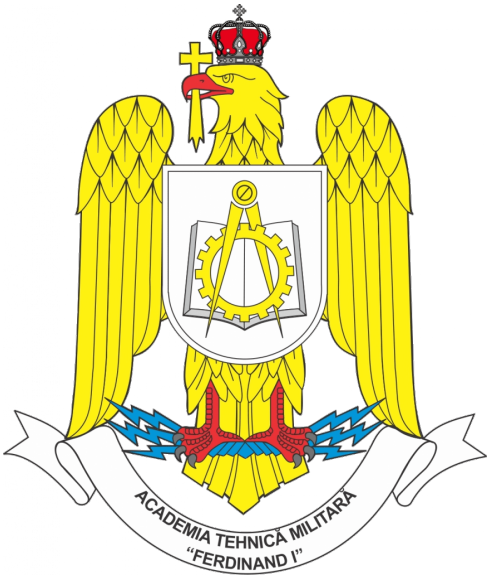
România
Ministerul Apărării Naționale
Academia Tehnică Militară "*Ferdinand I*"

Facultatea de Sisteme Informatice și Securitate Cibernetică
Calculatoare și Sisteme Informatice pentru Securitate si Apărare Națională



Unelte software bazate pe mecanisme de inteligență artificială aplicată în criptografie

Coordonator Științific
Cpt. Subașu Georgiana-Ramona

Absolvent
Std. Sg. Maj. Moldovan Andrei-Gabriel

București
2025

Abstract

Lucrarea propune o platformă integrată care combină diferiți agenți AI specializați ca utilitare de criptanaliză și audit de parole pentru a acoperi un flux complet de securitate modernă din punct de vedere criptografic. Sistemul folosește orchestrare prin microservicii containerizate, momentan, și include: un agent de decizie (SecureBERT) pentru extragere de intenție și de entități relevante; un detector de criptosisteme inspirat din CyberChef/dcode.fr; un orchestrator de spargere de hash-uri cu HashCat și John și generare de parole folosind PassGAN; un agregator de scoruri de parole (rețea neuronală, zxcvbn și HaveIBeenPwned), încă în lucru; un serviciu de testare primalitate/factorizare (YAFU + FactorDB); și un RAG local pentru asistență teoretică în criptografie. Se urmărește realizarea unei platforme centralizate care poate fi folosită local sau în cloud, cu capabilități AI/ML pentru detecție, analiză și suport educațional, punând accent pe modularitate, extindere ulterioară către Kubernetes și aliniere la bune practici de securitate.

Cuvinte cheie: inteligență artificială, criptanaliză, securitate cibernetică, parole, HashCat, John the Ripper, PassGAN, SecureBERT, RAG local, containerizare, microservicii, Kubernetes, FactorDB, YAFU, zxcvbn, HaveIBeenPwned.

Abstract (EN)

The thesis introduces an integrated platform that combines specialized AI agents as cryptanalysis and password-audit utilities to cover a complete, modern security workflow from a cryptographic perspective. The system currently relies on containerized microservice orchestration and includes: a decision agent (SecureBERT) for intent and entity extraction; a cryptosystem detector inspired by CyberChef/dcode.fr; a hash-cracking orchestrator using HashCat and John plus PassGAN-generated candidates; a password-score aggregator (neural network, zxcvbn, and HaveIBeenPwned) still in development; a primality/factorization testing service (YAFU + FactorDB); and a local RAG for theoretical assistance in cryptography. The goal is a centralized platform deployable locally or in the cloud, with AI/ML capabilities for detection, analysis, and educational support, emphasizing modularity, future expansion toward Kubernetes, and alignment with security best practices.

Keywords: artificial intelligence, cryptanalysis, cybersecurity, passwords, HashCat, John the Ripper, PassGAN, SecureBERT, local RAG, containerization, microservices, Kubernetes, FactorDB, YAFU, zxcvbn, HaveIBeenPwned.

Cuprins

1 Introducere **1**
1.1 Context general . . . 1
1.2 Problema abordată . . . 1
1.3 Scopul lucrării . . . 1
1.4 Obiective specifice . . . 1

2 Fundamente Teoretice **2**
2.1 Elemente de bază ale criptografiei . . . 2
2.1.1 Definiții și clasificare . . . 2
2.1.2 Standardizare . . . 2
2.2 Elemente fundamentale de inteligență artificială . . . 2
2.2.1 Paradigme de învățare . . . 2
2.2.2 Modele generative și transformere . . . 2
2.2.3 GAN și LLM în securitate . . . 3
2.3 Conexiunea AI–Criptografie . . . 3
2.3.1 Domenii de aplicare . . . 3
2.3.2 Limitări curente . . . 3

3 Soluția Propusă **4**
3.1 Arhitectura generală . . . 4
3.2 Metodologie și justificarea alegerilor . . . 4
3.2.1 Selecția tehnologiilor . . . 4
3.2.2 Modele AI utilizate . . . 4
3.2.3 Principii de securitate . . . 4
3.3 Descrierea componentelor . . . 4
3.3.1 Modul AI . . . 4
3.3.2 Modul criptografic . . . 4
3.3.3 Orchestrator și interfețe . . . 5

4 Implementare **6**
4.1 Mediu de dezvoltare . . . 6
4.2 Framework-uri și librării . . . 6
4.3 Containerizare și infrastructură . . . 6
4.4 Măsuri de securitate aplicate . . . 6
4.5 Automatizare . . . 6

5 Testare și Evaluare **7**
5.1 Metodologia de testare . . . 7
5.1.1 Teste unitare . . . 7
5.1.2 Teste de integrare . . . 7
5.1.3 Teste de performanță . . . 7

5.2 Metrici și criterii de evaluare 7
5.3 Validarea rezultatelor 7

6 Rezultate și Discuții **8**
6.1 Benchmark-uri comparative 8
6.2 Analiza performanței 8
6.3 Beneficii și limitări 8
6.4 Direcții de îmbunătățire 8

7 Concluzii **9**
7.1 Gradul de atingere a obiectivelor 9
7.2 Contribuții 9
7.3 Impact și dezvoltări viitoare 9

Bibliografie **10**

8 Anexe **11**
8.1 Listă de diagrame suplimentare 11
8.2 Configurații tehnice 11
8.3 Scripturi și manual de utilizare 11

Listă de Abrevieri

AI ..... artificial intelligence

ML ..... machine learning

PKI ..... public key infrastructure

RAG ..... retrieval-augmented generation

TLS ..... transport layer security

AES ..... Advanced Encryption Standard

DES/3DES .. Data Encryption Standard / Triple DES

RSA ..... Rivest–Shamir–Adleman (public-key cryptography)

ECC ..... elliptic curve cryptography

HMAC ..... hash-based message authentication code

AEAD ..... authenticated encryption with associated data

LLM ..... large language model

PQC ..... post-quantum cryptography

Capitolul 1: Introducere

1.1 Context general

Criptografia modernă a evoluat cu pași repezi, de la algoritmi simetrici clasici (DES, 3DES), către standarde robuste precum AES și suitele asimetrice (RSA, ECC), odată cu dezvoltarea infrastructurilor PKI și a protocoalelor TLS, precum și apariției PQC. În paralel, progresul AI a adus atât beneficii considerabile, cât și riscuri: modelele de tip ML/LLM pot accelera detecția anomaliilor și analiza traficului criptat, putând fi folosite și pentru generarea de atacuri (phishing, parole, malware) sau pentru asistarea criptanalizei. Astfel, securitatea cibernetică integrează din ce în ce mai mult tehnici AI precum răspuns rapid, corelare de evenimente și întărirea mecanismelor criptografice.

1.2 Problema abordată

Problema principală urmărește modul în care putem folosi agenți AI specializați pentru a automatiza analiza și răspunsul la amenințări criptografice, de la identificarea algoritmilor și auditul parolelor, până la factorizare pentru testare de securitate, cât și modul în care se poate îmbunătăți educația criptografică. Se observă, de asemenea, lipsa unei platforme integrate care să ofere aceste capabilități într-un mod modular, scalabil și sigur.

1.3 Scopul lucrării

Scopul lucrării este reprezentat de proiectarea unei platforme integrate, modulare și scalabile care folosește agenți AI pentru identificare de algoritmi, audit de parole, factorizare / teste criptografie, asistență teoretică, astfel încât detecția, analiza și răspunsul la amenințări să fie automatizate, reproductibile și ușor de folosit, atât local, cât și în cloud.

1.4 Obiective specifice

- Realizarea și testarea robustă a unei părți din agenții AI propuși.
- Integrarea tuturor agenților într-o infrastructură comună.
- Crearea unei soluții robuste de deploy și testare.
- Crearea unui Web Frontend și a unui Client CLI.
- Legarea componentelor într-un flux coerent.

Capitolul 2: Fundamente Teoretice

2.1 Elemente de bază ale criptografiei

Criptografia urmărește să asigure confidențialitate, integritate, autentificare și nerepudiere pentru date transmise pe canale nesigure. Se împart două familii majore: criptografia simetrică (aceeași cheie pentru criptare/decriptare) și criptografia asimetrică (pereche publică/privată), completate de funcții hash și coduri de autentificare a mesajelor (MAC/HMAC) [3, 1, 2]. Un criptosistem se definește formal prin spațiul mesajelor, al textelor cifrate, al cheilor și printr-o familie de funcții de criptare/decriptare parametrizate de cheie, iar securitatea se descrie prin modele de adversar și noțiuni riguroase de rezistență la atac. În practică, protocoalele moderne combină aceste primitive cu management de chei (generare, stocare, rotație) și cu mecanisme de transport securizat (ex. TLS), fiind fundamentele pe care se sprijină soluția propusă.

2.1.1 Definiții și clasificare

Include definițiile pentru criptografie simetrică, criptografie asimetrică, funcții hash și alte primitive relevante. Discută diferențele între acestea și cazurile tipice de utilizare.

2.1.2 Standardizare

Enumeră standardele și organismele relevante (NIST, IEEE, RFC, GDPR, standarde militare) și menționează rolul lor în conformarea soluției propuse.

2.2 Elemente fundamentale de inteligență artificială

Descrie conceptele cheie din domeniul inteligenței artificiale care vor fi folosite în lucrare.

2.2.1 Paradigme de învățare

Discută despre învățarea supravegheată, nesupravegheată și prin întărire, raportându-te la scenariul lucrării.

2.2.2 Modele generative și transformere

Introduce arhitecturile Transformer, modelele generative moderne și implicațiile lor în securitatea cibernetică.

2.2.3 GAN și LLM în securitate

Prezintă modul în care GAN și LLM sunt utilizate în detecția și generarea de conținut relevant pentru securitate, incluzând exemple recente.

2.3 Conexiunea AI–Criptografie

Leagă componentele AI și criptografie pentru a fundamenta soluția propusă.

2.3.1 Domenii de aplicare

Analizează scenarii precum cryptoanalysis asistată de AI, generarea de parole, detecția anomaliilor sau automatizarea proceselor de securitate.

2.3.2 Limitări curente

Identifică limitările actuale ale abordărilor combinate AI–criptografie și explică modul în care soluția propusă răspunde acestor provocări.

Capitolul 3: Soluția Propusă

3.1 Arhitectura generală

Descrie arhitectura macro a sistemului și include o diagramă care evidențiază principalele componente și fluxuri de date.

3.2 Metodologie și justificarea alegerilor

Explică abordarea metodologică, pașii parcurși și motivele pentru alegerea tehnologiilor și a modelelor AI.

3.2.1 Selecția tehnologiilor

Detaliază limbajele, cadrele și infrastructura utilizate și argumentează selecția lor.

3.2.2 Modele AI utilizate

Prezintă modelele AI integrate, modul în care sunt antrenate, configurate și orchestrate.

3.2.3 Principii de securitate

Descrie măsurile de securitate și mecanismele de protecție integrate încă din etapa de proiectare.

3.3 Descrierea componentelor

Analizează fiecare componentă a soluției folosind paragrafe dedicate ce includ rolul, funcționarea, diagrama și justificarea tehnologică.

3.3.1 Modul AI

Detaliază agentul AI, capabilitățile, datele utilizate și modul de interacțiune cu celelalte componente.

3.3.2 Modul criptografic

Descrie serviciile criptografice, protocoalele implementate și modul de integrare cu orchestrarea AI.

3.3.3 Orchestrator și interfețe

Prezintă modul de coordonare între componente, fluxurile de lucru și interfețele expuse (CLI, API, UI).

Capitolul 4: Implementare

4.1 Mediu de dezvoltare

Detaliază uneltele de dezvoltare, sistemul de operare, dependințele și configurațiile cheie.

4.2 Framework-uri și librării

Listează și descrie framework-urile, librăriile și modelele AI utilizate, inclusiv versiunile.

4.3 Containerizare și infrastructură

Prezintă modul în care aplicația este containerizată și orchestrată (Docker, docker-compose, Kubernetes etc.).

4.4 Măsuri de securitate aplicate

Enumeră controalele de securitate implementate (hardening, politici, rotație de chei, audit).

4.5 Automatizare

Descrie scripturile, pipeline-urile CI/CD sau orice automatizare care susține proiectul.

Capitolul 5:
Testare și Evaluare

5.1 Metodologia de testare

Descrie strategia generală de testare și criteriile utilizate pentru a valida soluția.

5.1.1 Teste unitare

Prezintă acoperirea testelor unitare, instrumentele folosite și exemple relevante.

5.1.2 Teste de integrare

Detaliază scenariile de integrare și modul în care componentele sunt validate împreună.

5.1.3 Teste de performanță

Specifică metodologiile și instrumentele folosite pentru măsurarea performanței și scalabilității.

5.2 Metrici și criterii de evaluare

Definește indicatorii cantitativi și calitativi utilizați în analizarea rezultatelor testelor.

5.3 Validarea rezultatelor

Analizează rezultatele obținute în raport cu obiectivele propuse și discută implicațiile.

Capitolul 6:
Rezultate și Discuții

6.1 Benchmark-uri comparative

Prezintă rezultate numerice și comparații cu soluții similare sau baseline-uri.

6.2 Analiza performanței

Evaluează latența, throughput-ul, utilizarea resurselor și scalabilitatea.

6.3 Beneficii și limitări

Rezumă beneficiile soluției și limitele identificate în urma testării.

6.4 Direcții de îmbunătățire

Propune optimizări și extensii viitoare.

Capitolul 7: Concluzii

7.1 Gradul de atingere a obiectivelor

Recapitulează modul în care au fost îndeplinite obiectivele definite în introducere.

7.2 Contribuții

Enumeră contribuțiile teoretice și practice ale lucrării.

7.3 Impact și dezvoltări viitoare

Evaluează impactul potențial și prezintă direcții de continuare a cercetării.

Bibliografie

[1] Bruce Schneier. *Applied Cryptography*. Wiley, 1996.

[2] William Stallings. *Cryptography and Network Security*. Pearson, 2017.

[3] Douglas R. Stinson. *Cryptography: Theory and Practice*. CRC Press, 2005.

Capitolul 8:
Anexe

8.1 Listă de diagrame suplimentare

Include diagrame detaliate (de exemplu, PlantUML, diagrame de secvență sau arhitecturi alternative) care completează prezentarea din capitolele principale.

8.2 Configurații tehnice

Prezintă fișiere de configurare relevante (de exemplu, `docker-compose.yml`, fișiere de mediu, politici de securitate) și explică modul în care acestea sunt utilizate.

8.3 Scripturi și manual de utilizare

Include scripturile auxiliare și un ghid succint de utilizare a aplicației pentru diferitele roluri implicate.