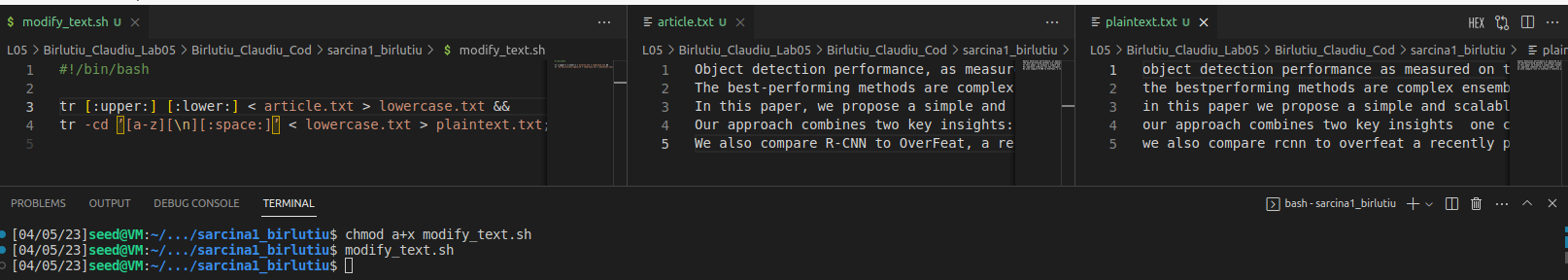
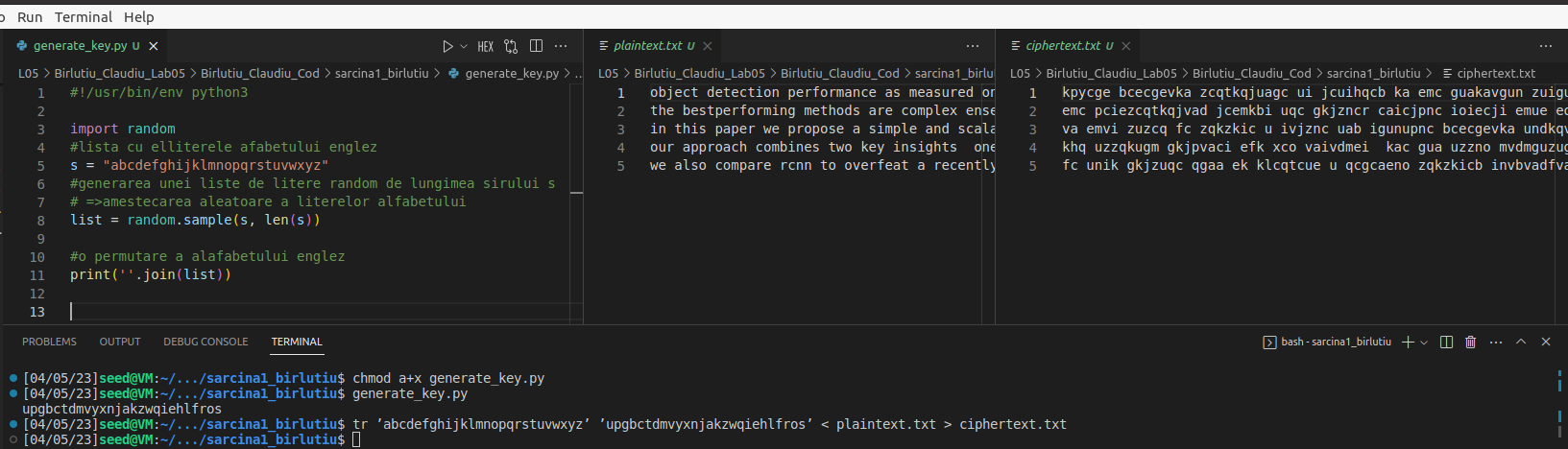
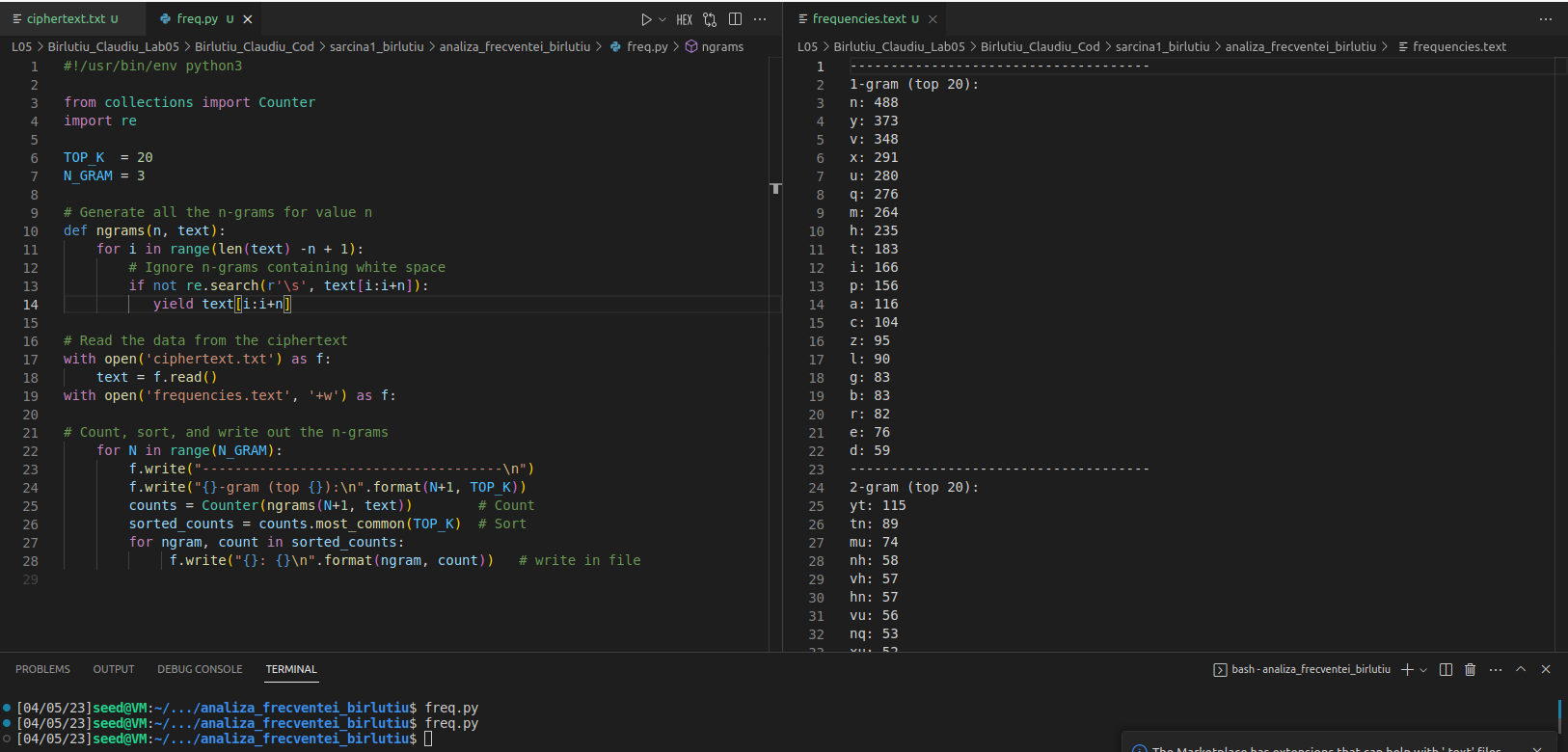
# Raport pentru lucrarea 5: Cifrarea cu cheie secretă

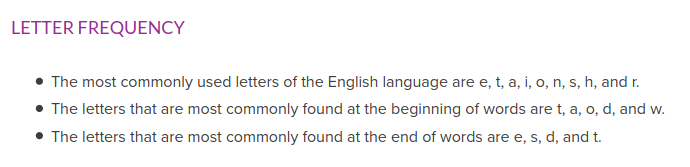
Autor: Birlutiu Claudiu-Andrei, gr 30643

## Sarcina 1: Analiza frecvenței împotriva unui cifru de substituție monoalfabetic

* În continuare am urmat tuorialul de criptare:
  + in prima faza am creat un script bash care ia cifrul și îl transforma în plain text (fără semene de punctuatie și litere mici) – fișierul se numește **modify\_script.sh** și i s-a dat permisiuni de execuție; se observa ca din textul article.txt s-a generat plaintext.txt care reprezintă textul fără cemne de punctuatie și lowercase
  + am creat un script python care genereaza o cheie aleatoare de mapare a literelor alfabetului la o alta litera și am făcut inlocuirile pe plaintext.txt => cipher.txt



* Am trecut la descifrarea textului criptat din lucrare. Scopul a fost sa analizez frecventa literelor sau grupurilor de litere astfel încât sa găsesc cheia de criptare a mesajului
* am modificat programul python de analiza a textului sa scrie într-un fisier frecventele
* am căutat pe internet care sunt cele mai frecvente litere din limba engleza



***Sarcina 2: Criptarea cu diferite cifruri și în diverse moduri***

## Sarcina 3: Modul de criptare -- ECB vs. CBC

## Sarcina 4 : Caractere de completare pentru textul în clar

### Care sunt caracterele de completare în cifrarea AES atunci când lungimea textului în clar este 20 octeți și 32 octeți

1. **Considerați modurile ECB, CBC, CFB, și OFB de cifrare a unui fișier. Care au caractere de completare și care nu au?**

## Sarcina 5: Propagarea erorilor -- Text cifrat alterat

### Câtă informație puteți recupera din descifrarea fișierului alterat, dacă modul de cifrare a fost ECB, CBC, CFB, respectiv OFB?

### Răspunsul dat înainte de efectuarea sarcinii

### Răspunsul după execuția acestei sarcini.

### Explicați de ce.

## Sarcina 6. Vectorul inițial (IV) și erori comune

### 6.1 Sarcina 6.1. Unicitatea IV

### 6.2 Sarcina 6.2. Eroare comună: folosirea aceluiași IV

### 6.3 Sarcina 6.3. Eroare comună: folosirea unui IV predictibil

## Sarcina 7: Programarea folosind biblioteca criptografică