Internet szolgáltatások, felhő alapú számítástechnika, adatvédelem

7. Előadás

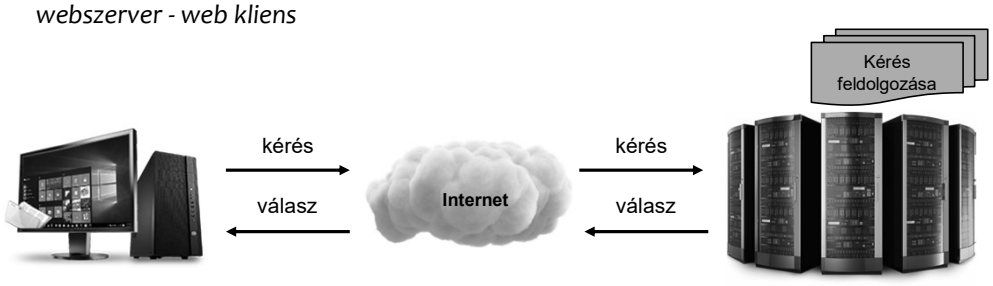
Tolnai József
Orvosi Fizikai és Orvosi Informatikai Intézet
2020.10.19

Internet szolgáltatások

Az internet szolgáltatások tipikusan szerver-kliens elven működnek

- **a kommunikációban résztvevő két fél nem egyenrangú** módon vesz részt
- dedikált szerepeket (szerver ill. kliens) töltenek be
- **a kliens kezdeményezi,** azért hogy valamilyen műveletet vagy lekérdezést végrehajtasson a szerverrel
- **a szerver a kérést feldolgozza,** majd **az eredményt a kliens felé továbbítja**

Pl. FTP szerver - FTP kliens
levelező szerver - levelező kliens
webszerver - web kliens



2

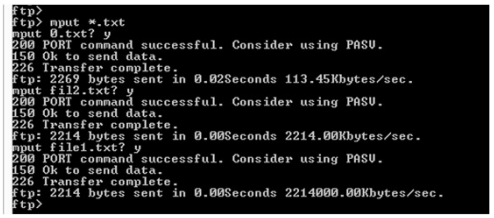
Internet szolgáltatások

Régi, alig vagy már egyáltalán nem használt szolgáltatások

- **levelezési listák:** azonos érdeklődésű emberek levelezési csoportja
- **hírcsoportok** (usenet)**:** egy erre dedikált szerveren gyűlnek az adott témába küldött levelek
- **Telnet** - távoli gépre történő bejelentkezés és munka
- **FTP** (File Transfer Protocol)**:** távoli gépek közötti állománycsere
- **Archie:** fájlkereső szolgáltatás → FTP
- **Finger:** információ hálózati felhasználókról
- **Talk:** kétirányú párbeszédes kapcsolat
- **IRC:** többcsatornás, többirányú chat
- **Gopher:** menürendszerű adatforrás-tallózó

Gyakran használt szolgáltatások

- **Elektronikus levelezés** (e-mail)
- **WWW** (1-2-3)

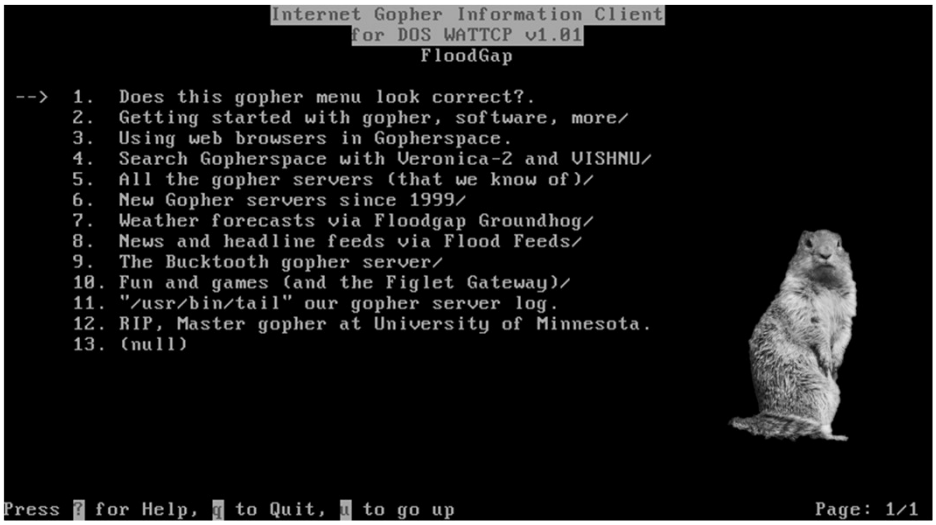


3

A régi **Archie** szerverek feladata az FTP szerverek fájladatbázisának leindexelése volt. Itt lehetett fájlnévre keresni. A találatok megmutatták, hogy az adott fájlokat milyen nyilvános FTP szerverről tudjuk letölteni, illetve azok pontosan milyen mappában találhatók.

Internet szolgáltatások

Gopher: karakter alapú, menürendszerű adatforrás-tallózó, a WWW elődje



gopher:// **ftp://**

4

A **Gopher** egy karakter alapú, menürendszerű adatforrás-tallózó és protokoll is egyben.

Karakteres menürendszerben lehetett elnavigálni a keresett információhoz, amit aztán akár le is tölthettünk. A WWW megjelenése előtt sokak által kedvel és használt internetszolgáltatás, amit a WWW elődjének tekintünk.

Saját protokollt használt az információ elérésére, amelyet a böngészők is támogatnak. A szokásos http:// protokoljelzés helyett ebben az esetbe a gopher:// taggal kell kezdenünk az URL megadását.

Elektronikus levelezés (e-mail)

- Előbb létezett, mint az internet (**1965**) , időosztásos (mainframe) nagy számítógép felhasználói közötti kommunikáció
- Szöveges üzenetek küldése különböző számítógépek felhasználói között (**1966**)
- Az @ jel elválasztja a felhasználó és a számítógép nevét (**1972**)
- Bármelyik felhasználó bármelyik másik felhasználónak küldhet levelet
- A címzett lehet a szomszéd szobában vagy a világ bármely pontján
- Nemcsak szöveges információt küldhetünk, hanem képet, hangot, mozgóképet, egyéb fájlokat.
- A címzettnek nem kell a gép előtt ülnie! (Postaláda!)

YAHOO! MAIL
Outlook
Gmail
Microsoft Outlook
Aol Mail.

Chuck Norris e-mail címe: gmail@chucknorris.com …

5

Elektronikus levelezés (e-mail) folyt.

e-mail cím: m.ede@med.u-szeged.hu (felhasználó@domain név)
e-mail cím tudakozó nincs!
Helyette: Postamester (postmaster@...)

@
- **at** (angol), hivatalos
- **kukac** (magyar)
- rózsa (török)
- disznófarok (dán)
- macskafarok (finn)
- éti csiga (francia)
- kacsa (görög)
- majomfarok (holland)
- rétes (izraeli)
- majom (lengyel)
- majomfarok (német)
- csavart alfa (norvég)
- csiga (olasz)
- kutya (orosz)
- sózott heringtekercs (cseh)
- kisegér (kínai)
- fahéjas tekercs, elefántfül (svéd)
- attu maaku (japán 'at')
- fi (arab 'at'), néha fül
- kismajom (szlovén)
- elefántormány (svéd)

- távíró kódja: • — — • — •

6

Elektronikus levelezés (e-mail) (folyt.)

fontos fogalmak
cc (carbon copy), bcc (blind carbon copy), folder (mappa), reply (válasz), forward (tovább küldés), address book (címlista), autoforward (automatikus továbbküldés), urgent message (sürgős üzenet), filtering rules (levelek szűrése), attachment (csatolt fájlok), signatures (aláírások), …

Smileok :) :(*(B-) :-.) (8-o)

karakteres képek

```
\////
(@ @)
---ooO-(_)-Ooo------
```

netiquette: hálózati etiquette
spam: kéretlen reklámlevelek
hoax: álhírt ill. egyéb beugratást tartalmazó levél
levélszemét

7

Hagyományos levélküldés - csigaposta (snail mail)

cc (carbon copy) – kik kapnak másolatot a levélből

bcc (blind carbon copy) – titkos másolat, az itt megadott címzettek is kapnak másolatot a levélből, de ezt a „sima" másolat kapók ezt nem látják

autoforward (automatikus továbbküldés) – előre megadott szabályok szerint a levelek továbbküldésre kerülnek, vagy minden levél egy adott címre lesz továbbítva automatikusan

signatures (aláírások) – Előre összeállított információs blokk, ami minden levél végéhez automatikusan hozzáfűződik

A **levélszemét** lehet minden olyan kéretlen üzenet, amelyet tömegesen küldenek (spam). Leggyakoribb formája a sok e-mail címre kiküldött üzleti.

A levélszemét küldése illegális. Védekezni ellenük levélszemét-szűrő megoldásokkal lehet, amely a komolyabb levelező szoftverekben be van építve.

Leggyakrabban botneteken (fertőzött zombihálózaton) keresztül terjesztik a kéretlen tartalmakat.

WWW (World Wide Web)
1989 (CERN)

Az egész világot behálózó, **hipertexten alapuló, osztott információs rendszer**, amely nem csak szövegeket, hanem képeket, mozgóképeket is tartalmaz

A **WWW** a grafikus lehetőségekre legjobban építő internet szolgáltatás

hipertext: szöveg, amelynek egyes pontjait, szavait kiválasztva egy másik szöveg(rész)hez jutunk - „nem szekvenciális írás" (1945)

HTTP (**Hypertext Transfer Protocol**): a hipertextek oldalak átvitelét leíró szabályrendszer

browser: tallózó, böngésző, pl. Mosaic (NCSA 1993), Netscape Navigator, Internet Explorer, Edge, Opera, FireFox, Safari, Chrome

URL (Uniform Resource Locator): egységes forrásazonosító
pl. *http://www2.szote.u-szeged.hu/dmi/index.php*
protokoll://domén/mappa/fájl[egyéb paraméterek]

plug-in: beszerkeszthető segédprogramok (Netscape 2.0)
pl. audió, animáció, videó lejátszás

Sir Timothy John Berners-Lee

8

CERN - Európai Nukleáris Kutatási Szervezet, Svájc, nagy hadronütköztető (LHC: Large Hadron Collider)

Web szerverek

Sir Timothy John Berners-Lee által a CERN-ben használt „web szerver” - 1989

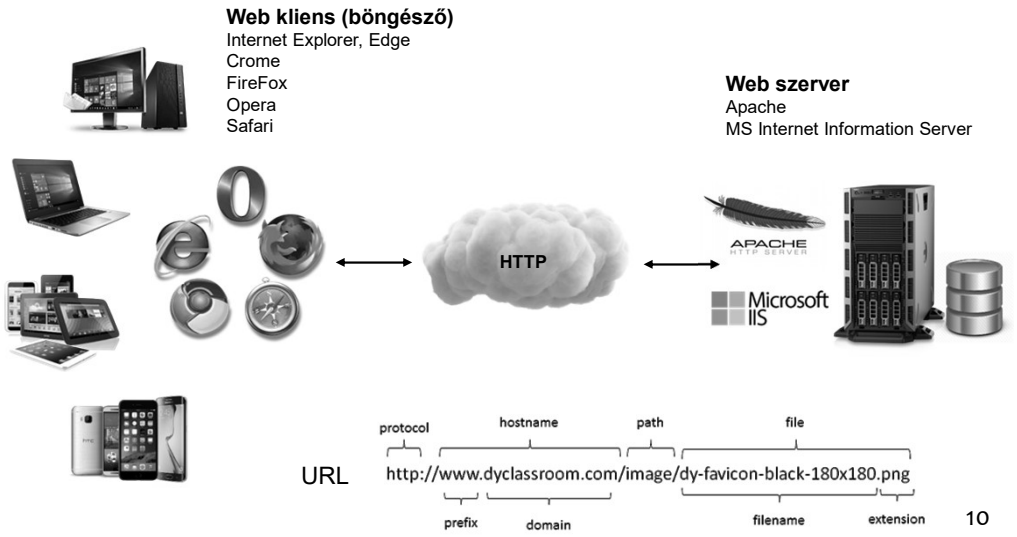
Szerverek a CERN adatközpontjában Worldwide LHC Computing Grid (WLCG)

9

Az első weboldal 1991. augusztus 6-án vált elérhetővé ...

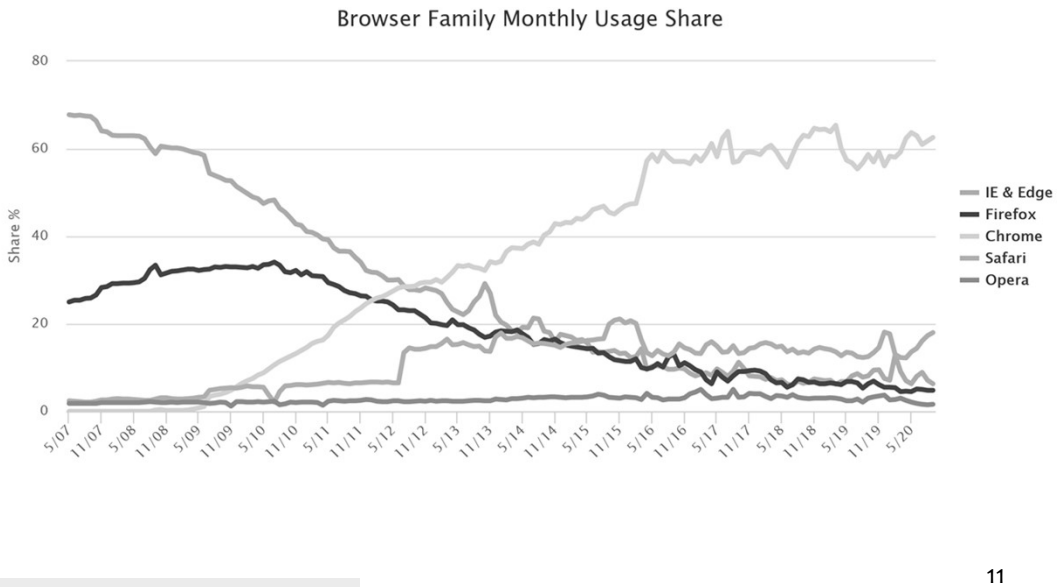
Web (http) szerver - kliens

A webböngészők a webszerverekkel HTTP (HyperText Transfer Protocol) protokollon keresztül kommunikálnak



10

Böngésző használati statisztika



11

http://www.w3counter.com/trends

- **Google (1998)**: keresőportál, térkép + több mint 20 szolgáltatás, **PageRank**
- **Bing (2009.06.01)**: Microsoft keresőportál
- **Facebook Search (2013)**: *Friends of my friends, Photos liked by me, Photos of [new zealand], restaurants, hotels, news, stb.*
- **Yahoo! (1994)**: „*juhéééé!*”, “*Yet Another Hierarchical Officious Oracle*”, első nyilvános e-mail-szolgáltatók egyike, 10 nyelven (pl. magyar), hierarchikus
- **Baidu (百度, 2000)**: kínai keresőportál, (weboldalak, zenei fájlok, képek)
- **Yandex (Яндекс, 1997)**: orosz keresőportál
- **Naver (네이버, 1999)**: dél-koreai keresőportál
- **DuckDuckGo (2008)**: felhasználók személyes adatainak a védelme, nincs személyre szabott keresés, mindenki ugyanazokat a találatokat kapja
- **Shenma (2014)**: kínai (Alibaba online áruház)

A felsorolásból kimaradt az **Ecosia** kereső, amely állítása szerint a keresések végrehajtásából keletkező bevételüket fák ültetésére fordítják.

A weboldal tanúsága szerint már több, mint 111 millió fa ültetését támogatták.

Keresők a weben (2018)

13

Web 1.0 vs 2.0

Web 1.0

- Hagyományos WWW szolgáltatás, a tartalmakat a szolgáltató nyújtja

Web 2.0

- internetes szolgáltatások, amelyek elsősorban a **közösségre épülnek**
- a **szolgáltatók csak a keretrendszert biztosítják**
- **a felhasználók közösen készítik a tartalmat** vagy megosztják egymás információit

Tipikus „webkettes" internet szolgáltatások:

- közösségi oldalak (Facebook, LinkedIn)
- képmegosztók (Instagram, Flickr)
- videómegosztó portálok (Youtube, Indavideo)
- blogok, mikroblogok (Twitter, Tumblr)
- aukciós oldalak (e-bay, Vatera)
- szabadon szerkeszthető ismerettárak (Wikipedia)

Web 3.0, szemantikus web (Tim Berners-Lee, 2001), különálló források egységes kezelése

14

Eduroam (Education Roaming)

- **Egy intézményi szövetség,** amely lehetővé teszi hallgatók és oktatók távoli hozzáférését a Campus erőforrásokhoz (*www.eduroam.org*)
- **A hozzáférés ellenőrzése az otthoni intézménynél történik** az eduroam együttműködés során kialakított **RADIUS hierarchia** segítségével
- A magyarországi RADIUS hierarchia legfelső szintjén az **NIIF** helyezkedik el, aki koordinálja és működteti ezt a szolgáltatást (**2006** eleje óta)
- Eredetileg európai kezdeményezésként indult

15

Az NIIF **2006** eleje óta tagja a nemzetközi eduroam szövetségnek

Eduroam eredetileg európai kezdményezésként indult, de ma már világ méretűvé vált.

Dolgok internetje (Internet of Things, IoT)

Jellemzők

- hálózatba kötött intelligens (okos) eszközök
- beépített szenzorokkal képesek adatot gyűjteni

Gyakorlati alkalmazás

- **okosotthon** (smart home, házban működő különböző rendszerek központi irányítása)
- **okos város** (smart city, döntéstámogató szolgáltatások a városi rendszerek pl. közművek, közlekedés, szolgáltatások, stb. működtetésében)
- **hálózatba kapcsolt autók** (automatikus forgalmi helyzet, segélyhívó, stb.)
- **ipari felhasználás** (Industrial Internet of Things, IIoT, pl. gyártás, szállítás)

Amazon Echo Family
Alexa, az Amazon hangsegédje

16

Apple Siri

Google Assistant

Felhő alapú számítástechnika

- **cloud computing**
- A **felhő alapú számítástechnika** a számítógépes erőforrások (hardver, szoftver) hálózaton keresztüli, szolgáltatásként való igénybevétele
- A szolgáltatásokat **nem** egy **dedikált hardvereszközön üzemeltetik**, hanem a szolgáltató eszközein elosztva, a szolgáltatás üzemeltetési részleteit a felhasználótól elrejtve

17

Felhő alapú számítástechnika, típusai

Szoftver szolgáltatás (*Software as a Service, SaaS*)
- Magát a szoftvert nyújtja szolgáltatásként, általában egy böngészőn keresztül. Pl. Google Docs, **Prezi**, Zoho Office, Microsoft Office Online

Platform szolgáltatás (*Platform as a Service, PaaS*)
- Az alkalmazás üzemeltetéséhez szükséges környezetet biztosítja Pl. Google App Engine, OpenShift, Microsoft Azure

Infrastruktúra szolgáltatás (*Infrastructure as a Service*)
- Virtuális hardvert (szervert, tárhelyet, hálózati kapcsolatot, számítási kapacitást) szolgáltat. Pl. Amazon EC2, Google Compute Engine

Tárhely szolgáltatás (*Storage as a Service*)
- A tárhelyet adja, mint szolgáltatást. Pl. Google Drive, Dropbox, Apple iCloud, Microsoft OneDrive, Amazon Cloud Drive

Hozzáférhetőség alapján: publikus, privát, hibrid felhő

18

Felhő alapú számítástechnika előnyei

Helyfüggetlen: bárhonnan könnyen elérhető

Méretezhető: növekvő vállalkozás → méretezhető a felhőszolgáltatás

Nagy rendelkezésre állás: a felhő alapú szolgáltatások mögött meghúzódó cégek folyamatos fejlesztése és komoly beruházásai a garancia arra, hogy a szolgáltatások megfelelő minőségben álljanak rendelkezésre

Költségkímélő: hardvereszközök megvásárlásának költsége helyett → a **szolgáltatás használatának díja** (pl. bérelt számítási kapacitás, hálózati forgalom, vagy felhasználók száma alapján kiszámolt összeg)
A **működtetési feladatok** nem a felhasználókat terhelik
Az **alkalmazások frissítésének** járulékos költségei is megtakaríthatók

Sky computing: A felhasználók sok egymástól izolált felhő szolgáltatást is igénybe vesznek

19

Köd alapú számítástechnika

Köd alapú számítástechnika esetében

- az adattárolók nem koncentráltan, hanem jóval szétszórtabban vannak elhelyezve, több kisebb adatközpont
- a hálózat elég **okos** ahhoz, hogy megkeresse a legközelebbit
- a felhasználó ebből továbbra sem lát semmit

20

Adatvédelem, adatbiztonság

Adatvédelem

Adatvédelem: az összegyűjtött adatvagyon sérthetetlenségét, integritását, használhatóságát és bizalmasságát lehetővé tevő technológiák és szervezési módszerek összessége.
Alapja **a felhasználók azonosítási** és **az információk hitelesítési** folyamatának kialakítása.

Eszközei

- **hardver védelme:** az eszköz elzárása, UPS, hűtés, tűzvédelem, hardverhibák, …
- **kommunikációs hálózat védelme:** hacker támadások, kémprogramok, vírusok elleni védelem (tűzfalak, privát hálózatok, vírusvédelem)
- **hozzáférések védelme:** jogosultsági szintek
- **az adatközlés, a kommunikáció titkosítása:** a közbülső szereplők se manipulálhassák az adatokat; jelszavas tömörítés, titkosítás, digitális aláírás…

22

Titkosítás

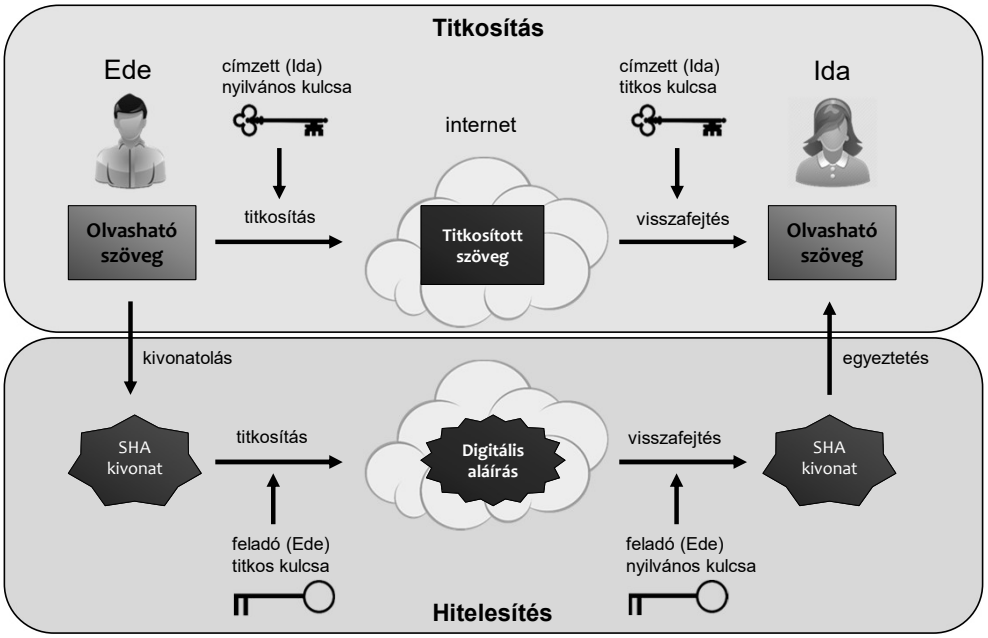
Nyilvános kulcsú titkosításnál minden felhasználóhoz két kulcs tartozik: egy **titkos**, és egy **nyilvános**. A két kulcs szerepe szimmetrikus.

Titkosítás: Minden felhasználónak generálnia kell egy **nyilvános/titkos kulcs párt**. A nyilvános kulcsot közzé lehet tenni, a titkos kulcsra értelemszerűen vigyázni kell.
Aki titkosított üzenetet akar küldeni, a fogadó nyilvános kulcsával kell kódolnia az üzenetet. A nyilvános kulcs ismerete nem segít abban, hogy a titkos kulcsot megfejtsük. **Ha egy üzenetet valaki nyilvános kulcsával kódoltunk, akkor már magunk sem tudjuk azt visszafejteni**, csakis a fogadó.

Hitelesítés: Ekkor a saját titkos kulcsunkat használjuk. Az **üzenetből képezünk**, egy az üzenetnél jóval rövidebb számot, amit az üzenet ellenőrző összege, (**ujjlenyomata**) Ezt a számot kódoljuk azután a saját titkos kulcsunkkal. A fogadó ezt csakis a mi nyilvános kulcsunkkal tudja kinyitni és így biztos lehet abban, hogy az üzenetet valóban mi küldtük.

23

Kétkulcsos titkosítás



24

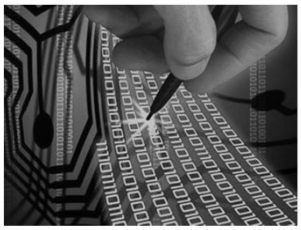
Digitális aláírás

elektronikus aláírás ≠ digitális aláírás

Az **elektronikus aláírás** minden olyan módszer, amellyel elektronikus dokumentumok "megjelölése", tágabb értelemben vett aláírása lehetséges
Pl. e-mail végén a nevünk, bedigitalizált kézzel írt aláírás, …
Nem biztonságos!!

A cél olyan elektronikus jelek biztosítása, melyek egy személyt vagy szervezetet hitelesen bizonyítanak.

A **digitális aláírás** a fentiekkel ellentétben olyan megoldás, ahol a végeredményként kapott **dokumentum aláírója, az aláírás ideje és helye, a dokumentum integritása** (tehát az, hogy azt illetéktelenül vagy véletlenül nem módosult) technikai szempontból igen **nagy biztonsággal bizonyítható**.
Pl. nyilvános kulcsú titkosítás



25

Amikor elektronikusan írunk alá egy dokumentumot, bonyolult kódolást végzünk el rajta. Az így létrejött aláírt, kódolt dokumentum olyan speciális szerkezettel rendelkezik, amelynek alapján bizonyítható, hogy ki volt az, aki a kódolást elvégezte, és az is bizonyítható, hogy az illető pontosan mely dokumentumot kódolta. (Így ha ugyanaz a személy több dokumentumot ír alá, **az egyes dokumentumokhoz tartozó aláírásainak különböznie kell egymástól**. Ha egy bűnöző átmásolja valakinek az elektronikus aláírását egy másik dokumentumra (amit az illető nem írt alá), kimutatható lesz, hogy az aláírás és ezen másik dokumentum nem tartoznak össze.)

A digitális tanúsítvány (digital certificate)

A nyilvános kulcsú titkosítási eljárások használatakor fontos, hogy a titkosított **üzenet küldése előtt** meggyőződjünk arról, hogy **valóban a címzett nyilvános kulcsát használjuk-e** (**hitelesítés**)

Az elektronikus tanúsítvány tartalmazza:

1. **Az adott személy/szervezet nyilvános kulcsát**; opcionálisan tartalmazhatja az adott személy/szervezet adatait (pl. nevét, lakhelyét vagy más adatait)
2. **Egy, vagy több digitális aláírást**, azoknak a szervezeteknek vagy személyeknek az aláírása, akik **igazolják a fentiek valódiságát**.

Ezek a szervezetek: **Hitelesítési Szolgáltatók** (Certification Authority, CA)

A hitelesítés szolgáltató létezését önmaga igazolja, egy önmaga számára kibocsátott tanúsítvánnyal: **főtanúsítvány**

26

Biztonság a weben

HTTPS (HTTP Secure)

- **biztonságos HTTP kapcsolat** (HTTP + SSL)
- a Netscape fejlesztette ki
- a webes kommunikáció titkosítható és autentikálható legyen
- biztonságilag kritikus kommunikációknál használják
  pl. fizetési tranzakciók, felhasználói jelszavas bejelentkezések
- alapja a kétkulcsos titkosítás
- nem önálló protokoll, **SSL** vagy **TLS** kapcsolat feletti HTTP kommunikáció

Transport Layer Security (TLS), Secure Sockets Layer (SSL)

Ellenőrző kérdések

1. Sorolj fel legalább 5 internet szolgáltatást!
2. Melyik internet szolgáltatás volt a WWW elődje?
3. Milyen elven működnek az internet szolgáltatások?
4. Mutass példát e-mail címre! Milyen részekre osztható az e-mail cím?
5. Mit jelent a hoax és a spam?
6. Mit jelentenek a következő kifejezések: WWW, hipertext, http, browser, plugin.
7. Sorolj fel legalább 5 böngészőt!
8. Mi a különbség a web 1.0 és a web 2.0 között?
9. Nevezz meg legalább 5 keresőportált!
10. Mit jelent a felhő alapú számítástechnika ?
11. A felhő alkalmazások 2 legfontosabb típusa?
12. Hogy működik a kétkulcsos titkosítás?
13. Mi a különbség az elektronikus és a digitális aláírás között?
14. Mit jelent a https?

28