Titkosítási eljárás erőssége

- algoritmus hatékonysága
- kulcs hossza
- a kulcs fizikai biztonsága (!)

# Titkosítási módok

- szimmetrikus titkosítás (pl. AES, 3DES)

$$E(x,k) \rightarrow y \dots D(y,k) \rightarrow x$$

- aszimmetrikus titkosítás (pl. RSA, DSA)

$$E(x,k1) \rightarrow y \dots D(y,k2) \rightarrow x$$

- hibrid titkosítás

# És hol a bizalom?

- tanúsítvány (certificate)
- certification authority (CA)
- registration authority (RA)
- Certificate Revocation List (CRL)
- Public Key Infrastructure (PKI)

# Ha már megvan a bizalom

- **Digitális aláírás (Digital Signature)**
- **Időpecsét (Time-Stamp)**

# Azonosítási módszerek

- tud valamit (jelszó)
- rendelkezik valamivel (csipkártya)
- valamilyen (ujjlenyomat, retina)
- két tényezős azonosítás

# Tevékenységek



# Átlag felhasználó

## Mit csinál?

- játszik
- kommunikál (levelezés, IM)
- le és feltölt (web, FTP, P2P)
- szórakozik (filmnézés, zenehallgatás)
- dokumentációt készít

# Átlag felhasználó

Hol találkozhat a kriptográfiával?

- belépés a rendszerbe
- HTTPS
- aláírt, titkosított levelezés
- titkosított adatok, fájlrendszerek
- különféle ellenőrző összegek

# Adminisztrátor

## ■ Mit csinál?

- telepít, konfigurál, karbantart
- hibát keres, szkripteket ír
- egyéb üzemeltetési munkákat végez

## ■ Hol találkozhat a kriptográfiával?

- PKI (részek)
- digitálisan aláírt programok, csomagok
- hibakeresés

# Fejlesztő

## ■ Mit csinál?

- tervezés
- fejlesztés
- követés

## ■ Hol találkozhat a kriptográfiával?

- protokollok, funkciók tervezése, fejlesztése
- tesztelés, hibakeresés
- csomagkészítés

# Alkalmazói programok

- webezés (Firefox)
- levelezés (Thunderbird, Evolution)
- dokumentáció kezelés (OpenOffice.org)

# Egyéb programok, megoldások

- vonali titkosítás (IPsec, SSL, PPTP, L2TP) - Linux kernel, OpenVPN
- csatorna titkosítás - OpenSSH, stunnel
- kiszolgálók (\*S) - apache, cyrus...
- svájci bicska - openssl
- fejlesztés - libcrypt, libssl

# Mi épül az openssl libekre?

apache2, bind9, courier, curl, cyrus, encfs, fetchmail, fwbuilder, heartbeat, heimdal, isakmpd, kerberos4kth, lighttpd, lprng, nessus, nmap, ntop, ntp, openssh, openswan, openvpn, postfix, postgresql, proftpd, pure-ftpd, qpopper, rdesktop, stunnel, tcpdump, vmware-player, w3m, wget, xchat, xmms...

SzSzN 2006

**Köszönöm a figyelmet.**

Faragó János  
<farago.janos@andrews.hu>

SzSzN 2006

# Titkosítás alkalmazásai szabad szoftverek alatt

Faragó János  
<farago.janos@andrews.hu>