Ministerul Educaţiei, Culturii și Cercetării

Universitatea Tehnică a Moldovei

Faculatea Calculatoare, informatică și microelectronică  
Departamentul Ingineria Software și Automatică



**RAPORT**

Lucrare de Laborator nr.4

Disciplina: Proiectarea sistemelor informaționale

A efectuat:

Chihai Adrian

A verificat:

Magdei Octavian

Chişinău 2024

# Descrierea procesului ales

Procesul selectat pentru realizarea acestei lucrări de laborator reprezintă procesul de cracking al hash-urilor utilizând tehnici brute-force. Acesta este conceput pentru a analiza și sparge hash-uri criptografice, oferind utilizatorului rezultate detaliate și rapoarte de performanță. Este un instrument valoros pentru profesioniștii în securitate cibernetică, deoarece le permite să identifice vulnerabilități și să optimizeze procesele legate de hashing.

Procesul poate implica următorii pași:

* Verificarea existenței hash-ului introdus: Sistemul verifică dacă hash-ul introdus este deja procesat și există un raport asociat.
* Identificarea tipului de hash: Dacă hash-ul este nou, sistemul determină tipul acestuia (ex: MD5, SHA-1, SHA-256).
* Executarea algoritmului de brute-force: Pe baza tipului de hash, se selectează algoritmii și wordlist-urile relevante pentru procesare.
* Generarea raportului: După procesare, sistemul creează un raport detaliat care include timpul de execuție, metoda utilizată și rezultatul (parola descoperită sau mesaj de eșec).

Unul dintre primii pași importanți este verificarea existenței hash-ului. În cazul în care hash-ul există, raportul corespunzător este accesat pentru a economisi timp și resurse. Dacă hash-ul nu există, sistemul continuă cu identificarea tipului și aplicarea algoritmului brute-force. În timpul procesului, utilizatorul este ghidat de interfața aplicației, care oferă informații și notificări despre progres.

La final, raportul generat este asociat hash-ului procesat și salvat pentru referințe viitoare. Acest raport poate fi utilizat pentru a analiza eficiența procesului și pentru a evalua performanța diferiților algoritmi utilizați. Procesul asigură utilizatorului o experiență simplificată și rezultatele sunt prezentate într-un format ușor de înțeles.

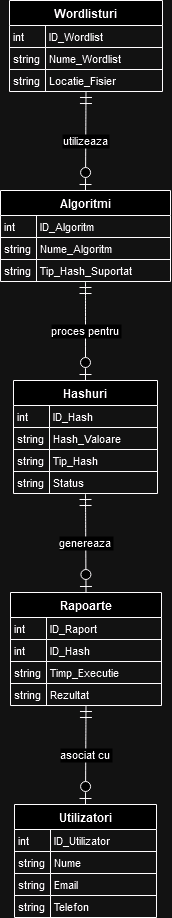
Procesul de cracking al hash-urilor cu brute-force contribuie semnificativ la înțelegerea și optimizarea securității criptografice. Este un instrument esențial pentru profesioniști și permite descoperirea vulnerabilităților în algoritmii de hashing, facilitând adoptarea de măsuri de protecție mai eficiente.

# Elaborarea unui model logic pentru procesul ales

Diagrama IDEF1x, cunoscută și sub denumirea de Integration Definition for Information Modeling, este o unealtă fundamentală utilizată în ingineria sistemelor, fiind special creată pentru a modela și descrie structura informațională a unui sistem. Dezvoltată inițial în cadrul programului IDEF de către Forțele Aeriene ale Statelor Unite, această diagramă se axează pe definirea și conturarea modelelor conceptuale pentru bazele de date și alte sisteme informaționale complexe, contribuind la o înțelegere clară a relațiilor și atributelor esențiale între diferite entități.

Această formă de reprezentare vizuală are la bază diverse componente esențiale, fiecare contribuind la o ilustrare detaliată a organizării informaționale într-un sistem. Entitățile, reprezentate prin dreptunghiuri, constituie elementele fundamentale ale sistemului, descriind conceptele sau obiectele care stochează informații. Atributele, exprimate prin elipse, caracterizează entitățile, oferind detalii despre proprietățile și trăsăturile acestora. Relațiile, reprezentate prin linii ce leagă entități, indică interdependențele și conexiunile dintre elementele sistemului. Cheile, ilustrate prin simboluri specifice, oferă detalii despre modul de identificare unică a entităților în cadrul sistemului.

Scopul principal al acestei diagrame este de a facilita proiectarea și înțelegerea structurii informaționale a sistemului. Prin oferirea unei reprezentări clare a relațiilor dintre entități, atribute și chei, diagrama IDEF1x devine un instrument deosebit de eficient pentru comunicarea cerințelor și specificațiilor între membrii echipelor implicate în dezvoltarea sistemului. Aceasta contribuie la eliminarea ambiguităților și promovează o înțelegere comună a arhitecturii sistemului, sprijinind astfel eficientizarea procesului de proiectare și implementare a sistemelor informaționale complexe.



**Figura 2.1** Diagrama IDEF1x pentru procesul ales

În cadrul diagramei IDEF1X pentru procesul de cracking al hash-urilor, sunt definite cinci entități principale: "Hashuri", "Algoritmi", "Rapoarte", "Wordlisturi" și "Utilizatori". Aceste entități sunt interconectate printr-un set de relații bine structurate conform notației IDEF1X.

Entitatea "Utilizatori" reprezintă utilizatorii aplicației, fiecare identificat printr-un ID unic. Acești utilizatori sunt legați de unul sau mai multe "Rapoarte", care reflectă rezultatele proceselor de cracking efectuate.

"Hashuri" este o entitate distinctă, caracterizată prin atribute precum valoarea hash, tipul și statusul acestuia. Fiecare hash poate avea un raport asociat, înregistrând rezultatele cracking-ului.

Entitatea "Rapoarte" acționează ca o punte între "Utilizatori" și "Hashuri", reflectând detalii despre procesul de cracking, precum timpul de execuție și rezultatul operației. Fiecare raport este conectat la un hash specific și asociat cu un utilizator.

"Algoritmi" reprezintă metodele utilizate pentru procesarea hash-urilor. Fiecare algoritm este caracterizat prin tipurile de hash-uri suportate și este utilizat în cadrul proceselor de cracking pentru a determina parolele asociate.

Entitatea "Wordlisturi" definește colecțiile de parole utilizate în timpul proceselor brute-force. Acestea sunt asociate cu algoritmi specifici pentru a optimiza cracking-ul hash-urilor.

Această diagramă IDEF1X furnizează o reprezentare clară și coerentă a relațiilor dintre entitățile din aplicația de cracking al hash-urilor, facilitând astfel proiectarea, dezvoltarea și gestionarea sistemului.

# Concluzie

Explorarea aplicației AllFusion ERwin Data Modeler a permis o înțelegere detaliată a conceptelor cheie asociate modelării datelor. Familiarizarea cu standardul IDEF1x pentru modelele logice de date a furnizat un cadru coerent și bine definit pentru proiectarea unui model logic al datelor în cadrul procesului ales, respectiv cracking-ul hash-urilor cu tehnici brute-force.

Modelarea datelor conform standardului IDEF1x pentru acest proces specific a rezultat într-o reprezentare detaliată și semnificativă a structurii sistemului, evidențiind entitățile implicate, atributele acestora și relațiile dintre ele. Această abordare a contribuit la claritatea și coerența conceptuală a întregului sistem, oferind un fundament solid pentru etapele ulterioare de dezvoltare și implementare.

Elaborarea modelului logic al datelor a implicat analiza atentă a cerințelor specifice procesului de cracking al hash-urilor, evidențiind fluxurile de informații și interacțiunile între entități. Modelul rezultat reflectă modul în care datele sunt structurate și utilizate în procesul de identificare a parolelor asociate hash-urilor, contribuind la o înțelegere mai profundă a necesităților sistemului.

În final, integrarea AllFusion ERwin Data Modeler și a standardului IDEF1x în procesul de proiectare a permis o modelare eficientă și coerentă a datelor pentru cracking-ul hash-urilor. Această abordare solidă constituie un punct de plecare esențial pentru dezvoltarea și implementarea eficientă a sistemului propus, asigurând o structură bine definită și o gestionare optimă a informațiilor asociate acestui proces specific.