# Raport pentru lucrarea 5: Cifrarea cu cheie secretă

Autor:

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

***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