Rezumat

Lucrarea de față își propune să creeze un mediu securizat care are ca scop protejarea datelor unui utilizator deținute de acesta pe un PC și având sistemul de operare Windows.

Creșterea exponențială a dezvoltării domeniului IT a dus atât la mărirea importanței datelor cât și implicit la creșterea pericolelor (atacuri) la care sunt supuse în prezent.

Conceptul de atac se referă la modul în care un hacker reușește să preia controlul unui sistem și ce poate sa facă cu el având ca scop principal alterarea datelor și accesul la informații confidențiale. Principalele tipuri de atacuri asupra rețelelor de calculatoare sunt următoarele: atacuri prin social engineering, DoS, scanări și spoofing, source routing, troieni, viruși și viermi .

O soluție viabilă care are ca scop securizarea datelor precum și diminuarea riscului unor atacuri provenite din exterior este reprezentată de criptografie.

Proiectul de față își propune utilizarea procesului de compresie urmată de criptare puse la dispoziție de mediul de programare Java, oferind astfel o securitate sporită a datelor.

Utilizarea procesului de compresie are ca scop principal diminuarea spațiului de stocare a datelor iar procesul de criptare are ca scop ascunderea informației. Odată ce o informație este criptată este aproape imposibil de vizualizat conținutul inițial fără a avea cheia de criptare/decriptare corespunzătoare. Criptarea datelor de realizează prin implementarea a cinci algoritmi de criptare dintre care patru sunt simetrici (AES, RC4, BlowFish, 3DES) și unul asimetric (RSA).

Compresia datelor se realizează simultan prin utilizarea librăriei zip4j din Java și implementarea algoritmului de codare Huffman.

Pentru a oferi utilizatorului o aplicație ușor de utilizat, din punct de vedere a tipului de utilizator, au fost implementate două module funcționale prin care acesta își poate proteja datele.

Primul modul funcțional, este destinat pentru utilizatorul „normal”. Modulul va oferi o interacțiune simplificată a utilizatorului cu aplicația prin faptul că acesta nu trebuie să introducă o parola sau să selecteze ce algoritm se folosește de fiecare data când se introduce un nou fișier în aplicație.

Al doilea modul adresat utilizatorului „expert” oferă acestuia posibilitatea selectării tipului algoritmului de criptare și a celui de compresie folosit precum și a alegerii unui parole.

Dimensiunea pentru fiecare fișier introdus în aplicație trebuie sa fie de maxim 100 MB.