# Exercitiul 1

1. Problema a fost rezolvata in limbajul c++
2. Pentru operatiile de criptare si decriptare am utilizat API-ul specificat in cerinta problemei si anume API EVP
3. In directorul Ex1 sunt urmatoarele fisiere:
4. **file\_service.h**

* Fisierul contine functii de baza pentru lucru cu fisiere (ex citire/scriere) precum si functiile trim si de padare

1. **criptor.cpp**

* Scopul acestuia este de cripta un un fisier de input si scrierea criptarii in fisierul output folosind o cheie random din dictionarul de cuvinte
* Modurile de criptare sunt cele cerute in enuntul problemei si anume ECB si CBC

1. **over\_AES\_service.h**

* Acest fisier h contine functiile de criptare si decriptare in ele doua moduri specificate mai sus
* Sunt implementate atat functile de criptare cat si cele de decriptare
* Ca variabila globala in acest fisier este initial\_vector

1. **main.cpp**

* programul care primeste plaintext-ul, criptotext-ul si modul de criptare si gaseste cheia cu care a fost criptat plaintext-ul.
* In acest fisier se apeleaza functionalitatiile din fisierele descries mai sus.

1. Idea de rezolvare:

* Ideea de rezolvare este una simpla avand urmatoarele date de intrare programul din fisierul main:
  + file\_in (plaintext)
  + file\_out (criptotext)
  + mode (modul de criptare)
  + datele de intrare se valideaza (sa existea file\_in, file\_out si mode sa fie unul din modurile specificate ECB si CBC
* pentru fiecare cheie din dictionar
  + se cripteaza plaintext-ul si se compara cu criptotextul
  + daca acestea corespund inseamna ca am gasit cheia potrivita
* daca cheia nu a fost gasita se afiseaza un mesaj corespunzator

1. Modul de rulare: in directorul Ex3 se afla fisierul MakeFile la rularea caruia
   1. Se ruleaza executabilul criptor pentru a cripta mai intai file\_in cu un mod specificat in file\_out
   2. Se ruleaza executabilul main pentru a gasi cheia cu care sa criptat file\_in si a fost obtinut file\_out de la pasul precedent