Információbiztonság és Adatvédelem

2025/2026

László Ernő

Félév teljesítése

- **Évközi feladatok házi feladatok**
  - nem teljesítés esetén nem lehet vizsgázni

- Vizsga / ZH
  - Teszt feladat – elmélet (40%)
  - Gyakorlati feladat (60%)

Miről lesz szó

- **Információelmélet alapfogalmak** – Shannon, entropia, tömörítés
- **Klasszikus kriptográfia** – Caesar, Vigenère, Enigma
- **Hibajavítás és csatornamodellek** – Hamming-kód, Reed–Solomon
- **Modern kriptográfia** – AES, RSA, hash-ek, digitális aláírás
- **Hálózati biztonság** – SSL, TLS, VPN, MITM támadások
- **Adatvédelem, GDPR** – anonimizálás, nyomkövetés, metaadat
- **Támadások és védekezés** – brute force, phishing, ransomware, sql injection
- **Jövő és kutatási irányok** – kvantumkriptográfia, AI biztonság

Gyakorlati feladatok

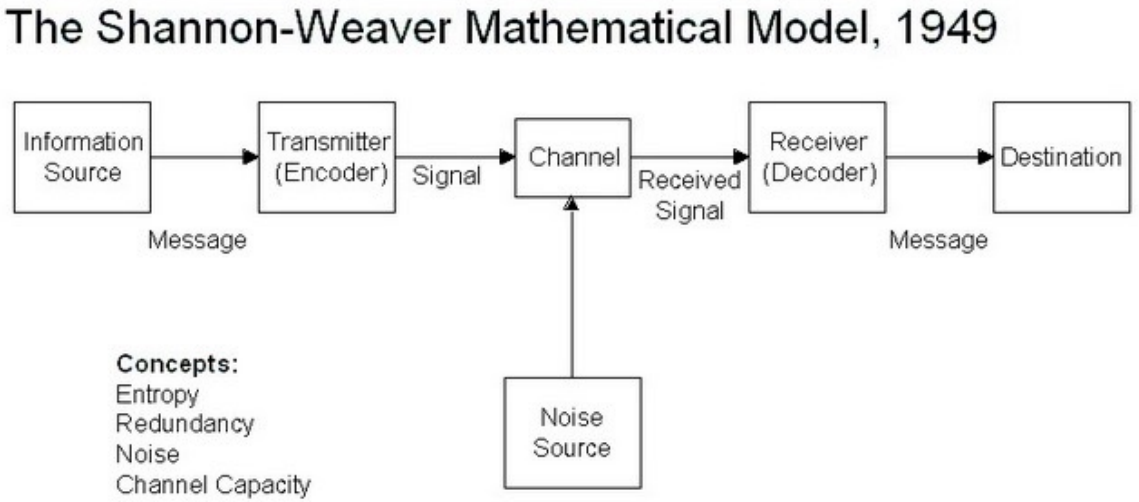
Információ

- **Információ = bizonytalanság csökkenése**.(Shannon) (https://hu.wikipedia.org/wiki/Shannon%E2%80%93Weaver-modell)

- Matematikai megközelítés

(mérhető)

  - Bit
  - Redundancia
  - Entrópia



Példák

- Holnap vizsga lesz!

Mekkora az információ tartalma?

- Minél kevésbé várt egy üzenet, annál több információt hordoz.

$$I(x) = -log_2(P(x))$$

- **I(x)** az x esemény információtartalma
- **P(x)** az esemény valószínűsége
  - Ha valami **valószínűtlen** (pl. 1/1000), akkor **sok bit** információt hordoz.
  - Ha valami **nagyon valószínű** (pl. 0.99), akkor **kevés bitet** (közel 0).

Példák

- Feldobott érme információ tartalma: 1 bit (-log2(0.5))
- Ha az érme mindig fejet mutatna akkor nincs információ tartalma mert nem közöl váratlant

Miért fontos ez?

- Pl kódolásnál Morsee kód . E a leggyakoribb betű ezért ez a legrövidebb mert a legkisebb az információ tartalma
- Q ritkább ezért hosszabb kód.

Esemény	Valószínűség	Információ (bit)	Megjegyzés
Napsütés nyáron	0.9	~0.15 bit	Nem sok új, várt esemény
Hóesés nyáron	0.01	~6.6 bit	Nagyon váratlan → sok információ
Érmefeldobás (fej/írás)	0.5	1 bit	Klasszikus példa
Új jelszó megadása	1/1,000,000	~20 bit	Ritka → magas információtartalom

Miért számít a biztonság?

- Ti hol tároltok jelszavakat?
- Törték már fel bármilyen online fiókodat?
- Mi baj származhat belőle?

Az információelmélet és az adatbiztonság kapcsolata

- Információelmélet: tömörítés, hatékony adatátvitel → **mit tudunk megspórolni?**
- Adatbiztonság: titkosítás, integritás, hitelesítés → **mit kell megvédeni?**
- A kettő közös alapja: **mintázatok felismerése és elrejtése**.

- Példa:
  - Tömörítés = a *mintázat* alapján eldobunk redundáns adatot (ZIP, JPEG)
  - Titkosítás = a *mintázat* elrejtése, hogy még az se értse meg, aki elfogja.

Adatszivárgás, adatlopás esetek (1)

– Enigma feltörése – mit okozott?

Év	Esemény
1918	Enigma-gép első változata (német fejlesztés)
1932	Lengyel matematikusok feltörik az Enigma egyszerűbb verzióját
1939	Turing csatlakozik a Bletchley Parkhoz (UK)
1940	Bombe gép működni kezd (Turing és Welchman)
1941	Daily kód feltörve – fordulópont
1945	Háború vége – a munka titkos marad évtizedekig

Adatszivárgás, adatlopás esetek (2)

- Enigma ismerttő: https://www.youtube.com/watch?v=G2_Q9FoD-oQ

- Titkosító eljárások kipróbálása: https://cryptii.com/pipes/enigma-machine

Adatlopás céljai (1)

- **1. Pénzügyi nyereségszerzés**
  - **Bankkártyaadatok** ellopása → közvetlen pénzlehívás, online vásárlás
  - **Ransomware**: fájlok titkosítása után váltságdíj követelése
  - **Adatok eladása** a dark weben (pl. jelszavak, email listák)
- **2. Kémkedés, hírszerzés**
  - Állami szintű kibertámadások → katonai, diplomáciai vagy gazdasági titkok megszerzése
  - Ipari kémkedés: versenytárs szellemi tulajdonának megszerzése
- **3. Profilalkotás és manipuláció**
  - Felhasználói szokások elemzése marketing vagy politikai célokra
  - Algoritmusok tanítása (AI modellek) ellopott adatokkal
  - Facebook / Cambridge Analytica → szavazók manipulálása

Adatlopás céljai (2)

- **4. Személyes zsarolás vagy bosszú**
  - Intim vagy kényes adatok kiszivárogtatása (pl. Ashley Madison hack)
  - „Doxing” – valaki személyes adatainak nyilvánosságra hozása
- **5. Szabotázs / rombolás**
  - Adatbázis törlés, módosítás → működésképtelenné tenni egy rendszert
  - Bizalom lerombolása (pl. nyilvánosságra hozott ügyféladatok)

Adatlopás által okozott károk

- **1. Gazdasági kár**
  - Váltságdíjak, bírságok (pl. GDPR → akár éves árbevétel 4%-a)
  - IT-rendszerek helyreállítási költsége
  - Ügyfelek elvesztése → bevételkiesés
- **2. Reputációs kár**
  - Ügyfelek, partnerek, befektetők **bizalmának elvesztése**
  - Negatív sajtómegjelenések → márka értékének csökkenése
  - Cégérték esése (pl. Yahoo felvásárlási ára is csökkent emiatt)
- **3. Személyes következmények**
  - Az érintett személyek:
    - elveszíthetik állásukat (pl. bizalmas e-mailek szivárgása)
    - pszichológiai terhelést élnek meg (megfélemlítés, stressz)
    - anyagi károkat szenvednek el (identitáslopás)

Adatlopás által okozott károk

- **4. Jogi következmények**
  - GDPR / adatvédelmi hatósági eljárás
  - Peres eljárások (kártérítési igények)
  - Hatósági vizsgálatok, törvényi felelősség
- **5. Szolgáltatás-kimaradás / leállás**
  - Adatlopás után a rendszer működése **leállhat** (pl. zsarolóvírus)
  - Kórházak, tömegközlekedés, közigazgatás működését is érintheti

Adatlopás által okozott károk

- **4. Jogi következmények**
  - GDPR / adatvédelmi hatósági eljárás
  - Peres eljárások (kártérítési igények)
  - Hatósági vizsgálatok, törvényi felelősség
- **5. Szolgáltatás-kimaradás / leállás**
  - Adatlopás után a rendszer működése **leállhat** (pl. zsarolóvírus)
  - Kórházak, tömegközlekedés, közigazgatás működését is érintheti

Adatszivárgás, adatlopás esetek

1. Feladat

Mindenki lehetőleg különböző adatszivárgás esetről írjon egy 1-2 oldalas ismertetőt.

- Mi történt?
- Mi volt a cél?
- Elkerülhető lett volna?
- Használták az információt?

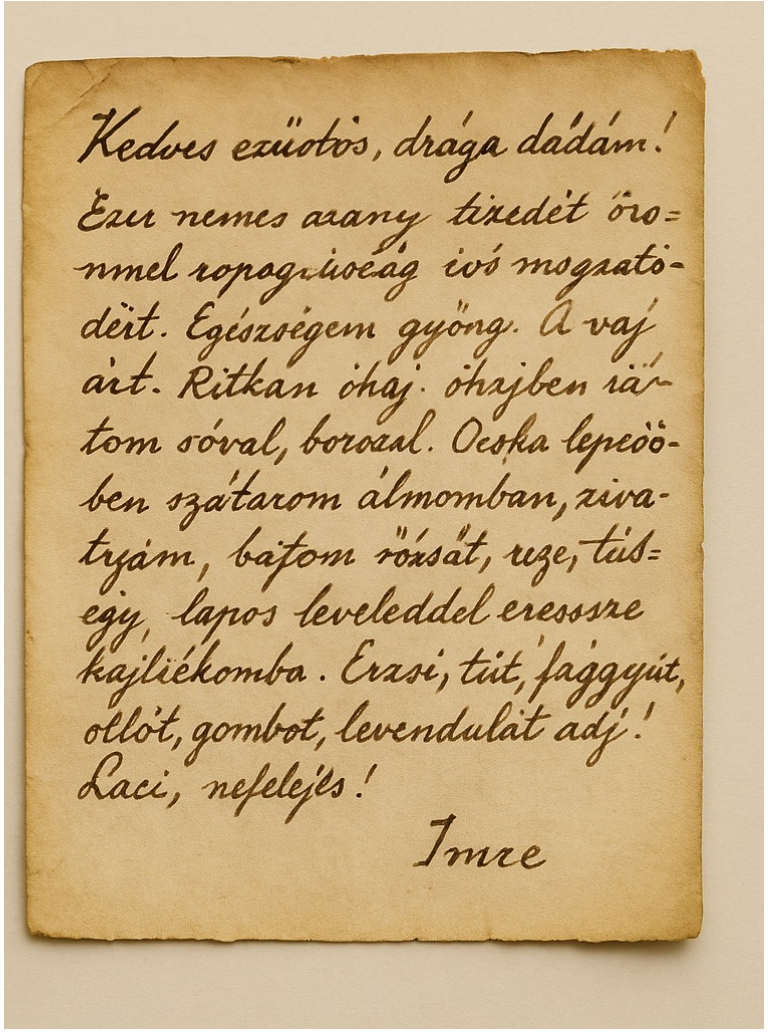
Szteganográfia

- Görög eredetű szó: *steganos* = fedett, *graphein* = írni
- Jelentése: információ elrejtése, nem csak titkosítása
- Cél: ne is derüljön ki, hogy üzenet van
- Kriptográfiával szemben nem a tartalom védelmét, hanem a **kommunikáció tényének** elrejtését célozza

Történelmi példák

- Hérodotosz: *viasztábla* (a viasz alá karcolt üzenet)
- Hisztiaiosz: rabszolga fejére tetovált titkos üzenet
- Láthatatlan tinta: citromlé, tej → meleg hatására válik láthatóvá
- Gárdonyi Géza: *Egy magyar rab levele* – akrosztichon (első betűk rejtik a valódi üzenetet)

Gárdonyi Géza – Egy rab levele


Kedves ezüstös, drága dádám!
Ezer nemes arany tizedét örömmel ropogtasdörök keserűség ivó magzatodért.
Egészségem gyöngy. A vaj ért. Ritkán óhajtomsóval, borssal. Ócska lepedőben szárítkozomálmomban, zivataros estén. Matyi bátyám, egypár rózsát, rezet, ezüstöt, libát egy lapos leveleddel eressze hajlékomba.
Erzsi, tűt, faggyút, ollót, gombot, levendulát adj!
Laci, nefelejts!
Imre

„Kedves ezüstös, drága dádém!
Ezer nemes arany tizedét örömmel ropogtasdörök keserűség ivó magzatodért.
Egészségem gyöngy. A vaj ért. Ritkán óhajtomsóval, borssal. Ócska lepedőben szárítkozomálmomban, zivataros estén. Matyi bátyám, egypár rózsát, rezet, ezüstöt, libát egy lapos leveleddel eressze hajlékomba.
Erzsi, tűt, faggyút, ollót, gombot, levendulát adj!
Laci, nefelejts!
Imre”

Gárdonyi Géza – Egy rab levele

„Kedves ezüstös, drága dádém!

Ezer nemes arany tizedét örömmel ropogtasd örök keserűség ivó magzatodért.

Egészségem gyöngy. A vaj árt. Ritkán óhajtom sóval, borssal. Ócska lepedőben szárítkozom álmomban, zivataros estén. Matyi bátyám, egypár rózsát, rezet, ezüstöt, libát egy lapos leveleddel eressze hajlékomba.

Erzsi, tűt, faggyút, ollót, gombot, levendulát adj!

Laci, nefelejts!

Imre”

Gárdonyi Géza – Egy rab levele

„Kedves ezüstös, drága dádém!

Ezer nemes arany tizedét örömmel ropogtasd örök keserűség ivó magzatodért.

Egészségem gyöngy. A vaj árt. Ritkán óhajtom sóval, borssal. Ócska lepedőben szárítkozom álmomban, zivataros estén. Matyi bátyám, egypár rózsát, rezet, ezüstöt, libát egy lapos leveleddel eressze hajlékomba.

Erzsi, tűt, faggyút, ollót, gombot, levendulát adj!

Laci, nefelejts!

Imre”

Kedden a török kimegy a városból. Száz emberrel el lehet foglalni.

Modern szteganográfia

- Digitális képek: pixelértékek legalacsonyabb bitjeiben rejthető adat (LSB)
- Hangfájlok: frekvenciák manipulálása az információ elrejtésére
- Videók, dokumentumok: metaadatok, fájlszerkezet használata
- Tipikus formátumok: PNG, WAV, MP4

Alkalmazási területek és kihívások

- Cenzúra megkerülése (diktatúrákban)
- Digitális vízjelek (pl. szerzői jogvédelem)
- Malware rejtése (kibertámadások)
- **Kihívások**: felismerés nehézsége, automatikus detektálás, ellenőrzés

- **Kriptográfiával** kombinálva hatékonyabb
- Szubliminális üzenetek - 25. képkocka
  - Éhes vagy!, Igyál kólát! => 58%-al nőtt a kóla és 18%-al a pattogatott kukorica eladása

Kriptográfia

- Ógörög eredetű: κρυπτός (kryptós) = „rejtett”, γράφειν (gráphein) = „írni”, tehát „titkosírás”
- Kriptográfia: információrejtés
- Kriptoanalízis: visszafejtés
- Kriptológia: kriptográfia + kriptoanalízis
- Állandó „harc”: rejtjelezők vs. kódfeltö

Kriptográfia célja

- **Titkosítás (Confidentiality)** – csak az olvassa, akinek szabad
- **Integritás (Integrity)** – ne lehessen észrevétlenül megváltoztatni
- **Hitelesítés (Authentication)** – tudjuk, ki küldte
- **Letagadhatatlanság (Non-repudiation)** – ne lehessen utólag letagadni

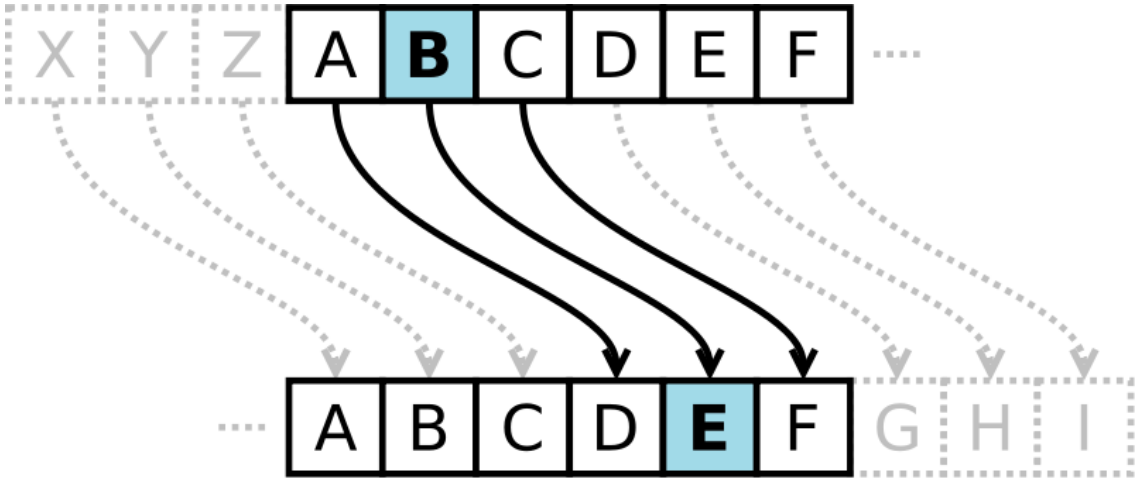
Klasszikus Kriptográfia

- **Példák:**
  - **Caesar-kód**: betűk eltolása egy fix kulccsal
    Pl. HELLO → KHOOR (3 pozícióval eltolva)
  - **Vigenère-kód**: kulcsszó alapján váltakozó eltolások
  - **Enigma-gép**: bonyolult rotoros mechanikus rendszer (WW2)
- könnyen megérthető, de könnyen feltörhető a mai technikával.

Klasszikus Kriptográfia

– **Caesar-kód**

Minden betűt kicserél egy,
az ABC-bentőle *k* távolságra
lévő betűvel



Általánosítva:

Minden betű helyett egy másikat használunk => bonyolultabb

26! Lehetőség

Ezt biztos nem lehet megfejteni, hiszen rengeteg párosítást kell végignézni… gondolták hosszú évszázadokig

Klasszikus Kriptográfia

Iszlám világ – Korán – több verzió – Mohamed szóban terjesztette később írták le

Arab tudósok vizsgálták mely részek származnak Mohamedtől és melyek nem.

Szavak előfordulását elemezték, majd a betűket is vizsgálták

Megszületett a **gyakoriságelemzés**

Klasszikus Kriptográfia

Smidla József tanár úr jegyzetei