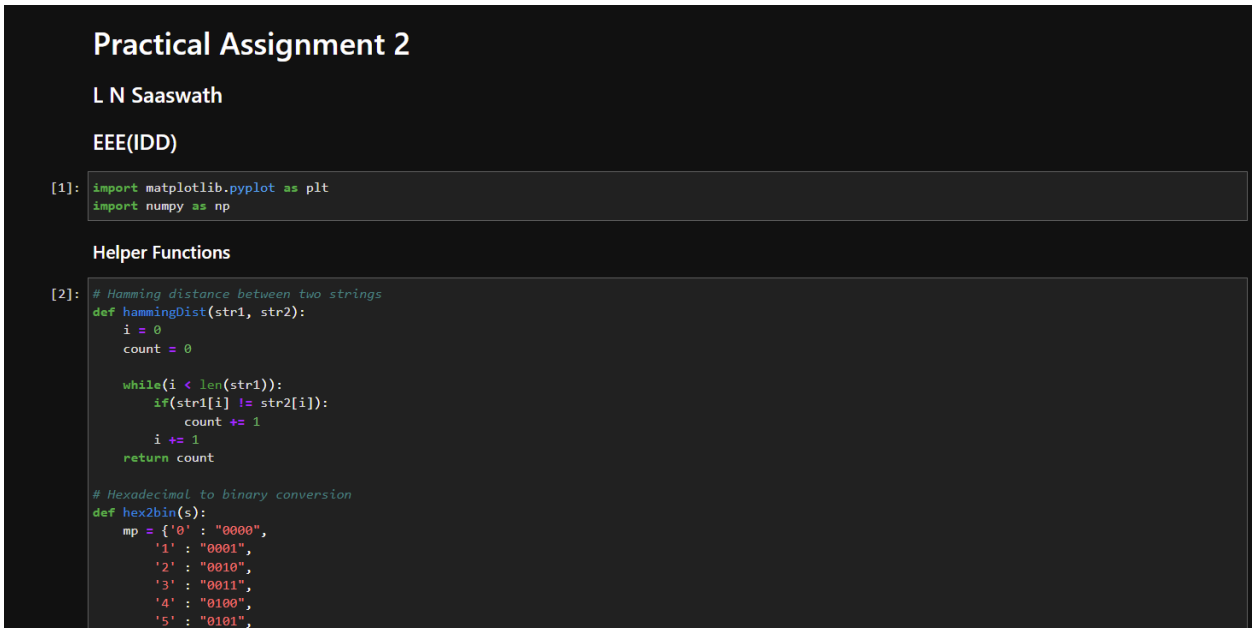
CS537

Practical Assignment 2

L N Saaswath, Part III - EEE



Practical Assignment 2

L N Saaswath

EEE(IDD)

[1]:
```
import matplotlib.pyplot as plt
import numpy as np
```

Helper Functions

[2]:
```
# Hamming distance between two strings
def hammingDist(str1, str2):
    i = 0
    count = 0

    while(i < len(str1)):
        if(str1[i] != str2[i]):
            count += 1
        i += 1
    return count

# Hexadecimal to binary conversion
def hex2bin(s):
    mp = {'0' : "0000",
        '1' : "0001",
        '2' : "0010",
        '3' : "0011",
        '4' : "0100",
        '5' : "0101",
```

Submission resources:

CS537 Assignments Repo

https://github.com/infini8-13/CS537-Network-Security

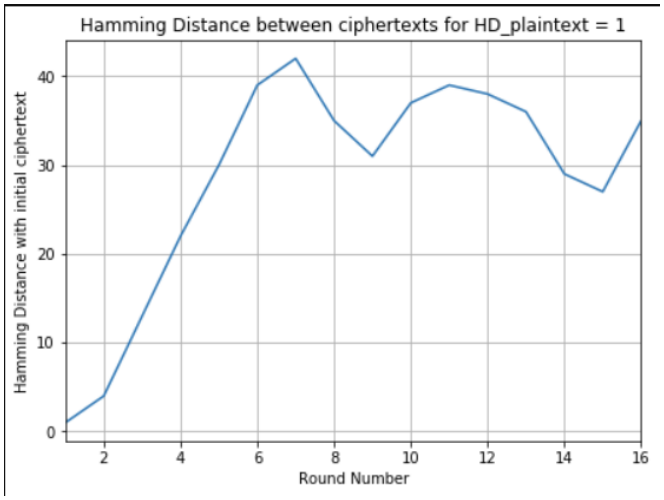
PA2 (current assignment)

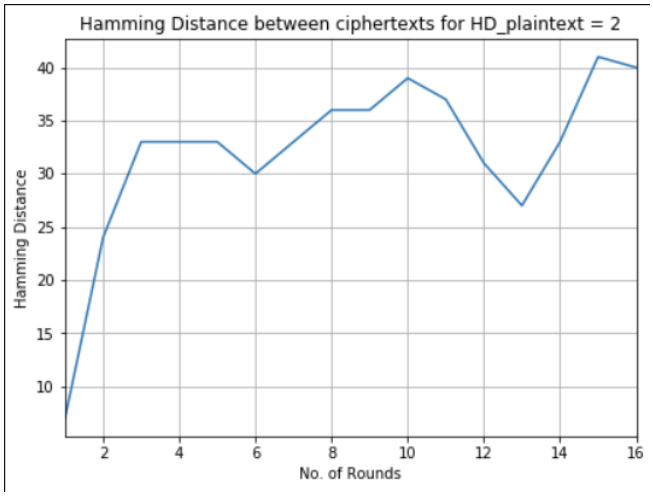
github.com/infini8-13/CS537-Network-Security/tree/main/Practical_Assignment_2

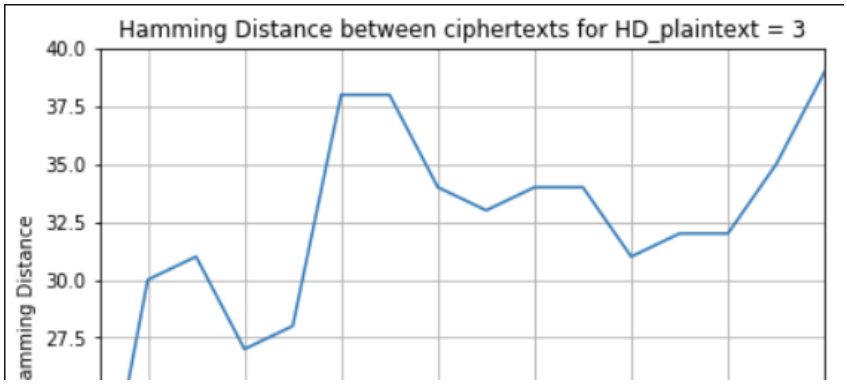
About - Experiments to explore the Avalanche Effect progression across the DES rounds. Use (i) 5 different plaintexts (ii) 5 different Hamming distances (HD) (iii) 5 different secret keys. Plotted Hamming Distances against the round number (Plots below).

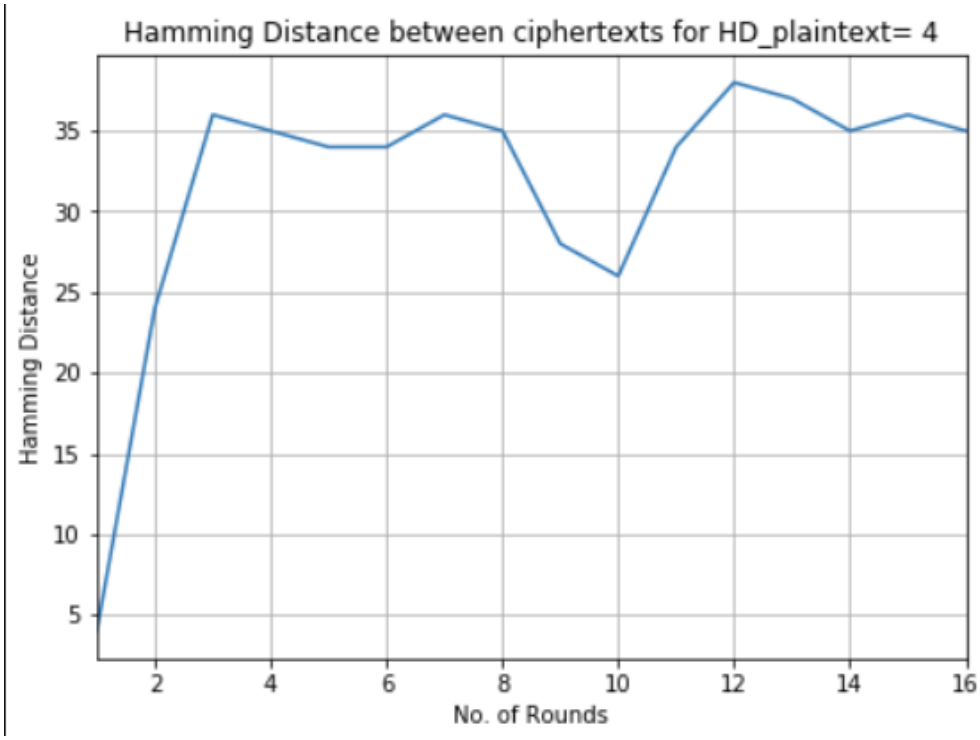
Plots:

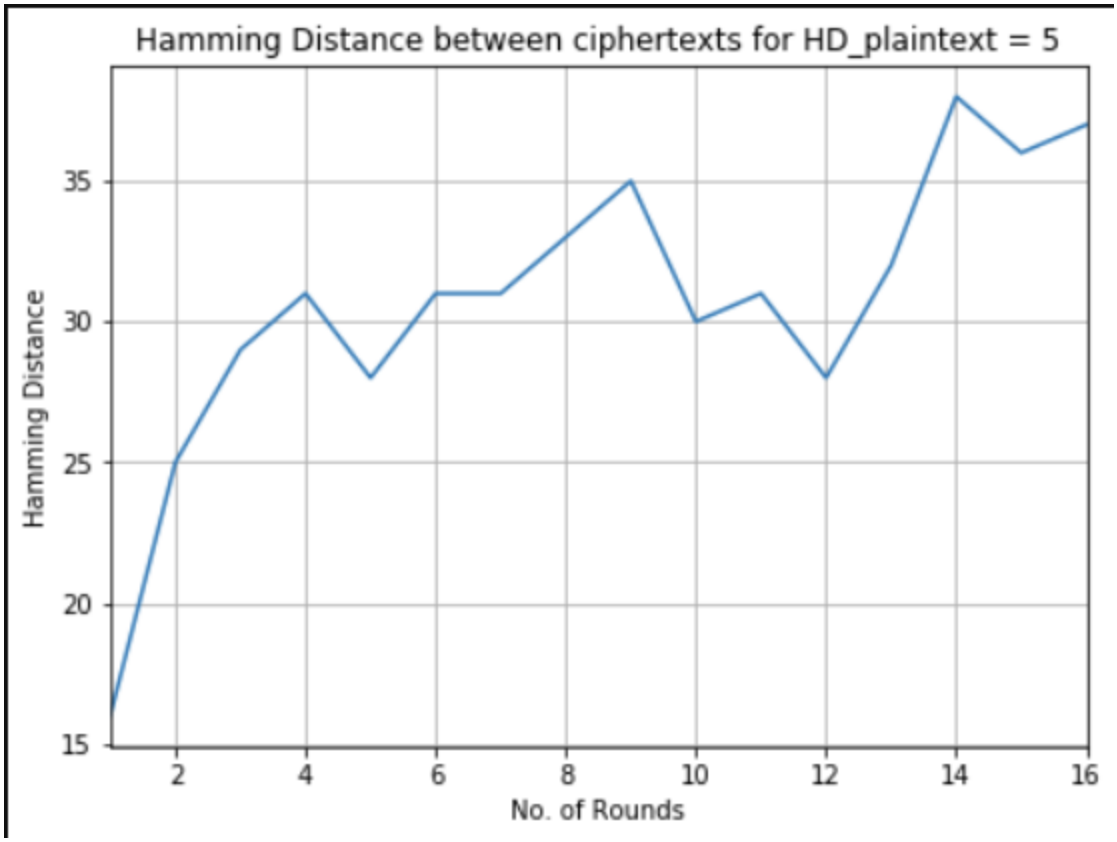
Plots obtained of Hamming Distances between ciphertexts for various Plaintexts:



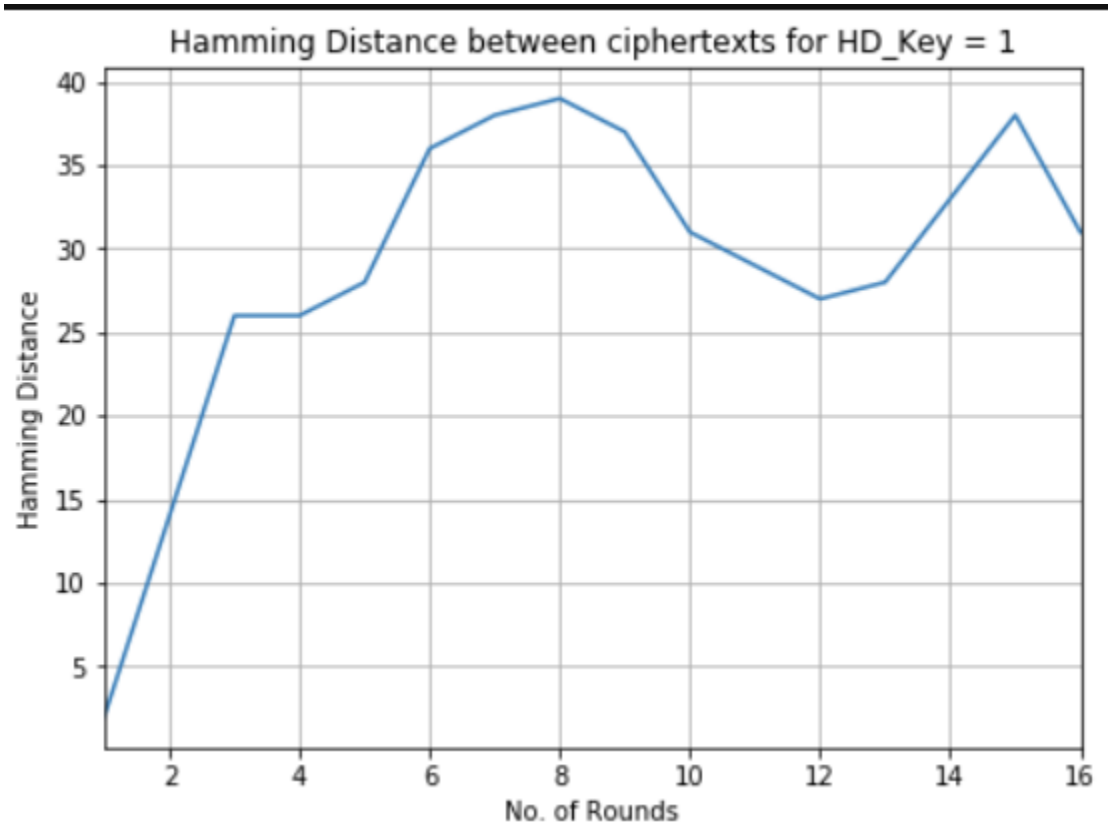


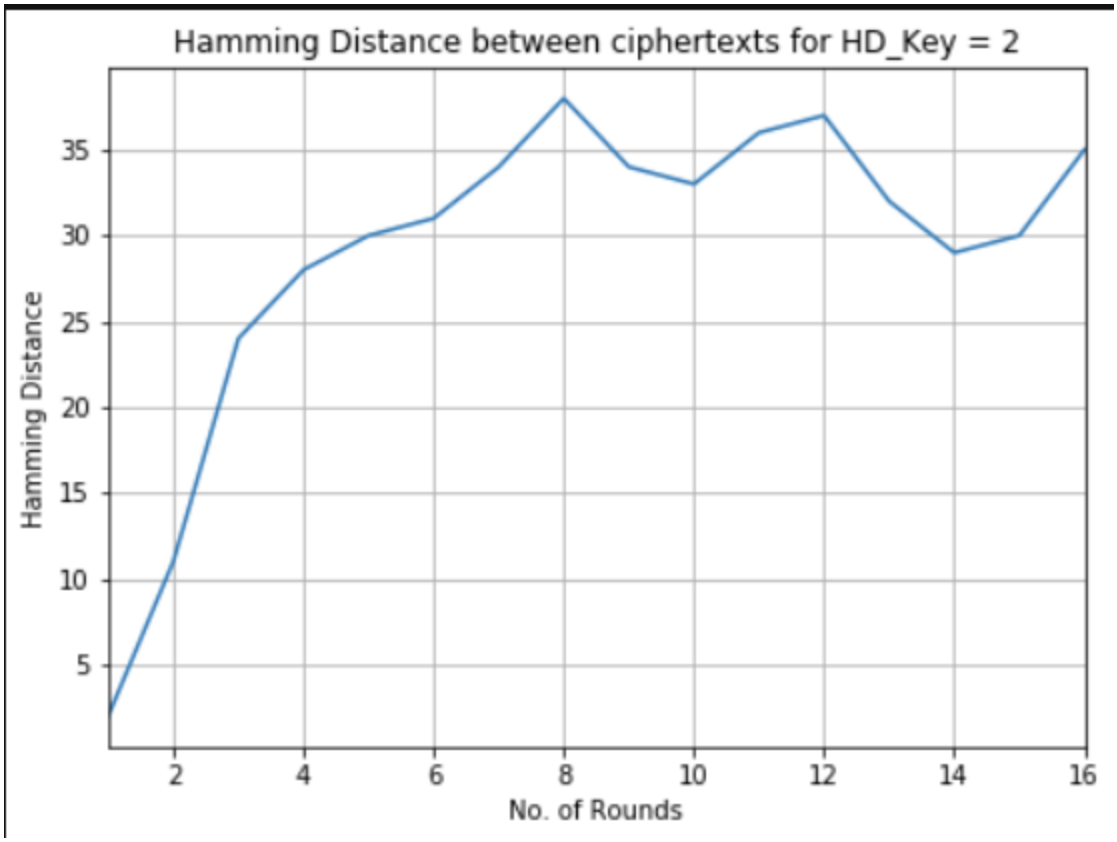


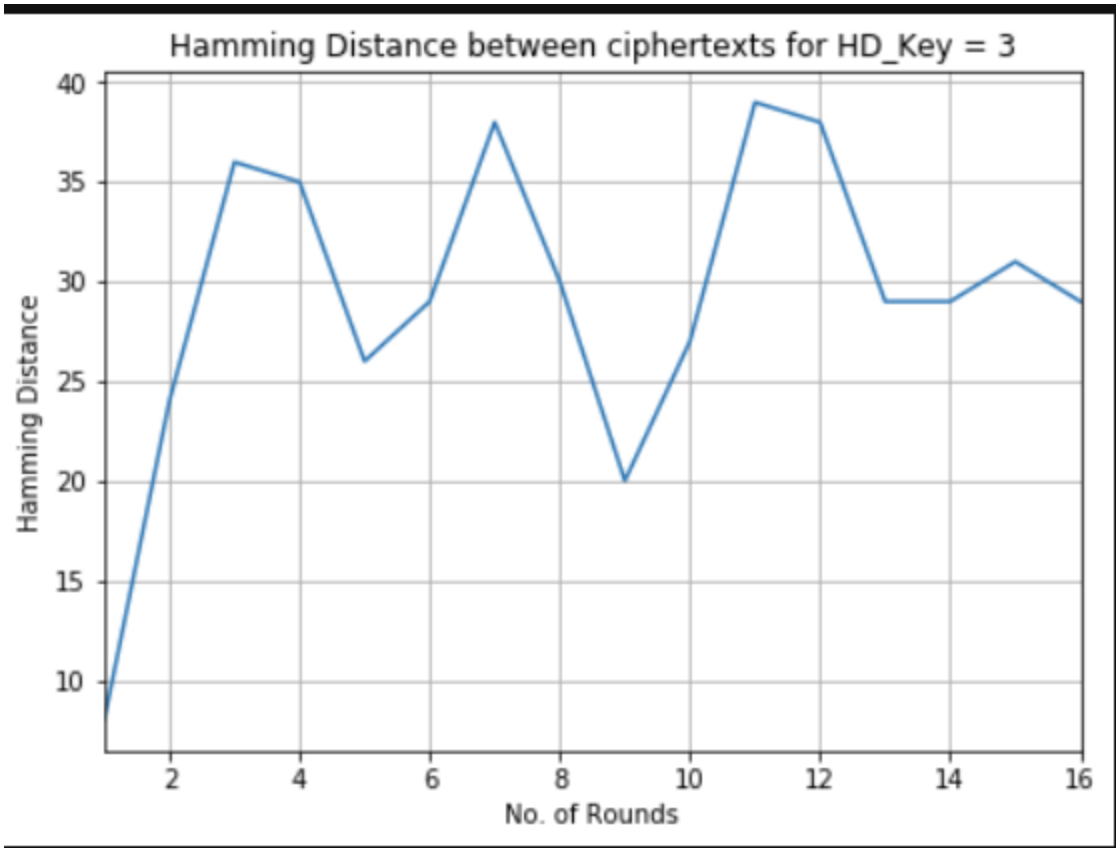

Hamming Distance between ciphertexts for HD_plaintext= 4
Hamming Distance
No. of Rounds
5
10
15
20
25
30
35
2
4
6
8
10
12
14
16

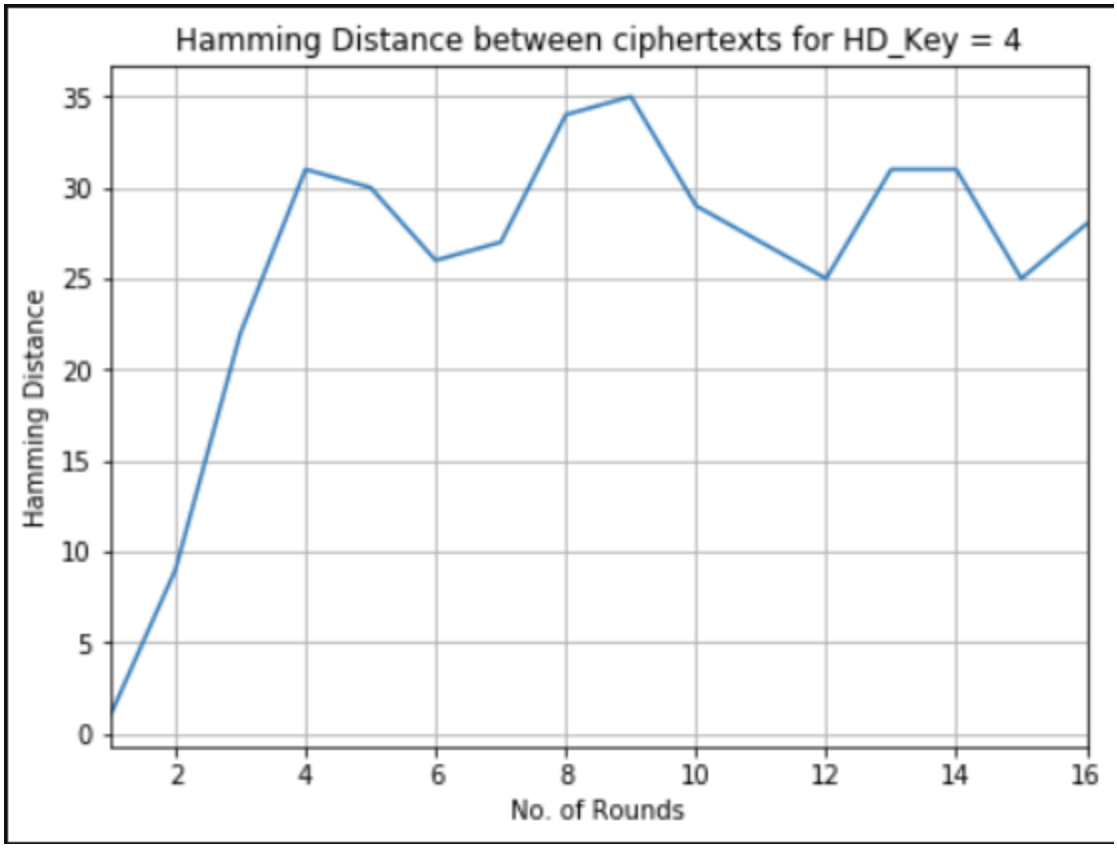

Hamming Distance between ciphertexts for HD_plaintext = 5
Hamming Distance
No. of Rounds
15
20
25
30
35
2
4
6
8
10
12
14
16

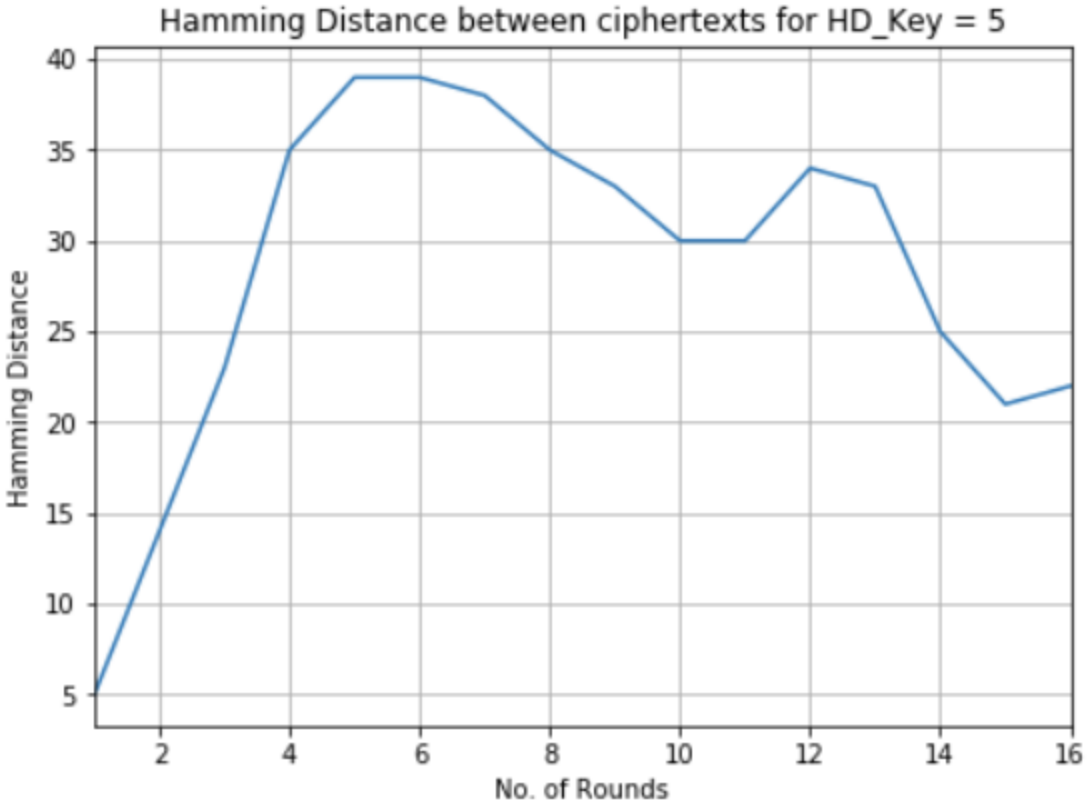
Plots obtained of Hamming Distances between ciphertexts for various keys:


Hamming Distance between ciphertexts for HD_Key = 1
Hamming Distance
No. of Rounds
40
35
30
25
20
15
10
5
2
4
6
8
10
12
14
16

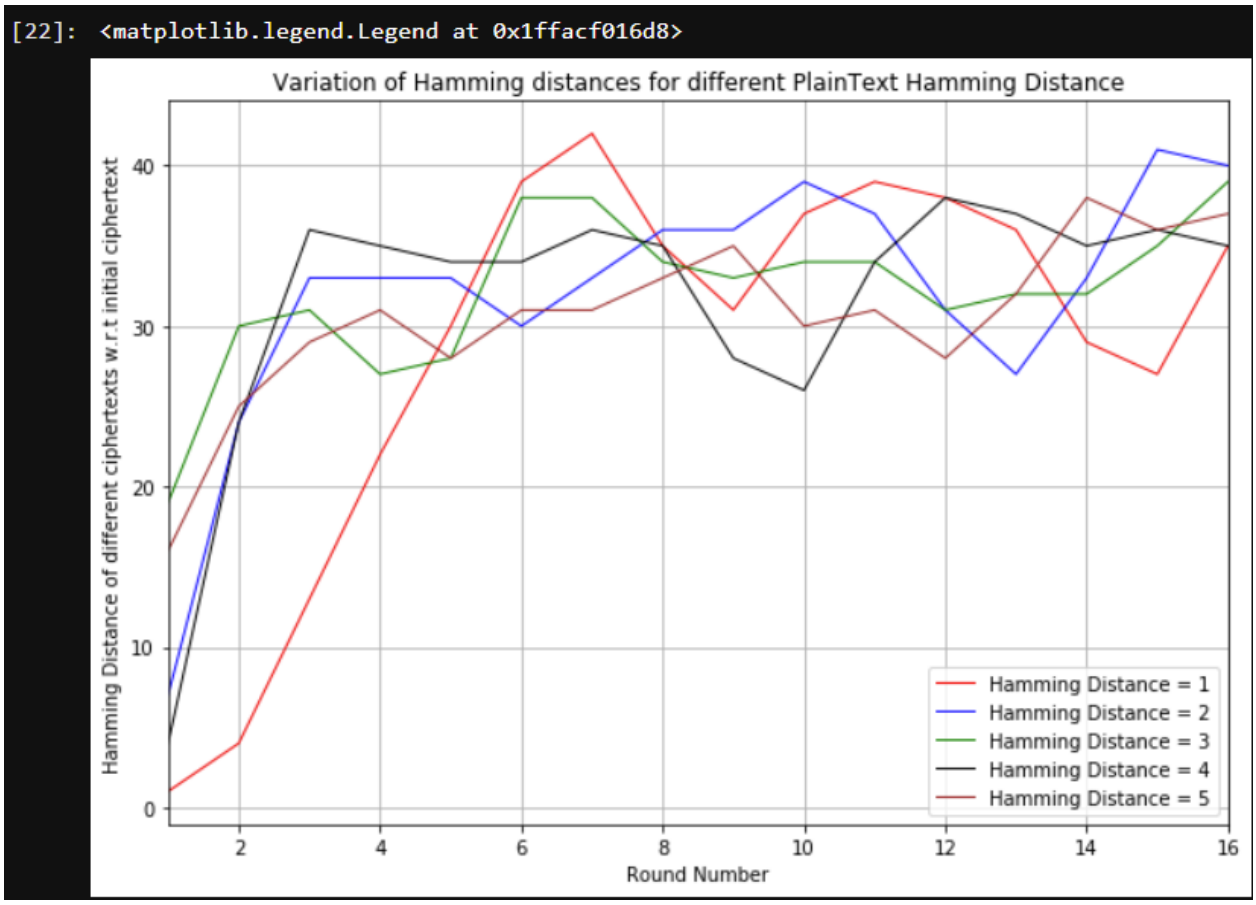

Hamming Distance between ciphertexts for HD_Key = 2
Hamming Distance
No. of Rounds
5
10
15
20
25
30
35
2
4
6
8
10
12
14
16


Hamming Distance between ciphertexts for HD_Key = 3
Hamming Distance
No. of Rounds
40
35
30
25
20
15
10
2
4
6
8
10
12
14
16

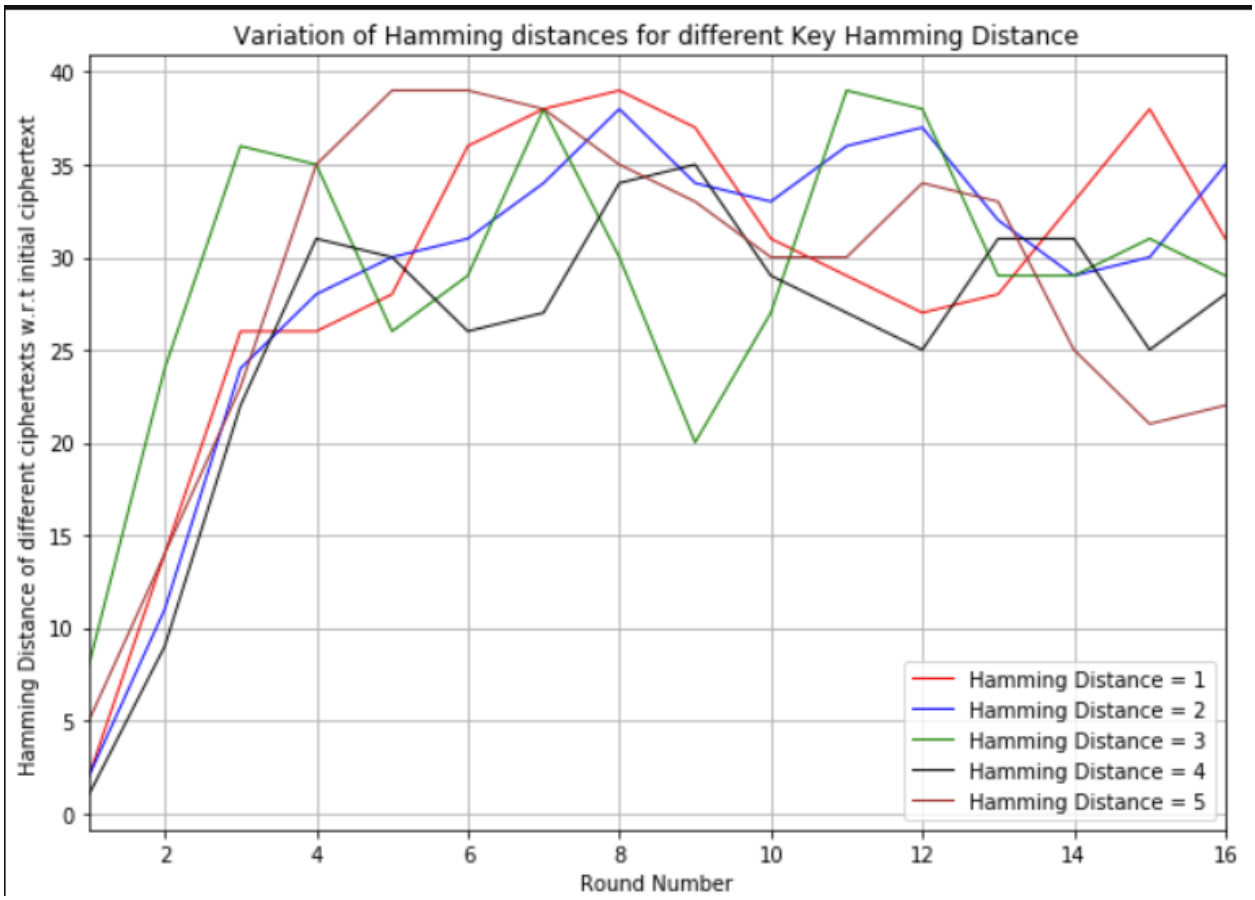

Hamming Distance between ciphertexts for HD_Key = 4
Hamming Distance
No. of Rounds
0
5
10
15
20
25
30
35
2
4
6
8
10
12
14
16


Hamming Distance between ciphertexts for HD_Key = 5
Hamming Distance
No. of Rounds
5
10
15
20
25
30
35
40
2
4
6
8
10
12
14
16

Changing Hamming Distance corresponding to Plaintext:



Changing Hamming Distance corresponding to Key:


Variation of Hamming distances for different Key Hamming Distance
Hamming Distance of different ciphertexts w.r.t initial ciphertext
Round Number
Hamming Distance = 1
Hamming Distance = 2
Hamming Distance = 3
Hamming Distance = 4
Hamming Distance = 5
0
5
10
15
20
25
30
35
40
2
4
6
8
10
12
14
16