ARHITECTURA SISTEMELOR DE CALCUL – PROIECT 0x00

CRIPTARE XOR

Cristian Rusu

PROIECT

- **cripare/decriptare XOR**
  - Scrieți scripturi python encrypt.py/decrypt.py care iau ca parametru în linia de comandă o cheie și un fișier și realizează criptarea/decriptarea XOR folosind cheia dată. Programul va folosi cheia pentru a cripta conținutul fișierului.

  Exemplu:
  - python encrypt parolamea2021 input.txt output
  - python decrypt output parolamea2021 input_recuperat.txt

  - Fișierul input.txt este mereu unul text. Fișierul output este unul binar, nu text (dar conține același număr de caractere ca și input.txt).
  - Selectați o bucată de text de minim 100KB (literatură clasică de exemplu, în orice caz text lizibil în limba română fără diacritice) și maxim 150KB în fișierul input.txt și generați fisierul output.

  - Nu scrieți niciunde parola folosită, aceasta trebuie să fie secretă. Nu spuneți parola și altor echipe.
  - Parola conține doar: litere mici, litere mari (ambele fără diacritice) și cifre. Dimensiunea parolei este între 10 și 15 caractere.

- **termen limită predat proiect final: 03.12.2021 ora 18:00**
- **punctaj total: maxim 0.4 (din 1 punct maxim posibil pentru proiecte extra)**
- **unde încărcați proiectul (proiectul este încărcat de o singură persoană, liderul echipei): https://forms.gle/FQUxVNL5LVfgSTtM7**
  - numele echipei
  - e-mail contact echipa
  - membrii echipei (prenume nume și grupa)
  - link public github la proiect (va conține: tot codul sursă, fișierele input.txt și output dar fără parola folosită)
  - cheia secretă folosită la criptare (doar aici scrieți cheia folosită pentru a genera output din input.txt)

- **echipa de 2-3 membrii (nu contează seria, grupa, dar minim 2 studenți)**

PROIECT (CONTINUARE)

- **este timpul să vă testați între voi abilitățile de cracker**
- **pe site-ul cursului, la secțiunea proiecte găsiți un fișier pdf unde am asociat aleator echipe**
- **dacă proiectul vostru este implementat corespunzător primiți 0.2 puncte**
- **obiectivul: aflați cheia cu care a fost criptat fișierul output al echipei adverse**
  - **prima parte** (0.2 puncte): folosiți fișierul input.txt, output și fișierele sursă de pe pagina github a echipei adverse pentru a afla cheia (dacă cheia este disponibilă undeva pe pagina github a echipei adverse, folosiți-o; folosiți-vă de orice mijloace tehnice pentru a descoperi cheia)
  - **a doua parte** (0.2 puncte): folosiți fișierul output și fișierele sursă de pe pagina github a echipei adverse pentru a afla cheia (NU aveți voie să folosiți input.txt)
- **chiar dacă echipa adversă "a greșit cu ceva", aflați cheia folosită (aveți acces la codul lor sursă)**
- **în readme pe pagina github scrieți: numele echipei voastre, al echipei adverse și cheia echipei adverse. explicați cum ați rezolvat problema/problemele**
- **tot pe github încărcați orice programe (python sau altceva) ce ați folosit pentru a obține cheia echipei adverse**
- **termen limită predat proiect final: 07.12.2021 ora 23:59**

.

.