KRIPTOGRÁFIA 1.

IT hálózat biztonság

Tibi V 2020

Titkosítás tudományok

- **Szteganográfia** – az üzenet elrejtése (pl.: láthatatlan tinta, viaszos palatábla stb.)
- **Kriptográfia** – az üzenet tartalmának az elrejtése (pl.: titkosírás, kódolás stb.)
  - Modern kriptográfia (katonai alkalmazás mellett megjelent a polgári felhasználában is).
  - Szabványosítás (1970-es évektől)

Szteganográfia

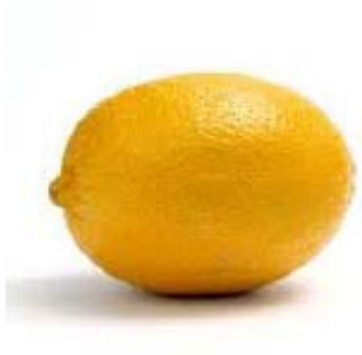
Szteganográfia (adatrejtés, data hiding):

az üzenetek elrejtése, tipikusan az üzenetnél nagyobb adathalmazban úgy, hogy az üzenetátadás ténye is rejtve marad a külső megfigyelő számára. (pl.: láthatatlan tinta, viaszos palatábla uv tinta, stb.)

A citromlével készített

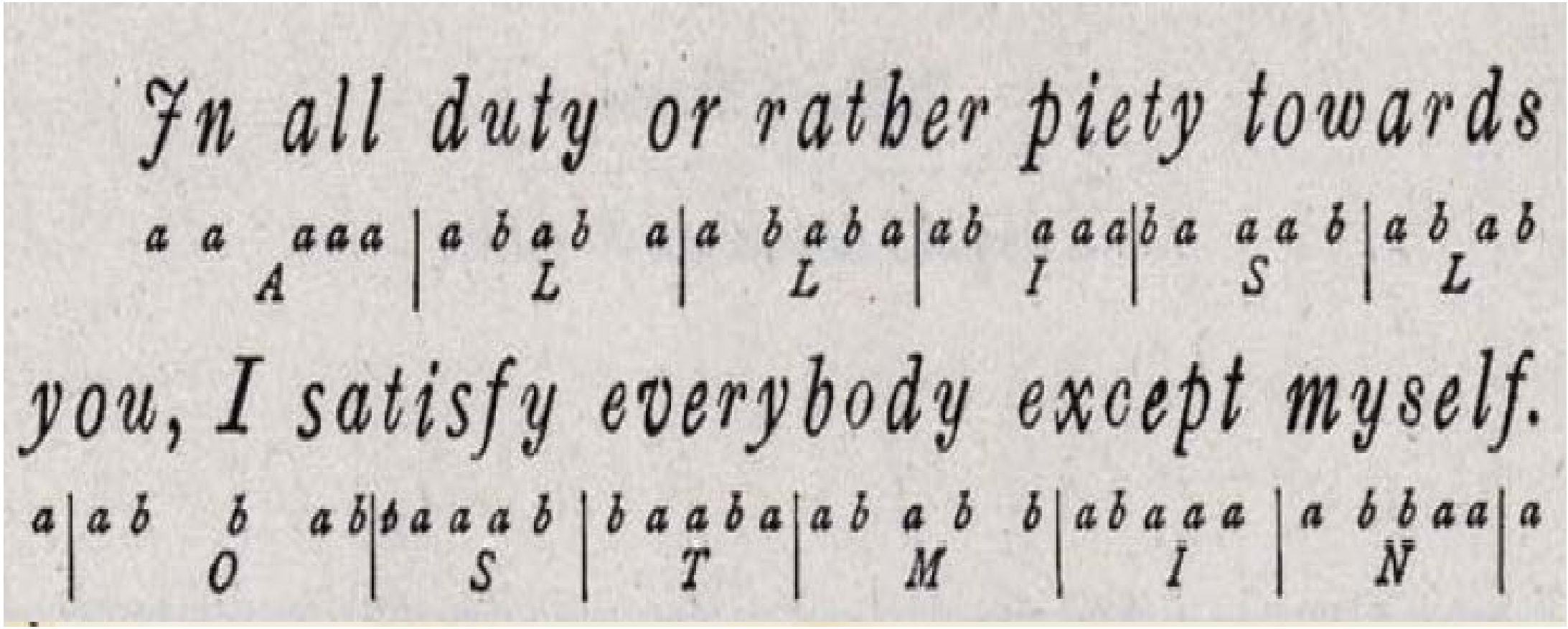
felirat hő hatására

válik olvashatóvá.



Francis Bacon (1561-1626) módszere

Az alacsonyabban fekvő betűk ‘a’ a megemeltek ‘b’ bináris jelet kódolnak.



Képekben …

- A színeket leíró bájtok alacsony helyiértékű bitjeiben (szabad szemmekl nem látható) rejtett információ.
- A baloldali képben a jobboldali van elrejtve.

Kriptográfia

Mi a Kriptográfia?

- Kriptográfia: a szó görög eredetű (kriptos = eltitkolt, elrejtett + graphein= írni)
- A 70-es évekig csak a üzenetek titkosításának módszereit értették alatta.
- Mára jelentése kibővült:

Az információvédelem algoritmikus (nem fizikai, ügyviteli) oldala.

,, A kriptográfia azoknak a matematikai eljárásoknak, algoritmusoknak, biztonsági rendszabályoknak kutatását, alkalmazását jelenti, amelyek elsődleges célja az információnak illetéktelenek előli elrejtése.”

Kriptográfiai alapfogalmak 1

- Nyílt szöveg (plain text): az eredeti, mindenki által értelmezhető információ
- Titkosított szöveg (ciphertext): a titkosított információ
- Titkosítás (encryption): eljárás, mely során az információt a birtokosa titkossá nyilvánít.
- Visszafejtés (decryption): a titkosított információból az eredeti visszaállítása.
- A titkosító algoritmus (cipher)

Kriptográfiai alapfogalmak 2

- Kulcs (key): az az információ, amelynek segítségével a rejtjelezés történik. (Két típus: nyilvános [publikus = public key] és titkos [privát = private key])
- Ábécé (alphabet): véges elemszámú halmaz, melynek elemei különböző szimbólumok (pl. 0,1).
- Feltörés (break):
  - /első közelítésben/ a titkosított szövegből a nyílt szöveg rekonstruálása a kulcs ismerete nélkül
  - /általánosabban/ a kulcs kiszámítása, akár a titkos és nyiltszöveg ismeretében
- Kriptoanalízis: a gyenge pontok felderítése.
- Kriptológia = kriptográfia + kriptoanalízis.

Kriptoanalízis

- **Kriptoanalízis:** kriptográfiai rendszerek elemzése, és feltörésének kutatása.
- Hagyományosan a titkosított üzenet megfejtése a kulcs ismerete nélkül.
- A cél a kulcs megtalálása, nem csak az üzenet megfejtése
- általános megközelítésben lehet:

  - teljes kipróbálás (exhaustive search, brute-force) az összes lehetséges kulcs kipróbálása

  - kriptoanalízisen alapuló támadás pl. betűgyakoriságra v. más statisztikai jellemzőkre támaszkodva

Kerckhoffs követelmények

Auguste Kerchoffs holland nyelvésztől (1883-ból!)

1**. Ha egy rendszer elméletileg nem feltörhetetlen, akkor a gyakorlatban legyen az**. Egy rendszer:

• elméletileg biztonságos, ha feltörésének valószínűsége független a támadó számítási kapacitásától és a támadásra szánt időtől.

• gyakorlatilag biztonságos, ha a feltöréséhez szükséges legjobb (ismert!) algoritmus idő vagy tárkorlátja annak alkalmazását lehetetlenné teszi.

• nem biztonságos, ha ismert feltöréséhez kielégítő tár és időkorlátos algoritmus.

2. **A rendszer egy részének (tipikusan a használt titkosító algoritmusnak) a kompromittálódása (kitudódása), ne okozza a rendszer egészének kompromittálódását.**

A biztonság fogalma

- **Feltétlen biztonság** (unconditional security, perfect secrecy)

– Függetlenül a rendelkezésre álló titkos szöveg mennyiségétől, időtől és számítási kapacitástól a titkosítás nem törhető fel, mert a titkosított szöveg a kulcs ismerete nélkül nem hordoz elég információt a nyílt szöveg rekonstruálásához. (Csak az egyszeri hozzáadásos módszer /one-time pad/ ilyen.)

- **Kalkulációs biztonság** (computational security)

– Adott korlátos számítási kapacitás mellett (pl. a szükséges idő több mint az univerzum életkora) a titkosítás nem törhető fel a ma ismert(!) algoritmusokkal (pl. teljes kipróbálással (Brute Force), vagy ismert faktorizációs algoritmussal.)

Mennyire biztonságos?

- A kriptográfiai algoritmus biztonsága függ
  - a választott algoritmus erősségétől
  - a kulcs hosszától
- Jó algoritmus esetén a kulcs hossz növelésével a biztonság növelhető.

Például, ha egy algoritmus csak teljes kipróbálással törhető, akkor plusz egy bit kétszeres biztonságnövelést jelent.

Alapkérdés: Mit, ki ellen, mennyi ideig kell védeni?

- magántitok / üzleti titok / állam titok
- szomszéd / vállalt / állambiztonsági szervek
- 10 perc / 1 év / 30 év

Kriptográfiai módszerek csoportosítása

1. Helyettesítés titkosítás:

- Monoalfabetikus
  - Egy abc-t használunk
- Polialfabetikus
  - Több abc-t használunk (kulcs)
- Poligrafikus
  - Ne betűket, hanem karaktercsoportokat cseréljünk.

2. Keverő (Permutációs) titkosítás

- Sor keverő
- Oszlop keverő
- Duplán keverő

3. Produkciós titkosítók

- Egykulcsos/szimmetrikus titkosítás
- Kétkulcsos/aszimmetrikus titkosítás

Teljes kipróbálás - Brute Force

- **mindig lehetséges az összes kulcskipróbálása**
- a legalapvetőbb támadás
- kulcstér (összes kulcsok halmaza)
- méretével arányos (ez exponenciálisan nő a kulcs hosszával!)
- feltételezi hogy a nyílt szöveg ismert vagy felismerhető megkülönböztethető az értelmetlen jelsorozatoktól)

A kriptográfia részterületei

- Titkos kulcsú (szimmetrikus) kriptográfia: egy kulcs van a titkosításhoz és a visszafejtéshez (pl. DES).
- Nyilvános kulcsú (aszimmetrikus) kriptográfia: két kulcsot használ, egyiket a rejtjelezéshez, másikat a visszafejtéshez (pl. RSA).
- Protokollok: az algoritmusok használatának a módja (pl. digitális aláírás, elektronikus kommunikáció)
- Technikák: a nyílt szöveg feldolgozásának módja (előre meghatározott hosszúságú blokkok kezelése).
- Egyéb alkalmazások: pl. felek azonosítása, hitelesítés, sértetlenség…

Szimmetrikus kriptográfia

- A kódoláshoz és a dekódoláshoz használt kulcs ugyanaz.
- Cél: algoritmus létrehozása a titkosításhoz.
- Lényeg: a titkos kulcs (a feltöréshez „csak” ezt kell kitalálni).
- Gyengeség: a kulcsot mindkét félnek ismerni kell az üzenetváltás előtt.
- Több kommunikációs csatorna esetén a sok kulcs kezelése komplikált.
- Feltörhetőség. DES: 56 bites. 128 bit esetén 2^{128} már elég jónak számít.

Aszimmetrikus kriptográfia

- 1976. – kétkulcsos rendszer (nyilvános, privát).
- Követelmény:
  - A kódolás és visszafejtés után teljes egészében álljon elő az eredeti üzenet.
  - A kódoló és a visszafejtő algoritmus és az azokban használt kulcsok egymástól függetlenek legyenek.
  - A kódolás feltörhetetlen legyen választott nyílt szöveg típusú támadással.
- Lényege: ha valaki titkos üzenetet szeretne fogadni, kialakít egy algoritmust és a hozzá tartozó nyilvános kulcsot, amit közzétesz. Ezzel bekódolt üzenetet a saját (titkos) kulcsával tudja megfejteni.