CS 5158/6058 Data Security and Privacy, Fall 2022

Project 2: Symmetric-Key Encryption

Margi Amin M15219371

Software: Python 3.6.3 is required to run this if you're using Windows 10.

Program Location: ..\prp_m15219371\prp

Files and structure:

Files included in program:

-ciphertext.txt

-permutation.txt

- permutation.py

-prp.py

-prp_enc_dec .py

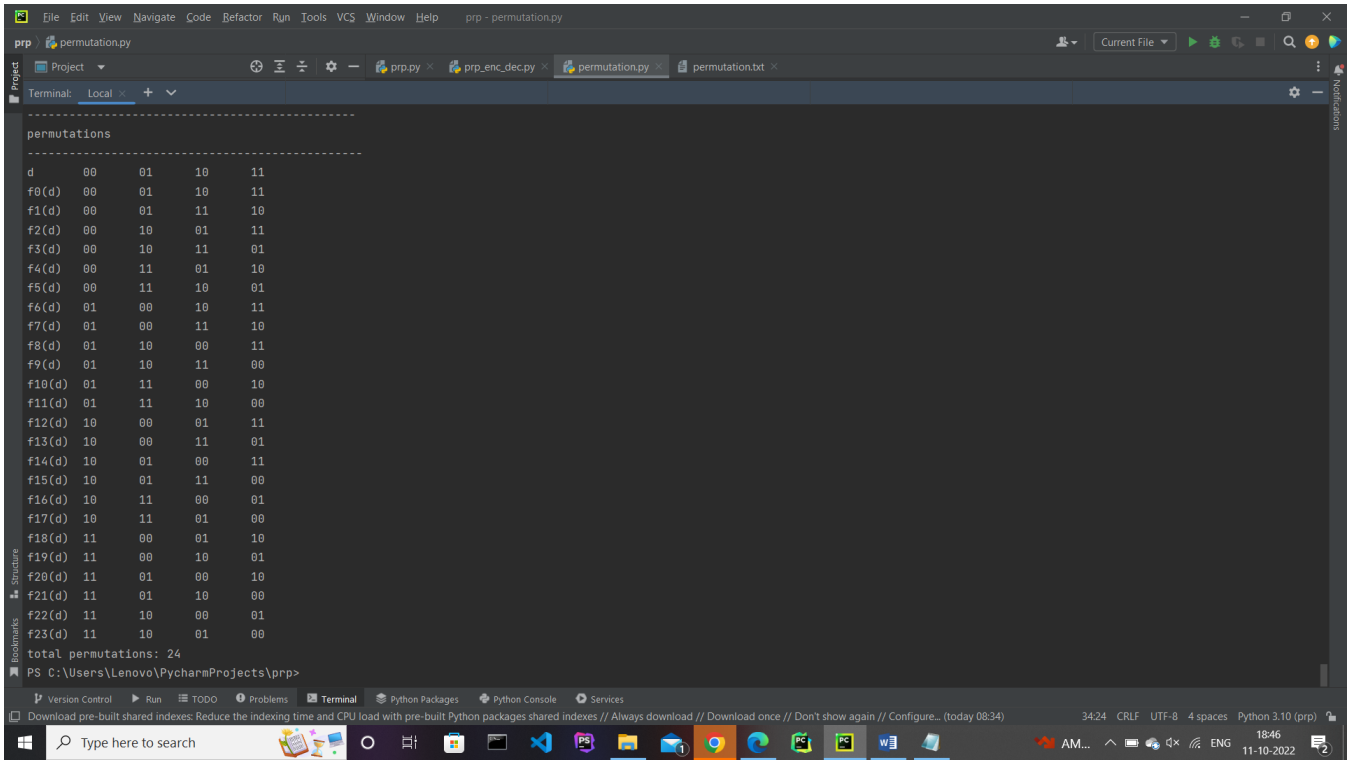
-PseudorandomPermutation.txt

Description:

a) **Permutation__Family function:**
This program generates all the permutation of permtation family *Perm(n,n)* and saves those in the file permutation.txt .

Command to run:
python permutation.py –permutegen n=2 permutation.txt

Output:
Here is screenshot of output of the permutationFamily function with input of n=2 . and it gives 24 permutation as req.



b) Pseudorandom permutation function:

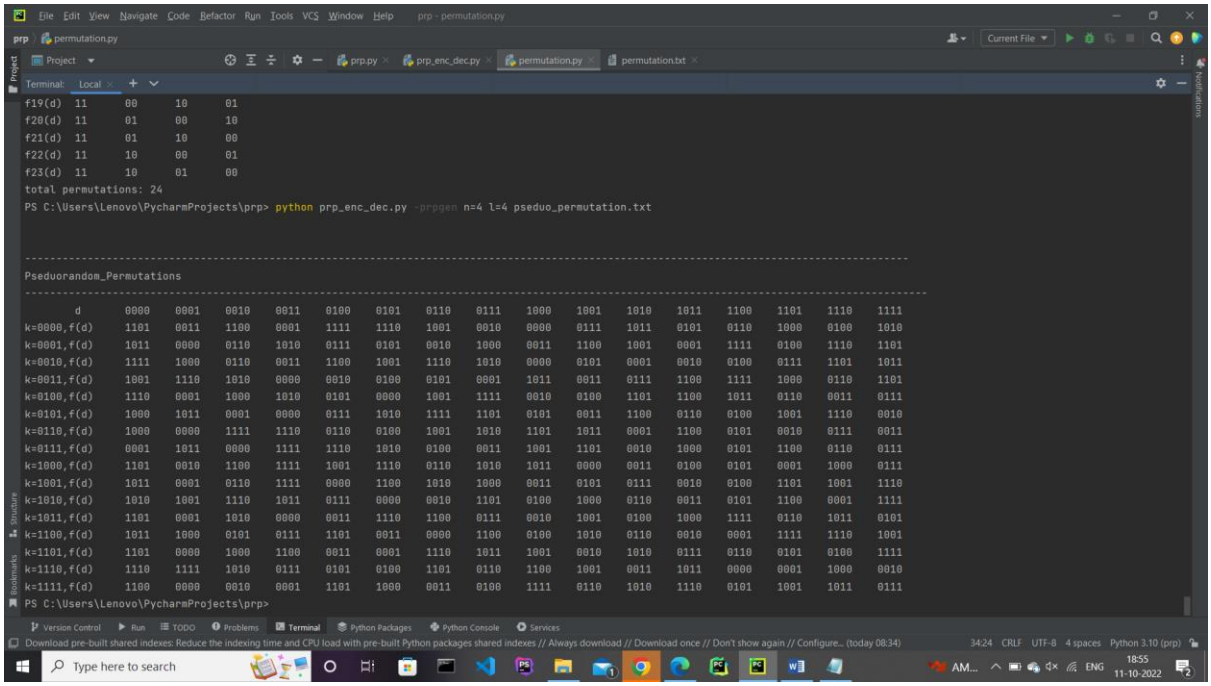
This program generate all the permutation included in psedorandom permutation F: K×D ->R . with parameter n and l . and saves the output in pseudo_permutation.txt file.

Command to run:

Python prp_enc_dec.py –prpgen n=4 l=4 pseduo_permutation.txt

Output:

Here is the screenshot of output where n=4 and l=4.

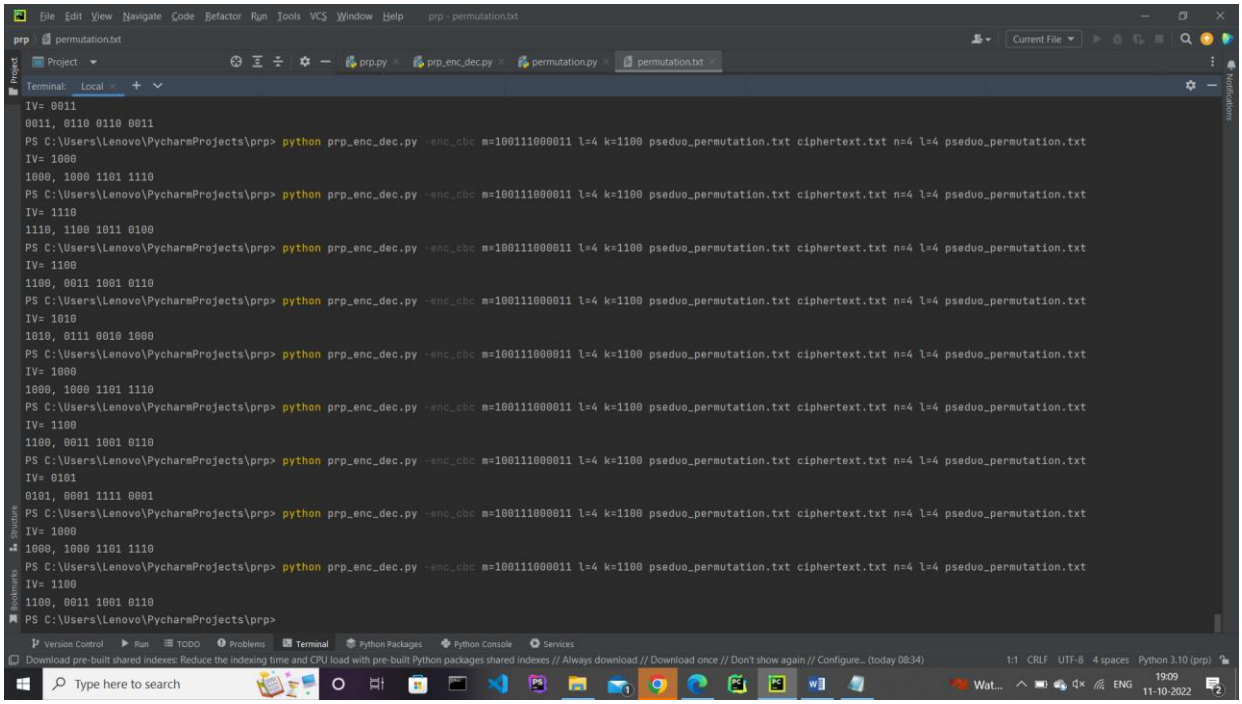


c) Encryption with block cipher CBC mode:

This function encrypt the message in CBC mode with 4-bit key , generate a 4-bit random IV and use prp and output ciphertext and saves in the ciphertext.txt file.

Command to run:
Python prp_enc_dec.py –enc_cbc m=100111000011 l=4 k=1100 pseduo_permutation.txt cipher.txt n=4 l=4 pseduo_permtation.txt

Output:
Here is screenshot of output with random Iv and different ciphertext every time.



d) Decryption with block cipher in CBC mode:

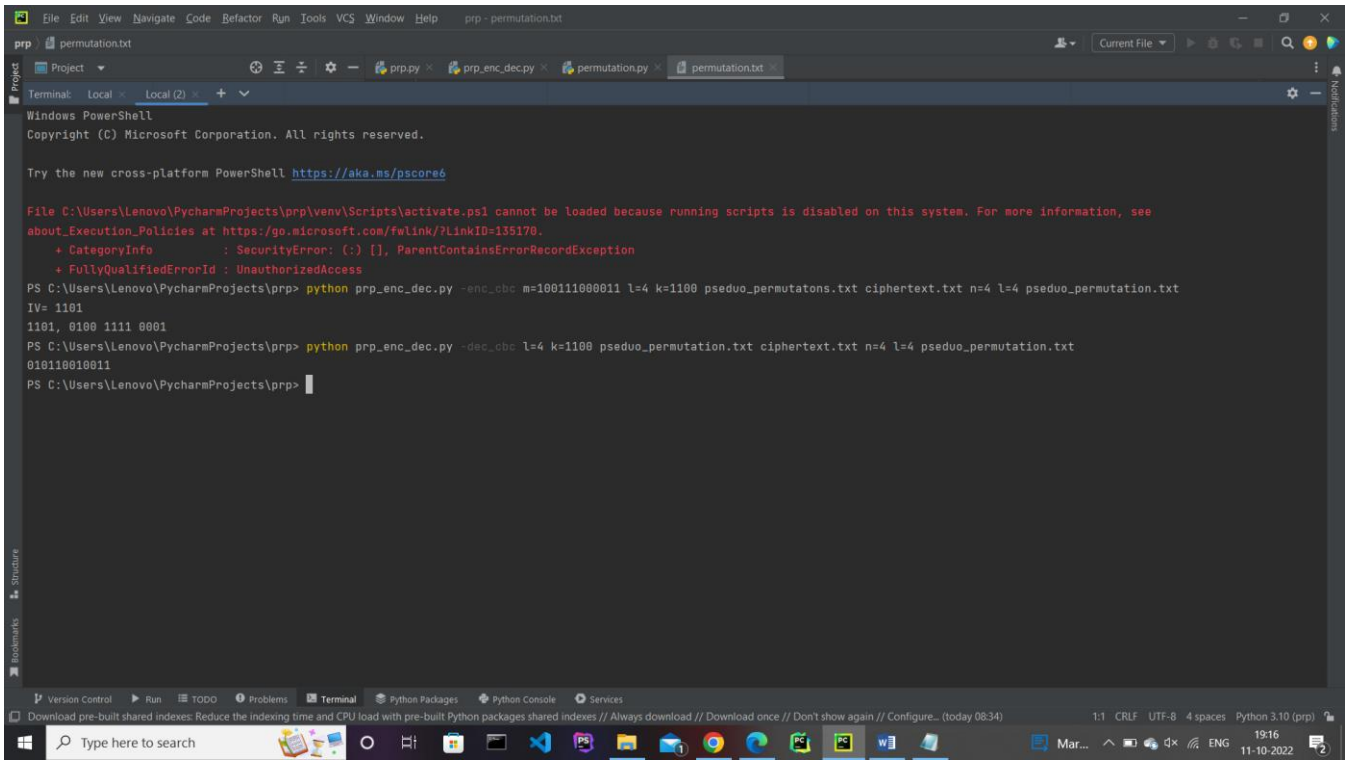
In this function cipher text in the cipher tcxt file Is decrypted with the given key and recovers the message and prints it in terminal.

Command to run:

Python prp_enc_dec.py –dec_cbc l=4 k=1100 pseduo_permutation.txt ciphertext.txt n=4 l=4 pseduo_permutation.txt

Output:

Here is the screenshot of output.

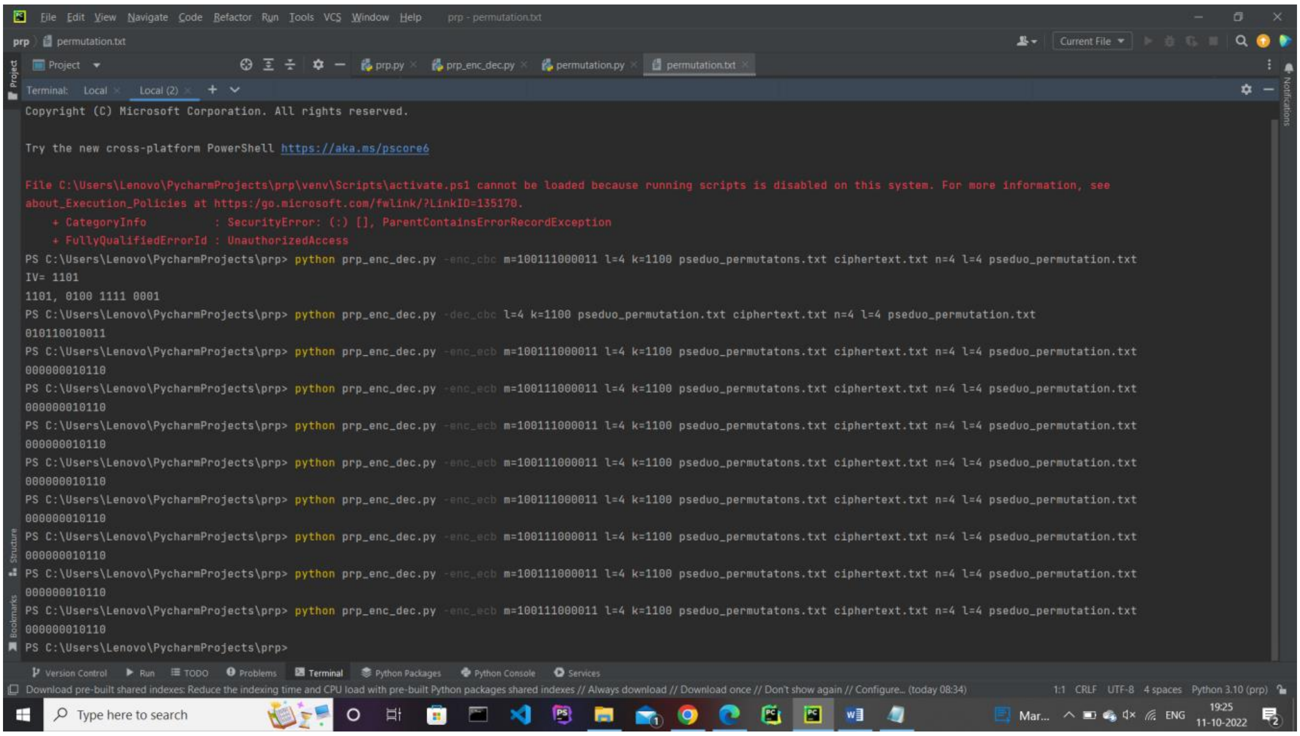


e) Encryption with block cipher in ECB mode:

This function encrypt the message in ECB mode with 4-bit key and use prp and output ciphertext and saves in the ciphertext.txt file.

Command to run:
Python prp_enc_dec.py –enc_ecb m=100111000011 l=4 k=1100 pseduo_permutation.txt cipher.txt n=4 l=4 pseduo_permtation.txt

Output:
Here is screenshot of output with same ciphertext every time.



```
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

File C:\Users\Lenovo\PycharmProjects\prp\venv\Scripts\activate.ps1 cannot be loaded because running scripts is disabled on this system. For more information, see
about_Execution_Policies at https:/go.microsoft.com/fwlink/?LinkID=135170.
    + CategoryInfo          : SecurityError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : UnauthorizedAccess
PS C:\Users\Lenovo\PycharmProjects\prp> python prp_enc_dec.py -enc_cbc m=100111000011 l=4 k=1100 pseduo_permutatons.txt ciphertext.txt n=4 l=4 pseduo_permutation.txt
IV= 1101
1101, 0100 1111 0001
PS C:\Users\Lenovo\PycharmProjects\prp> python prp_enc_dec.py -dec_cbc l=4 k=1100 pseduo_permutation.txt ciphertext.txt n=4 l=4 pseduo_permutation.txt
010110010011
PS C:\Users\Lenovo\PycharmProjects\prp> python prp_enc_dec.py -enc_ecb m=100111000011 l=4 k=1100 pseduo_permutatons.txt ciphertext.txt n=4 l=4 pseduo_permutation.txt
000000010110
PS C:\Users\Lenovo\PycharmProjects\prp> python prp_enc_dec.py -enc_ecb m=100111000011 l=4 k=1100 pseduo_permutatons.txt ciphertext.txt n=4 l=4 pseduo_permutation.txt
000000010110
PS C:\Users\Lenovo\PycharmProjects\prp> python prp_enc_dec.py -enc_ecb m=100111000011 l=4 k=1100 pseduo_permutatons.txt ciphertext.txt n=4 l=4 pseduo_permutation.txt
000000010110
PS C:\Users\Lenovo\PycharmProjects\prp> python prp_enc_dec.py -enc_ecb m=100111000011 l=4 k=1100 pseduo_permutatons.txt ciphertext.txt n=4 l=4 pseduo_permutation.txt
000000010110
PS C:\Users\Lenovo\PycharmProjects\prp> python prp_enc_dec.py -enc_ecb m=100111000011 l=4 k=1100 pseduo_permutatons.txt ciphertext.txt n=4 l=4 pseduo_permutation.txt
000000010110
PS C:\Users\Lenovo\PycharmProjects\prp> python prp_enc_dec.py -enc_ecb m=100111000011 l=4 k=1100 pseduo_permutatons.txt ciphertext.txt n=4 l=4 pseduo_permutation.txt
000000010110
PS C:\Users\Lenovo\PycharmProjects\prp> python prp_enc_dec.py -enc_ecb m=100111000011 l=4 k=1100 pseduo_permutatons.txt ciphertext.txt n=4 l=4 pseduo_permutation.txt
000000010110
PS C:\Users\Lenovo\PycharmProjects\prp> python prp_enc_dec.py -enc_ecb m=100111000011 l=4 k=1100 pseduo_permutatons.txt ciphertext.txt n=4 l=4 pseduo_permutation.txt
000000010110
PS C:\Users\Lenovo\PycharmProjects\prp>
```