

The background of the slide is a light green color with a complex network of thin green lines and small green dots, resembling a molecular structure or a data network, which is slightly out of focus.

# Információs rendszerek biztonságtechnikája

Bevezetés

*Vakulya Gergely*

# Követelmények

## 2 db ZH

- 6. hét (március 19.)
- 13. hét (május 7.)
- Kb. 60 perces feladatsor.
- Pótlási lehetőség: 14. hét (május 14.)

## Beszámoló

- Rövid prezentáció önállóan feldolgozott informatikai biztonsági témából

## Elmaradó órák

- Március 26. (kari tavaszi túra)
- Április 2. (rektori szünet)
- Április 9. (atomerőmű látogatás)

# Érintett témák

## Kriptográfia

- Szimmetrikus kulcsú algoritmusok
- Nyilvános kulcsú algoritmusok
- Üzenet pecsét algoritmusok
- Digitális aláírás
- Titkosított adattárolás
- Titkosított kommunikáció

## Sebezhetőségek

- Sebezhetőségek típusai
- Konkrét példák
- CVE adatbázis
- Védekezési lehetőségek

# A kriptográfia előzményei

- Motiváció
  - Üzenetek átvitele nem biztonságos csatornán
    - Kommunikáció háborús körülmények között
    - Magánjellegű kommunikáció (szerelmes levelek...)
  - Üzenetek elrejtése mindenki más elől
    - Titkos napló
- Megoldási lehetőségek
  - Lakattal lezárt tároló
  - Lepecsételt boríték
  - **Szteganográfia**

# Szteganográfia a kezdetekben

- Jelentése: leplezni (ógörög eredetű)
- Az információt nem rejtjelezzük, hanem elrejtik egy szokványos adathalmazban, amire senki sem figyel.
- Az adat elrejtése az adatban
- Az ókortól kezdve alkalmazzák

## Kínai módszer

A hírvivő lenyelte a gombócba gyúrt, viaszba mártott levelet.

## Rabszolga fejére írt szöveg

A rabszolga fejét kopaszta borotválták és arra írták a szöveget. Amikor a haja kinőtt, elküldték a címzetthez, ahol újra leborotválták a haját.

# Szteganográfia a kezdetekben

## Viasztáblás módszer

A viasztábláról lekaparták a viaszt és a csupasz deszkára vésték a szöveget. Ezután visszahelyezték a viaszt.

## Dupla levél

A hírvivő egy állevelet visz, de van nála (elrejtve, pl. lábbelibe varrva) egy másik levél is.

## Halhólyag

A felfújtt hólyagra írják az üzenetet, amit aztán leeresztenek. Elolvasáskor újra fel kell fújni.

## Láthatatlan tinta

A klasszikus módszer. Régóta ismertek hozzá megfelelő anyagok.

## Gárdonyi Géza: Egy magyar rab levele

„Kedves ezüstös, drága dádém! Ezer nemes arany tizedét  
örömmel ropogtasd örök keserűség keservét 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”

Próbáljuk meg megfejteni!

# Modern kori szteganográfia

Általában egy fájlban rejtene el egy másik fájlt.

## Camouflage

A Camouflage egy olyan program, amivel bármilyen fájlt például képfájlba, vagy Word dokumentumba lehet rejtteni. Zeneszámok terjesztésére használták.

## Kép a képben

Különböző megoldások, amikkel egy kép pixeleinek minimális módosításával rejthetőek el adatok. Inkább érdekesség.



# A kriptográfia múltja

## A szó eredete

- Szintén ógörög
- *kryptós*: rejtett
- *gráphein*: írni
- **titkosítás**

## Alapfogalmak

- Kriptográfia: információrejtés, rejtjelezés
- Kriptoanalízis: visszafejtés
- Kriptológia: Mind a kriptográfiát, mind a kriptoanalízist magában foglaló tudomány

## Spártai bórszój

- Egy bórszójat egy megadott átmérőjű hengerre tekerték fel.
- A henger alkotói mentén írták fel a szöveget.
- A letekert szíjon a betűk sorrendje összekeveredett.
- A dekódoláshoz egy azonos átmérőjű henger kellett.

## Caesar-kód

- Minden betű helyett az ABC-ben 3-mal odébb levő betűt írták.
- Általánosított Caesar-kód: 3 helyett  $k$  hellyel odébb csúsztatták az ABC-t.

# Egyéb módszerek

## Rejtjel-rács

- Egy négyzet alakú rácsot használnak, amin kivágások vannak.
- A kilátszó betűket kell felülről lefelé olvasni.

## Egybetű-helyettesítés

- Minden betűt egy másiknak feleltetnek meg az ABC-ben.
- A Caesar-kód egy speciális Egybetű-helyettesítés.

## Kódkönyv

- Az elküldött számok egy könyv oldalainak, szavainak felelnek meg.

## Egybetű-helyettesítéses kódolók

- Egy  $n$  betűs ABC esetében  $n!$  féle egybetű-helyettesítés készíthető.
- A nyers erő módszerével a próbálkozás elvileg reménytelen.
- Megoldás: A természetes nyelvek statisztikai tulajdonságai. Gyakoriság-elemzés. Betűpárok, betűhármak keresése.

## Próbáljuk meg megfejteni

í iak üökoíhaúú pu ub í iak pmvbnwom í euibg ibíodwíh í iak őídkk  
íz akmo hézemkmp b íz mpámr iakcí m hézeab píví