Proiect – Elemente avansate de programare

-Documentație-

Proiectul consta intr-o aplicatie JAVA care permite criptarea unui fisier text folosind un cifru Vernam. Aplicatia are o interfata grafica si permite efectuarea a mai multor operatii, cum ar fi: selectarea unui generator de numere pseudo-aleatoare, salvarea cheii de decriptare intr-un fisier text, selectarea si afisarea unui fisier text, criptarea fisierului folosind un cifru Vernam si salvarea acestuia.

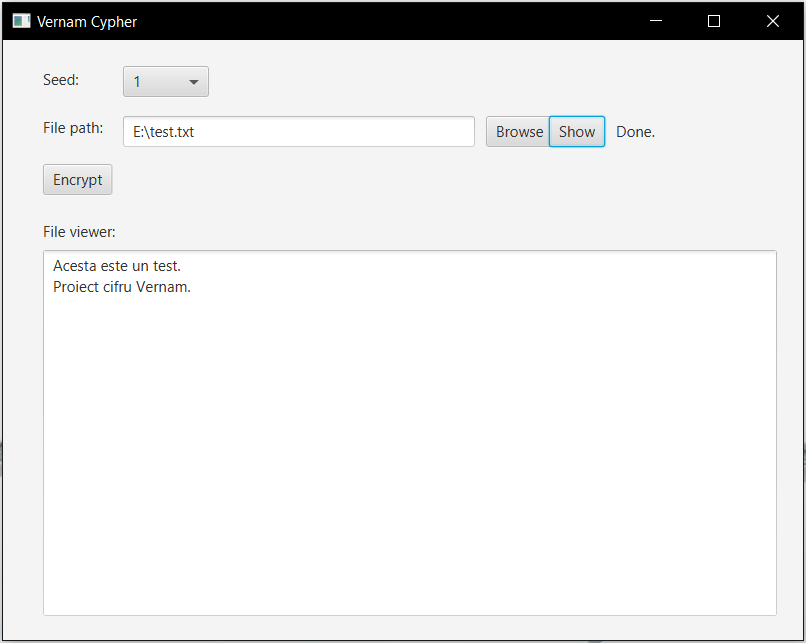
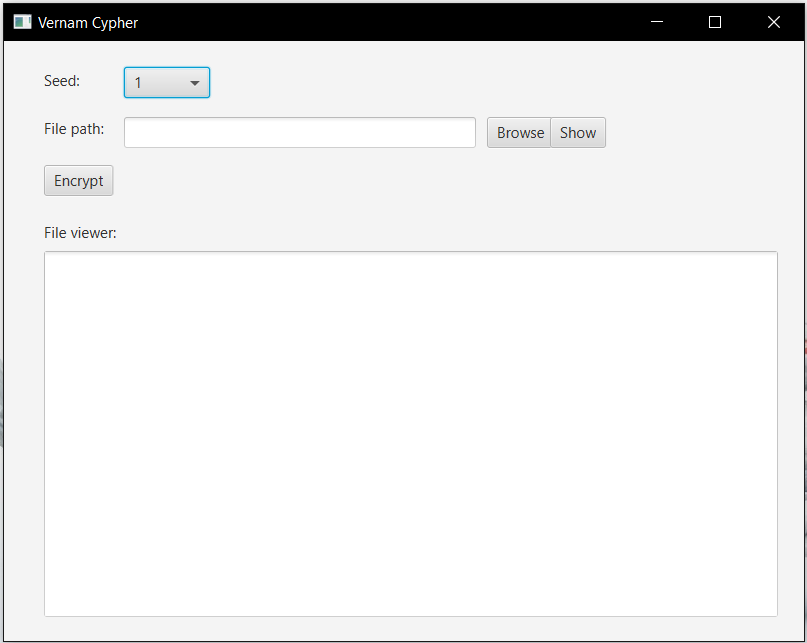
Echipa care a realizat proiectul este compusa din studentii **Buduianu Alexandru** si **Paraschiv David-Nicola** de la grupa CTI 253.

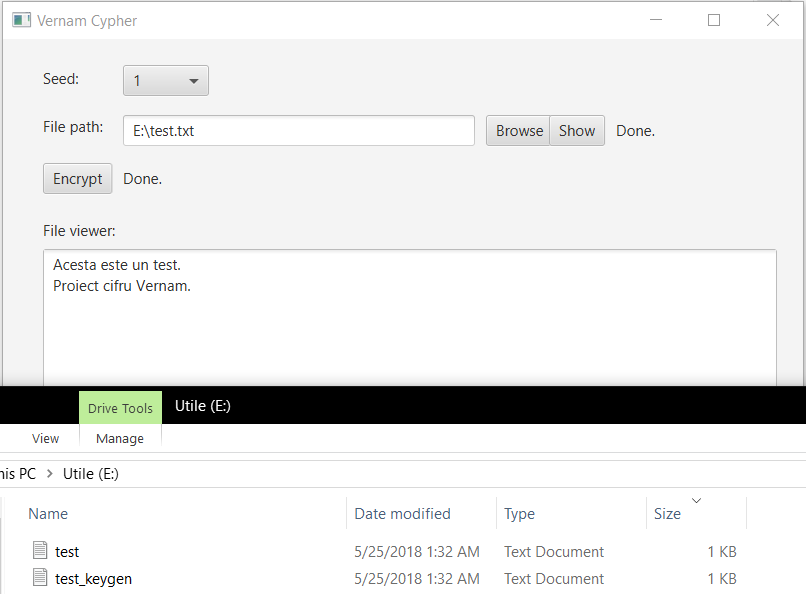
Etapele de dezvoltare ale proiectului au constat in: documentarea despre cifrul Vernam, realizarea unei interfete grafice(Java FX), programarea evenimentelor(ce face fiecare buton) si testarea erorilor. Am folosit SecureRandom(generarea vectorului de numere pseudo-aleatoare), Java FX, NIO.

In procesul de criptare al unui fisier text, utilizatorul alege o cheie de incriptare(un generator de numere aleatoare, implicit e „1”) din „Seed”. Urmatorul pas este acela de a alege fisierul text pe care sa-l cripteze(acesta trebuie sa aiba extensia .txt pentru a putea fi criptat), utilizatorul alegandu-l apasand pe butonul „Browse” si selectand din calculator fisierul text dorit, urmand ca in campul „File path” sa fie afisata adresa fisierului text selectat. Utilizatorul are optiunea de a arata in interiorul aplicatiei textul fisierului, prin apasarea butonului „Show”(se va afisa „Done.” daca a avut succes). Avand selectate fisierul text si cheia de incriptarea, pentru a cripta efectiv textul, se apasa pe butonul „Encrypt”, acesta afisand textul „Done.” dupa ce criptarea a avut loc. La incriptare, se genereaza automat un fisier de forma „fisier-text-ales\_keygen.txt” care contine cheia de criptare a fisierului text ales. Criptarea se va suprascrie peste fisierul text selectat de utilizator. Pentru decriptarea acestuia, utilizatorul trebuie sa foloseasca aceeasi cheie de criptare(din „Seed”) cu care a incriptat fisierul text, care este salvata in fisierul generat la incriptare.

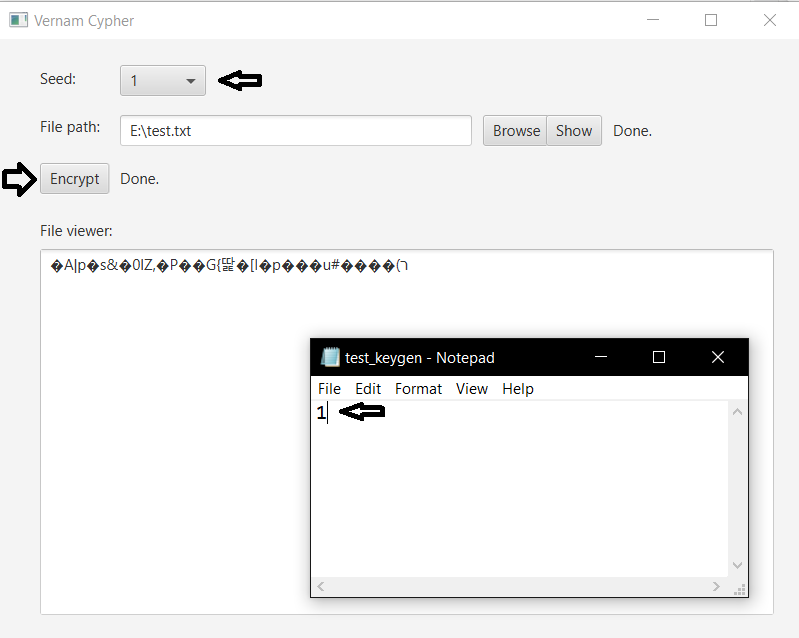
Aplicatia lucreaza cu date stocate in fisiere, pentru aceasta am folosit NIO(New Input/ Output, o biblioteca a limbajului de programare Java).

Sectiunile importante ale aplicatiei sunt prezentate in urmatoarele imagini:









In urma realizarii acestui proiect, am acumulat cunostinte despre cifrul Vernam(matematica si criptografie) si totodata ne-am imbunatatit abilitatile de munca in echipa.