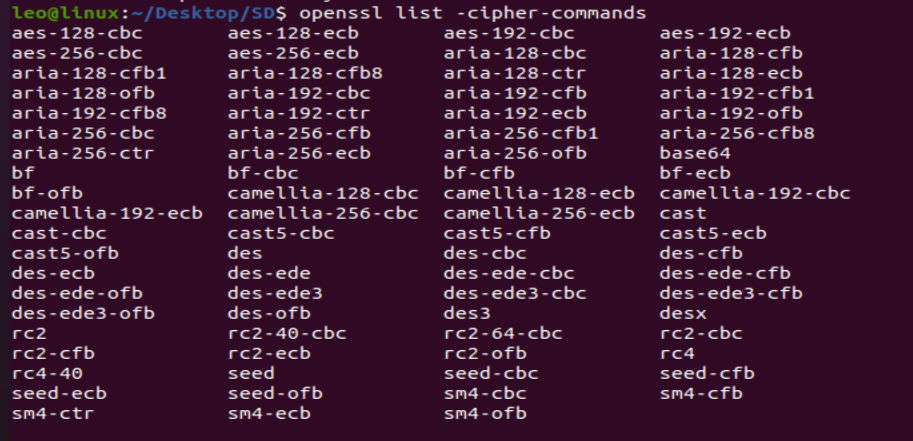
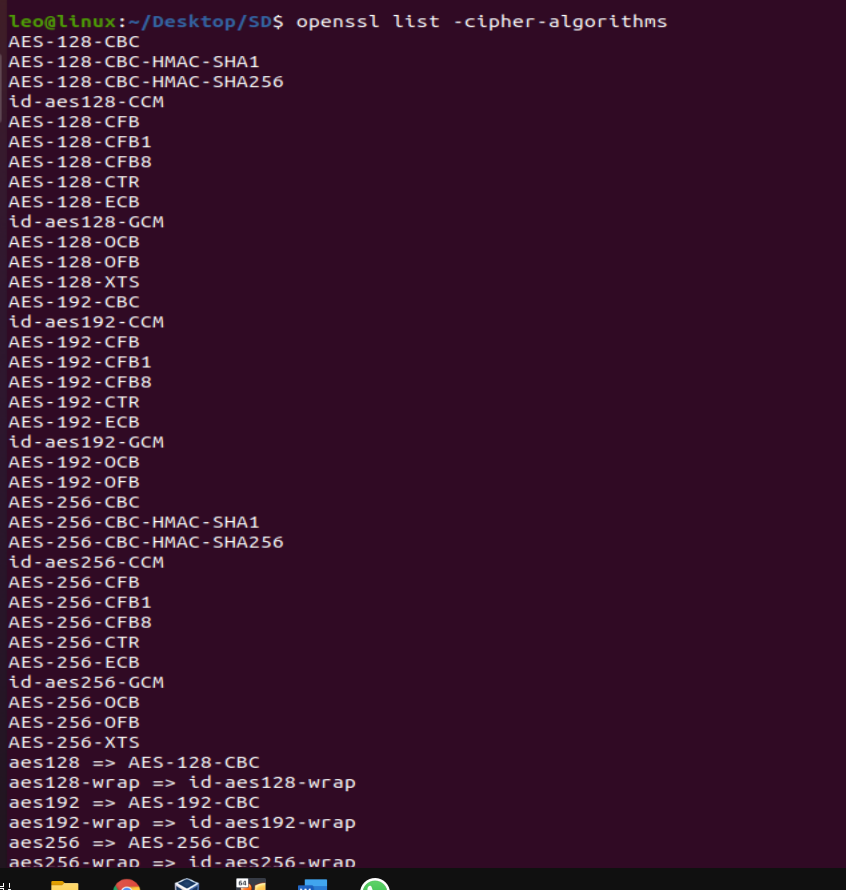
Laborator 4

Pârvan Andrei Leonard Calculatoare 4 4LF781

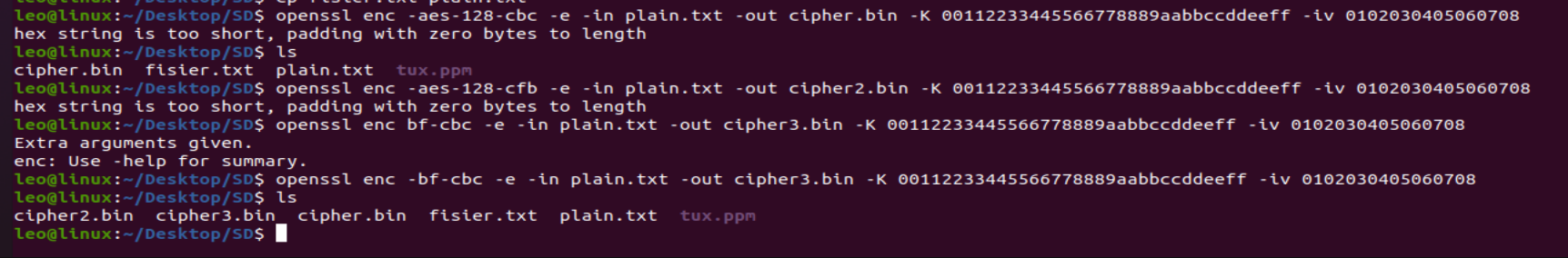
1. Familiarizati-va cu comanda *openssl: man openssl.*Cautati parametrul list si listati *cipher-commands*si*cipher-algorithms*.



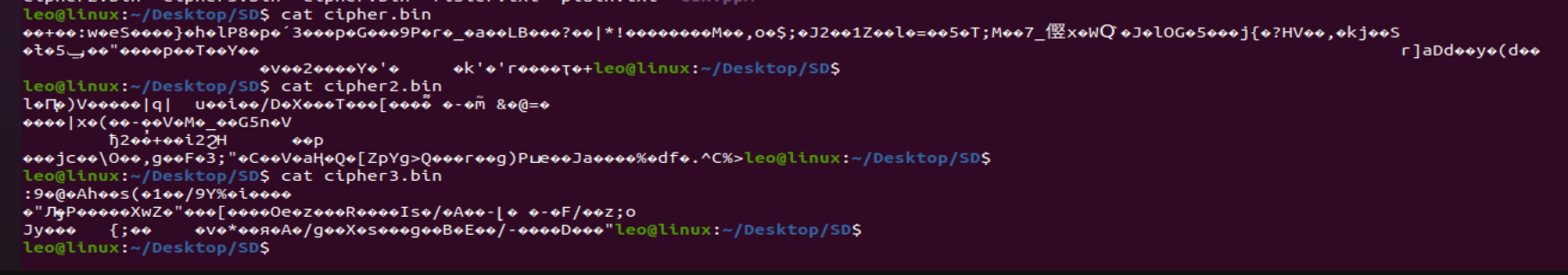


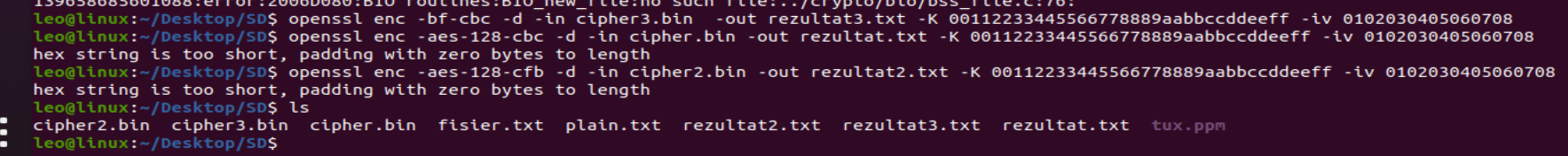
2. La această activitate se vor testa diverşi algoritmi de criptare şi moduri de cifrare. Pentru a cripta/decripta un fişier puteţi folosi următoarea comandă *openssl enc.* Pentru a consulta paginile de manual tastaţi *man openssl* şi *man enc*.  
Creaţi un fişier text care are o dimensiune de cel puţin 64 de octeţi  
***openssl enc ciphertype -e -in plain.txt -out cipher.bin -K 00112233445566778889aabbccddeeff -iv 0102030405060708***Înlocuiţi *ciphertype* cu un tip specific de cifru cum ar fi*–aes-128-cbc*, *aes-128- cfb*, *bf-cbc*, etc. Semnificaţia opţiunilor din linia de comandă precum şi cifrurile suportate pot fi aflate tastând man enc. În continuare sunt prezentate o serie de opţiuni folosite frecvent cu comanda*openssl enc*:

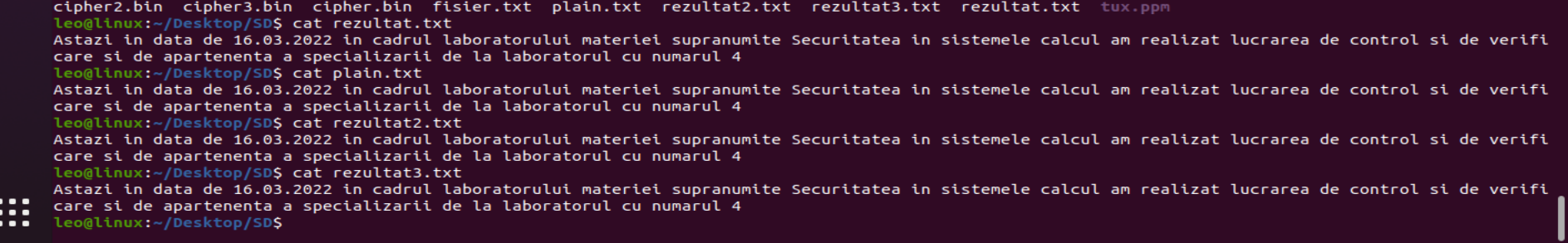
La această activitate trebuie să criptati cel puţin 3 cifruri şi 3 moduri de cifrare diferite. Schimbati numele output-ului astfel incat sa aveti fisiere diferite pentru fiecare metoda de criptare. (Puteti folosi aes-cbc aes-ecb, aes-cfb, aes-ofb)



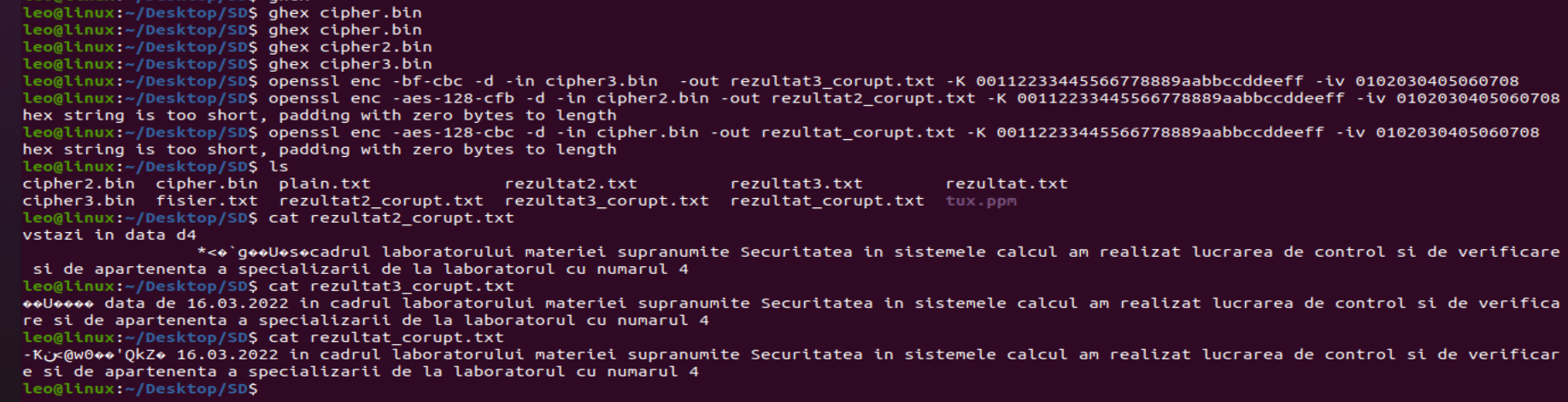
3.  Folosind comanda *cat,*vizualizati continutul fisierelor criptate.Decriptati fisierele criptate mai sus si verificati continul lor.



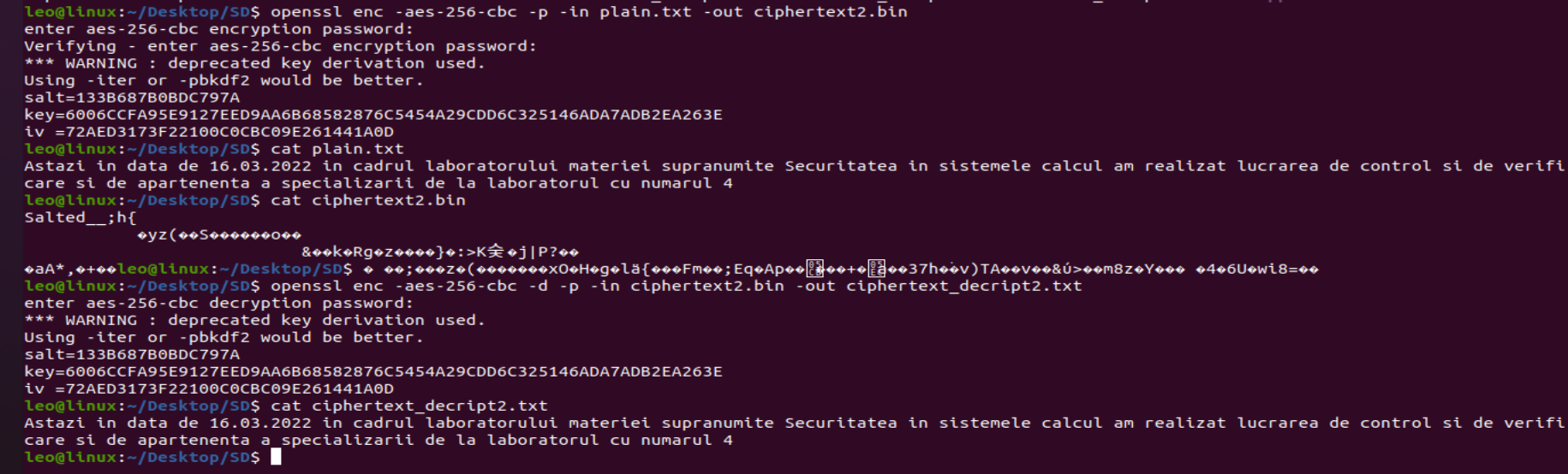




4. Pentru fiecare fisier rezultat prin criptarea modurilor de mai sus, folosind *ghex* modificati un singur bit din fisier. Decriptaţi fişierul corupt (criptat) folosind chei şi vectorul de iniţializare corecte. Decriptati fiecare fisier corup. Câtă informaţie puteţi recupera după decriptarea fişierului corupt, dacă modul de criptare este (a) EBC, (b) CBC, (c) CFB şi (d) OFB?



5. Criptati si decriptati un fisier folosind modul interactiv de introducere al parolei. Eliminati *-k* si *-iv* si folositi *-p  
openssl enc -aes-256-cbc -p -in plaintext.txt -out ciphertext.bin*



6. Folosind *gimp,*deschideti fisierul [tux](https://elearning.unitbv.ro/mod/resource/view.php?id=95734).ppm incarcat in acest laborator.   
Separati headerul de body din [tux](https://elearning.unitbv.ro/mod/resource/view.php?id=95734).ppm: 

*head -n 3*[*tux*](https://elearning.unitbv.ro/mod/resource/view.php?id=95734)*.ppm* - vizualizare primele 3 linii din header

*head -n 3*[*Tux*](https://elearning.unitbv.ro/mod/resource/view.php?id=95734)*.ppm >*[*Tux*](https://elearning.unitbv.ro/mod/resource/view.php?id=95734)*.header*

             t*ail -n +4*[*Tux*](https://elearning.unitbv.ro/mod/resource/view.php?id=95734)*.ppm >*[*Tux*](https://elearning.unitbv.ro/mod/resource/view.php?id=95734)*.body -*de la linia 4 pana la final este body-ul imaginii

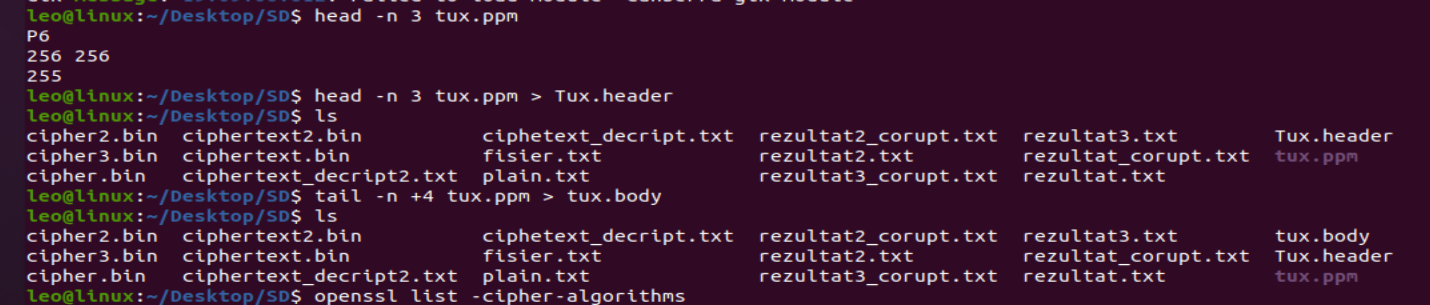
Criptati fisierul body folosind metoda ecb:

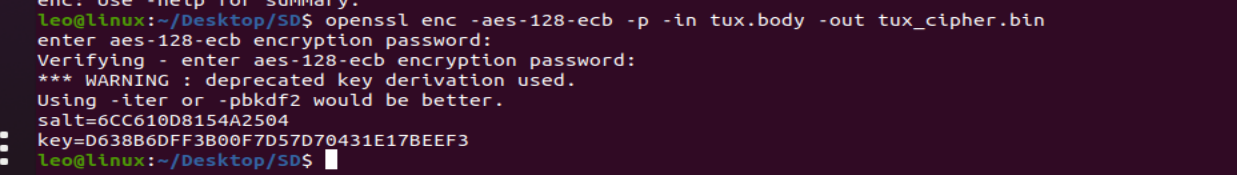
*openssl ...*

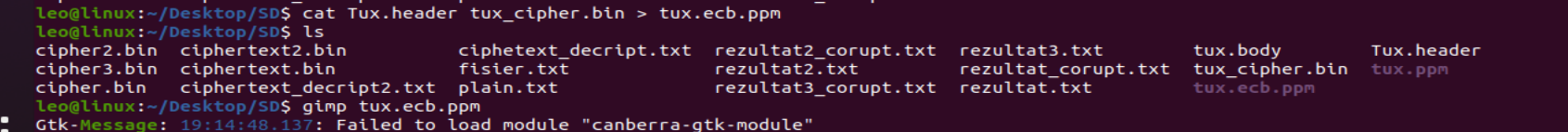
Folosind metoda *cat*, combinati fisierele header si body intr-un singur fisier.

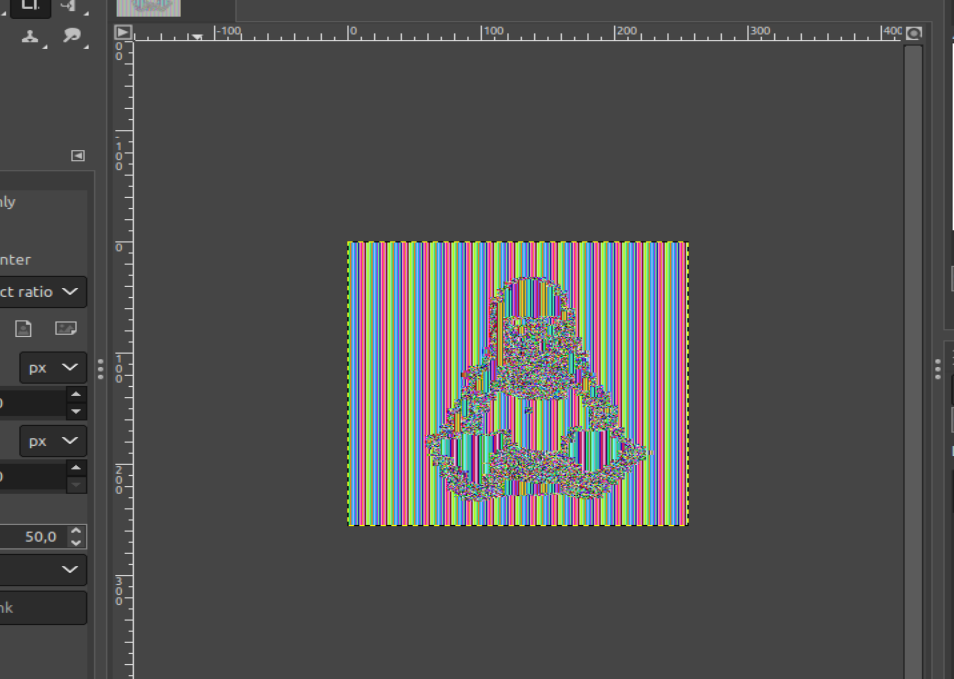
*cat*[*Tux*](https://elearning.unitbv.ro/mod/resource/view.php?id=95734)*.header*[*Tux*](https://elearning.unitbv.ro/mod/resource/view.php?id=95734)*.body.ecb >*[*Tux*](https://elearning.unitbv.ro/mod/resource/view.php?id=95734)*.ecb.ppm*

Folosind *gimp,*vizualizati fisierul nou rezultat ([*Tux*](https://elearning.unitbv.ro/mod/resource/view.php?id=78681)*.ecb.ppm =*headerul original + body-ul criptat). Ce observati comparativ cu imaginea originala?



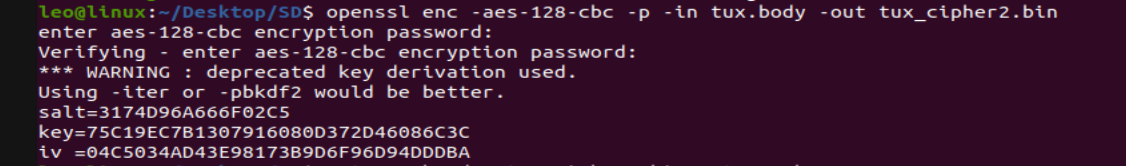






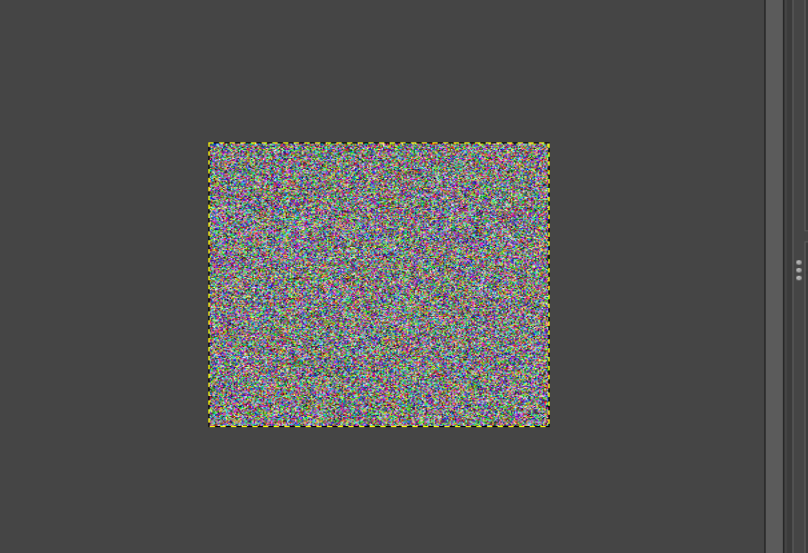
Imaginea nu este criptata in totalitate, chiar daca culorile au fost criptate, conturul imaginii inca se poate intelege.

7. Propuneti si testati un alt mod de criptare pentru a elimina problema modului *ecb*

**

**

**

**