Bevezetés a számítástechnikába

Linux - 2

Siklósi Bálint

Pázmány Péter Katolikus Egyetem - Információs Technológiai és Bionikai Kar

siklosi.balint@itk.ppke.hu

2020. október 20-22.

Grep feladatok

- Töltsd le a következő fájlt: http://users.itk.ppke.hu/~sikba/bevtech_material/error_messages.txt
- Listázd ki az összes sort az error_messages.txt fájlban, ahol szerepel az "Error" szó.
- Írasd ki, hogy hányszor szerepel az "Error" szó! (Válasz: 3)
- Írasd ki, hogy hányszor szerepel az "ERROR", vagy "Error", vagy "error" szó! (Válasz: 13)
- Írd ki azokat a sorokat, ahol nem szerepel az "error" szó (kis és nagybetűtől függetlenül) (23 ilyen sor van)

Regex feladatok

- Írj regexet, ami illeszkedik a $a^n ba^m$ alakú sztingekre (pl. aaaba, baa, aba, aaaaab)
- Írj regexet, ami illeszkedik a mondatvégi pontra
- Írj regexet, ami illeszkedik az ITK-s email címekre
- Menj végig ezeken a példákon: https://regexone.com/

Extra feladatok

- Listázd ki az aktuális könyvtárban az alkönyvtárakat!
- Írj regexet a hárommal osztható binárisan reprezentált számokra!

Hasznosságok

- Kiírja az egész fájlt és kiszínezi a mintára illő szavakat:

```
less error_messages.txt | egrep -i --color=always "^|Error"
```

- Regex tesztelő: https://regexr.com/
- Regex gyakorló: https://regexone.com/
- Regex szórakozás :) https://regexcrossword.com/

Titkosítás (encryption)

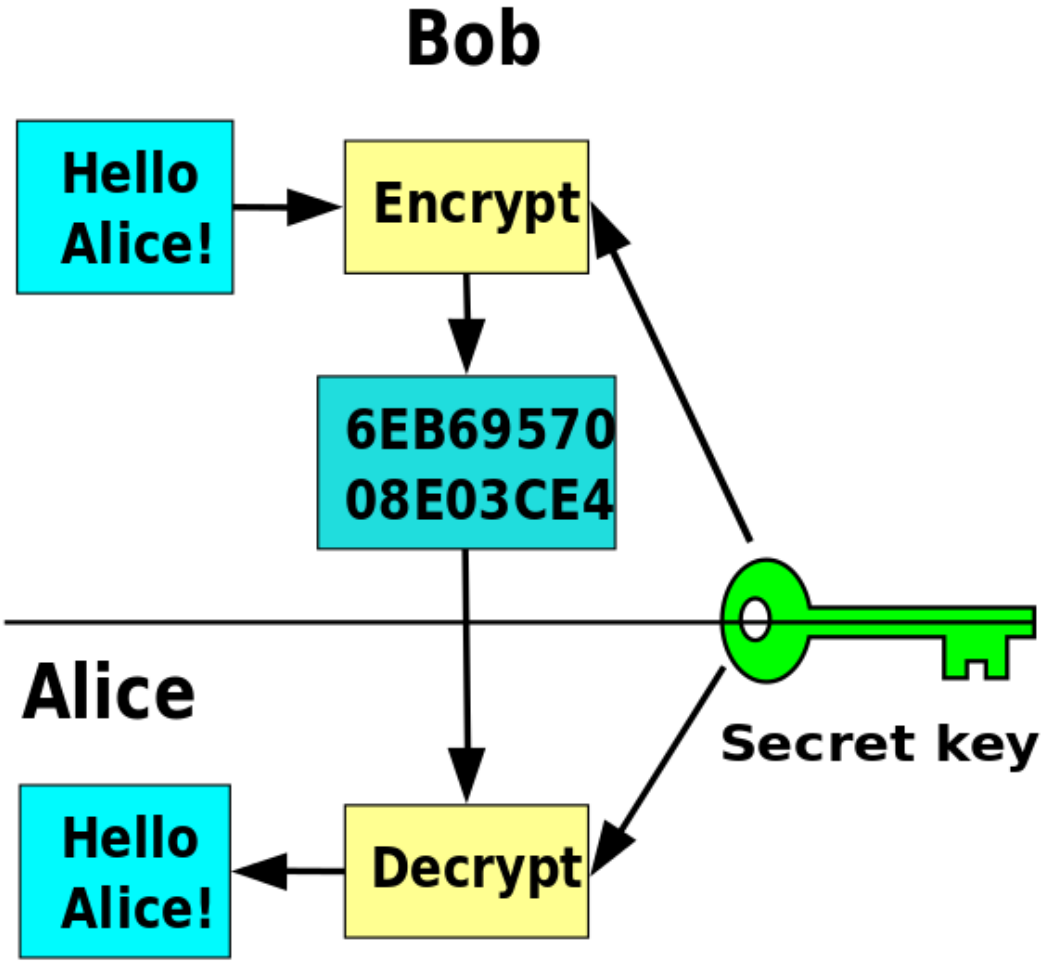
Problémafelvetés: az adatot csak egy kulcs birtokában lehessen elolvasni (visszafejteni)

Alkalmazás:

- HTTPS
- fájlrendszer titkosítása
- adatbázisok titkosítása

Szimmetrikus titkosítás

A kódolás és a visszafejtés ugyanazzal a kulccsal történik.



Szimmetrikus titkosítás

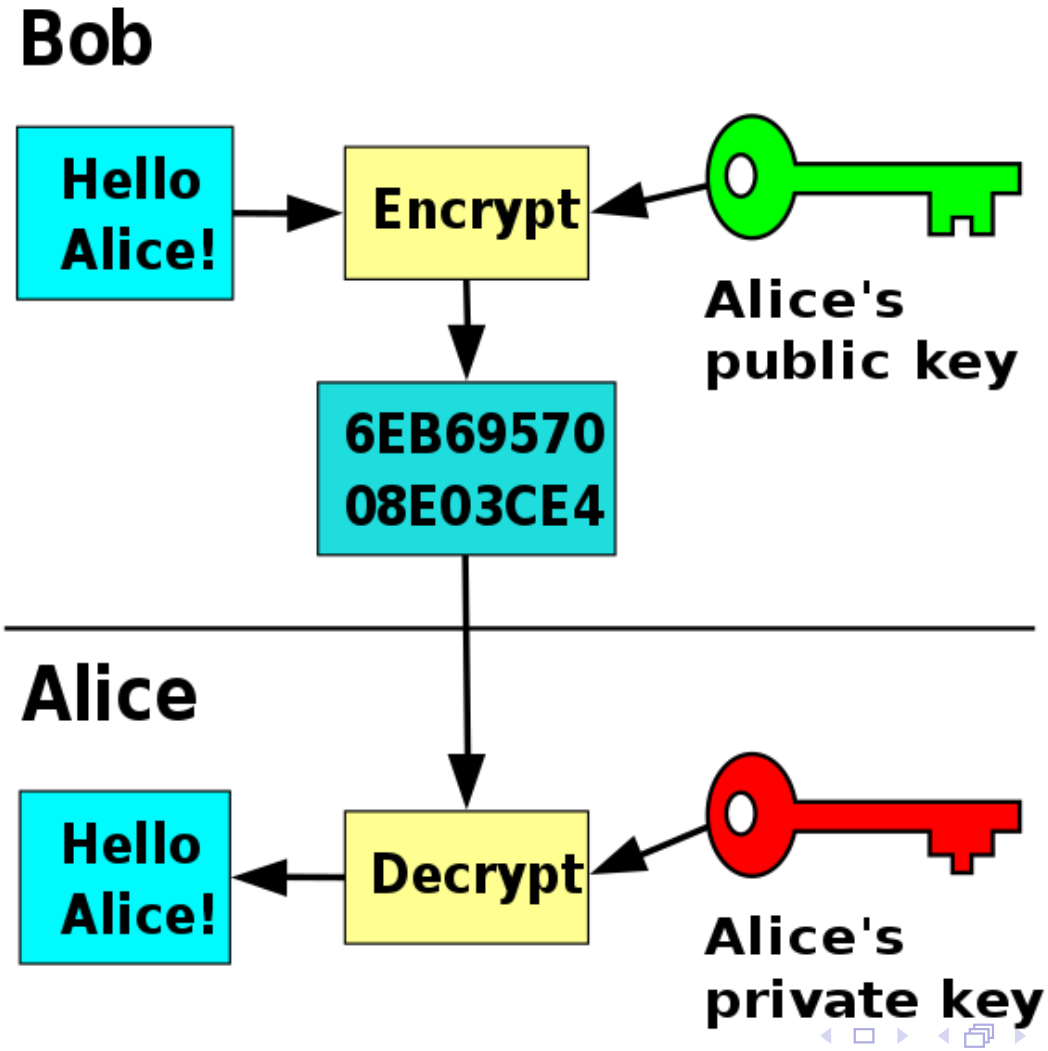
A kódolás és a visszafejtés ugyanazzal a kulccsal történik.

Példák:

- rotation cypher
  https://www.xarg.org/tools/caesar-cipher/
- one-time pad
- AES
  https://aesencryption.net/
- `gpg --symmetric -o cypher.gpg plain`

Asszimmetrikus titkosítás

Hogyan juttassuk el a kulcsot a címzettnek?



Asszimmetrikus titkosítás

Hogyan juttassuk el a kulcsot a címzettnek?

Trükk: kulcspár

- Az egyikkel kódolni, a másikkal visszafejteni lehet.
  - Nem lehet egy kódolt üzenetet a kódoláshoz használt kulccsal visszafejteni.
  - Egyik kulcsból sem lehet a másikat kiszámolni.
- Az elsőt mindenki publikussá teszi, a másodikat megtartja magának (privát kulcs).
- A címzett publikus kulcsával titkosítom az üzenetet
- A nekem címzetteket csak én tudom elolvasni, mert csak nekem van meg a privát kulcs.

Rivest-Shamir-Adleman

Ilyen például az RSA algoritmus,
amelynek matematikai háttere a prímfaktorizáció nehézsége.
(Egy adott számról kellene megmondani, hogy melyik két prím szorzata.
Összeszorozni viszont könnyű a két prímet.)

http://travistidwell.com/jsencrypt/demo/

Olyan kapcsolat esetén, amikor mindkét fél jelen van egyszerre, általában a kommunikáció elején megbeszélnek egy közös kulcsot, és szimmetrikus titkosítással folytatják (gyorsabb).

Titkosítás feladat

Feladat: levelezz a szomszédoddal titkosan!

```
# Generalj egy sajat kulcsot
# RSA tipusu, 1024 meretu legyen.
# (vagy https://pgpkeygen.com/ es aztan import...)
gpg --gen-key

#Listazd ki az elerheto kulcsokat
gpg --list-secret-keys

#Oszd meg a publikus kulcsod a szomszeddal
gpg --export --armor XXXXXXXX

#Illetve importald a szomszedod kulcsat
gpg --import ./szomszed_kulcsa
```

Titkosítás feladat

```
#keszits egy bizalmas uzenetet!
echo "Szia, tetszik a mosolyod! :)" > titkos_uzenet

#Titkositsd az uzeneted
#Majd oszd meg a szomszedoddal
gpg --encrypt --recipient szomszed@email.com \
    --armor titkos_uzenet

#Nyisd meg a sajat kulcsoddal a berkezett uzenetet
gpg --decrypt bejovo_uzenet
```

Részletes tutorial:

https://www.devdungeon.com/content/gpg-tutorial

To be continued...