**Dezvoltarea unei Platforme Centralizate pentru Analiza Criptografică Avansată cu Integrare de Inteligență Artificială**

# Introducere

În domeniul criptografiei, există o gama larga de instrumente specializate, dar acestea sunt adesea dispersate și greu accesibile. Această lucrare propune dezvoltarea unei platforme centralizate care să integreze diverse funcționalități criptografice, să utilizeze tehnici avansate de recunoaștere a modelelor și să incorporeze inteligența artificială pentru analize mai profunde.

# Analiza Problemelor Existente

* **Fragmentarea Instrumentelor:** Instrumentele criptografice sunt diverse și fragmentate, ceea ce îngreunează accesul și utilizarea lor eficientă.
* **Lipsa Centralizării:** Nu există o platformă unică care să ofere acces centralizat la algoritmi, sisteme criptografice și instrumente de analiză.
* **Potențialul IA Neexploatat:** Integrarea inteligenței artificiale în analiza criptografică are un potențial semnificativ, dar este insuficient explorată.
* **Analiza Statistică Limitată:** Lipsa unor instrumente centralizate pentru analiza statistică a metodelor de criptare utilizate.
* **Baze de Date Incomplete:** Baze de date cu numere prime și semiprime sunt dispersate și nu sunt centralizate.

# Obiectivele Proiectului

* Dezvoltarea unei platforme web și CLI pentru analiza criptografică.
* Integrarea instrumentelor existente (RsaCtfTool, AES-CTF-Tool, CyberChef, etc.).
* Implementarea algoritmilor de recunoaștere a modelelor pentru identificarea criptosistemelor.
* Utilizarea IA pentru analiza securității parolelor și criptoanaliză.
* Centralizarea bazelor de date cu numere prime și semiprime.
* Oferirea de analize statistice avansate ale criptogramelor.

# Inspiratie

* Utilitar de atac **RSA**
  + [**https://github.com/RsaCtfTool/RsaCtfTool**](https://github.com/RsaCtfTool/RsaCtfTool)
* Baze de date **open source** cu numere **prime**
  + **https://github.com/ryosan-470/factordb-python/tree/master**
* Utilitar de atac **AES**
  + [**https://github.com/hofill/AES-CTF-Tool**](https://github.com/hofill/AES-CTF-Tool)
* Utilitar generic de **detectie al criptosistemului folosit**
  + [**https://www.dcode.fr/cipher-identifier**](https://www.dcode.fr/cipher-identifier)
* Utilitar de **analiza de criptograma**
  + [**https://gchq.github.io/CyberChef/**](https://gchq.github.io/CyberChef/)
* Utilitar de **hash cracking**
  + [**https://crackstation.net/**](https://crackstation.net/)
* Utilitar de **hash identifier**
  + [**https://www.kali.org/tools/hash-identifier/**](https://www.kali.org/tools/hash-identifier/)
* Criptoanaliza statistica a **criptogramelor de tip bloc**
  + [**https://www.researchgate.net/publication/37413901\_Statistical\_cryptanalysis\_of\_block\_ciphers**](https://www.researchgate.net/publication/37413901_Statistical_cryptanalysis_of_block_ciphers)
* Vulnerabilitati in **design-ul sistemelor criptografice**
  + [**https://ieeexplore.ieee.org/abstract/document/708447**](https://ieeexplore.ieee.org/abstract/document/708447)
* Clasificare algoritmilor de criptare folosind **tehnici de patern recognition**
  + [**https://ieeexplore.ieee.org/abstract/document/5689769**](https://ieeexplore.ieee.org/abstract/document/5689769)
* Aplicatii ale **Inteligentei Artificiale in Criptografie**
  + [**https://arrow.tudublin.ie/engscheleart2/223/**](https://arrow.tudublin.ie/engscheleart2/223/)
* Analiza **rigurozitatii unei parole folosind Inteligenta Artificiala**
  + [**https://link.springer.com/chapter/10.1007/978-981-97-5791-6\_51**](https://link.springer.com/chapter/10.1007/978-981-97-5791-6_51)
* Teste **probabilistice de primalitate**
  + [**https://www.sciencedirect.com/science/article/pii/0022314X80900840**](https://www.sciencedirect.com/science/article/pii/0022314X80900840)
* Analiza **empirica** a coliziunilor algoritmilor de **hashing**

# Functionalitati

*  **Identificare Criptosistem:**
  + Implementarea algoritmilor de recunoaștere a modelelor pentru identificarea automată a tipului de criptare utilizat.
  + Integrarea cu baze de date de semnături criptografice.
*  **Analiza Criptogramelor:**
  + Integrarea CyberChef pentru manipularea și analiza criptogramelor.
  + Implementarea de analize statistice (frecvența literelor, analiza bigramelor, etc.).
  + Implementarea testelor de primalitate (Miller-Rabin, etc.).
*  **Atacuri Criptografice:**
  + Integrarea RsaCtfTool și AES-CTF-Tool pentru atacuri specifice.
  + Implementarea algoritmilor de hash cracking (integrare cu CrackStation).
  + Analiza vulnerabilităților în designul sistemelor criptografice.
*  **Analiza Securității Parolelor:**
  + Utilizarea modelelor de IA pentru evaluarea complexității și securității parolelor.
  + Generarea de rapoarte detaliate privind punctele slabe ale parolelor.
*  **Baze de Date Centralizate:**
  + Crearea unei baze de date cu numere prime și semiprime, optimizată pentru căutări rapide.
  + Integrarea cu baze de date existente.
*  **Analiza Coliziunilor Hash:**
  + Implementarea analizei empirice a coliziunilor algoritmilor de hashing.

# Idee de implementare

* Structura flexibila folosind limbaje de programare precum **C/C++** pentru eficienta
* Utilizare python pentru gestione utilizare **utilitare** existente
* Gestiunea prin intermediul **docker** a bazelor de date
* Solutie software utilizabile din **Browser** si din **linie de comanda**
* Interfata asemanatoare cu **dcode.fr**
* Framework folosit pentru **frontend: React**
* Gestiune **backend: python/js**
* Gestiune **Server Web: Nginx**
* Gestiune baze de date optimizate pentru un numar mare de intrari: **PostgresSQL/MongoDB**
* LLM-uri antrenate cu **TenserFlow** sau **Pytorch** pentru triaj siguranta parolei
* Procurare de date pentru antrenare din utilitare si baze de date **generate + existente**