



Proiect de curs: Implementarea algoritmilor folosind programarea structurata

Parole sigure utilizând tehnici de criptografie

Secure passwords using cryptographic techniques

Student:

gr. TI-231 FR,
Apareci Aurica
Celan David
Vreme Adrian

Coordonator:

Andrievschi-Bagrin Veronica,
asist.univ.

Problema

Una dintre cele mai comune vulnerabilități este utilizarea parolelor slabe
ceea ce poate duce la acces neautorizat și alte tipuri de fraude.

59% dintre utilizatori folosesc aceeași parolă pentru mai multe conturi, iar **13%** folosesc o singură parolă pentru toate conturile.

(Sursa: Google/Harris Poll, 2021)

Scop

Dezvoltarea unei librării software care să contribuie la securizarea aplicațiilor prin validarea și generarea parolelor sigure, bazate pe principii moderne de criptografie.

Obiective

- 1 Identificarea cerințelor de securitate pentru parole prin studierea standardelor existente.
- 2 Dezvoltarea unei aplicații pentru validarea și generarea parolelor, incluzând verificarea lungimii, implementarea unui algoritm de generare pseudo-aleatorie, posibilitatea de a genera parole memorabile.
- 3 Testarea și validarea programului pentru verificarea funcționalităților, evaluarea performanței algoritmilor utilizați, realizarea documentației complete a aplicației.

A night landscape of a mountain range, likely Yosemite, with a starry sky and a red streak. The mountains are rugged and rocky, with some snow patches. The sky is dark blue with many stars. A red streak is visible in the upper left part of the sky.

MemoPass

soluția propusă

MemoPass

Generate strong, memorable passwords using a 4-step
algorithmic pipeline

Entropy Engine → Story Builder → Leet Transformer → Strength Evaluator

MemoPass Generator

Generate memorable yet strong passwords with mnemonic stories

Generate Password


Check Strength

Word Count: 5

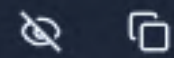


Substitution Complexity: 50%



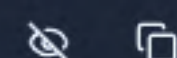
 Generate

Story Password (Original)



robot and nylon event delta

Final Password (With
Transformations)



R0bo7andny1oneventd3lta

Type your own story here to customize

Emoji Visualization

Visual memory aid



Cerințele funcționale

- generarea de parole pe baza unei fraze mnemonice;
- aplicarea de transformări stil Leet în funcție de un nivel de complexitate selectabil;
- evaluarea în timp real a tăriei parolei (cu scor, entropie și estimare brute force);
- posibilitatea de personalizare a parolei prin ajustarea numărului de cuvinte și a complexității;
- opțiunea de copiere rapidă a parolei în clipboard.

Cerințele nefuncționale

- executarea locală completă, fără transmiterea datelor către server;
- răspuns în timp real, fără întârzieri percepute de utilizator (timp de răspuns sub 100 ms);
- interfață intuitivă, prietenoasă, responsive și accesibilă.

Dezvoltarea platformei

Aplicația MemoPass este construită pe baza unei arhitecturi modulare de tip client side, în care toate operațiile sunt executate local, în browserul utilizatorului.

Tehnologii utilizate

Pentru implementarea aplicației MemoPass, au fost selectate tehnologii moderne și ușor portabile, care permit rularea completă a aplicației pe partea de client (client side), fără a necesita un backend. Alegerea acestor tehnologii a avut în vedere trei criterii esențiale: siguranță, performanță și compatibilitate multiplatformă.

Algoritmi utilizați

Diceware · xcvbn · custom MemoPass

Algoritmi utilizați

Diceware · xcvbn · custom MemoPass

Diceware este o metodă de generare a parolelor sigure folosind zaruri pentru a selecta cuvinte aleatorii dintr-o listă predefinită. Fiecare cuvânt este asociat cu o combinație de cinci cifre.

Prin concatenarea mai multor astfel de cuvinte (de obicei 4–7), se obține o parolă ușor de reținut pentru oameni, dar extrem de dificil de ghicit de către un calculator.

Algoritmi utilizați

Diceware • xcvbn • custom MemoPass

xcvbn este o bibliotecă dezvoltată de Dropbox pentru a **evalua puterea parolelor** într-un mod mai realist decât metodele tradiționale bazate pe reguli.

- analizează parolele ținând cont de dicționare comune, nume proprii, tipare de tastatură, date și expresii frecvent folosite;
- estimează **cât timp i-ar lua unui atacator** să spargă parola, oferind un scor de la 0 la 4;

Algoritmi utilizați

Diceware • xcvbn • custom MemoPass

Procesul de generare a parolelor este alcătuit dintr-o succesiune logică de pași, fiecare bazat pe tehnici algoritmice distincte, alese în mod deliberat pentru a echilibra securitatea, uzabilitatea și personalizarea.

pipeline determinist, care organizează logica funcțională în patru pași:

1. selecție criptografică
2. construcție mnemonică
3. transformare contextuală
4. evaluare de tărie

Algoritmi utilizați

Diceware • xcvbn • custom MemoPass

Entropy & Selection Engine, acest modul are sarcina de a produce o bază aleatorie sigură, care stă la baza fiecărei parole generate.

Mnemonic Story Builder scopul acestui pas este de a transforma un șir de cuvinte izolate într-o frază coerentă, ușor de reținut de către utilizator.

Transformare vizuală șirul de caractere este modificat printr un algoritm de tip Leet speak.

Evaluarea entropiei parolei

MemoPass introduce un mecanism de control automat al calității.

“

**securitatea nu se improvizează.
Se construiește**

”

**securitatea nu se improvizează.
Se construiește cu algoritmi potriviți.**

Vă mulțumim pentru atenție !



Want to make a presentation like this one?

Start with a fully customizable template, create a beautiful deck in minutes, then easily share it with anyone.

Create a presentation (It's free)