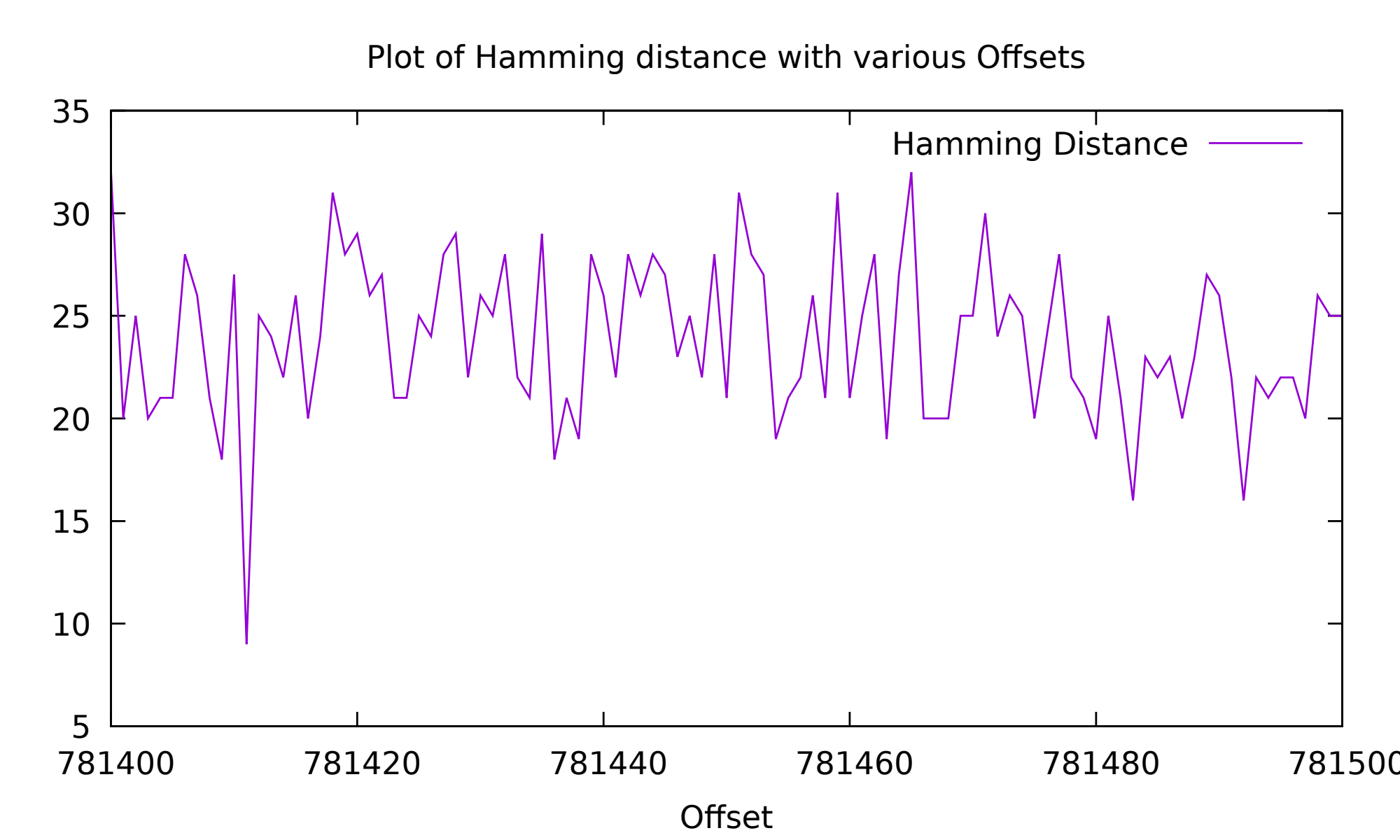
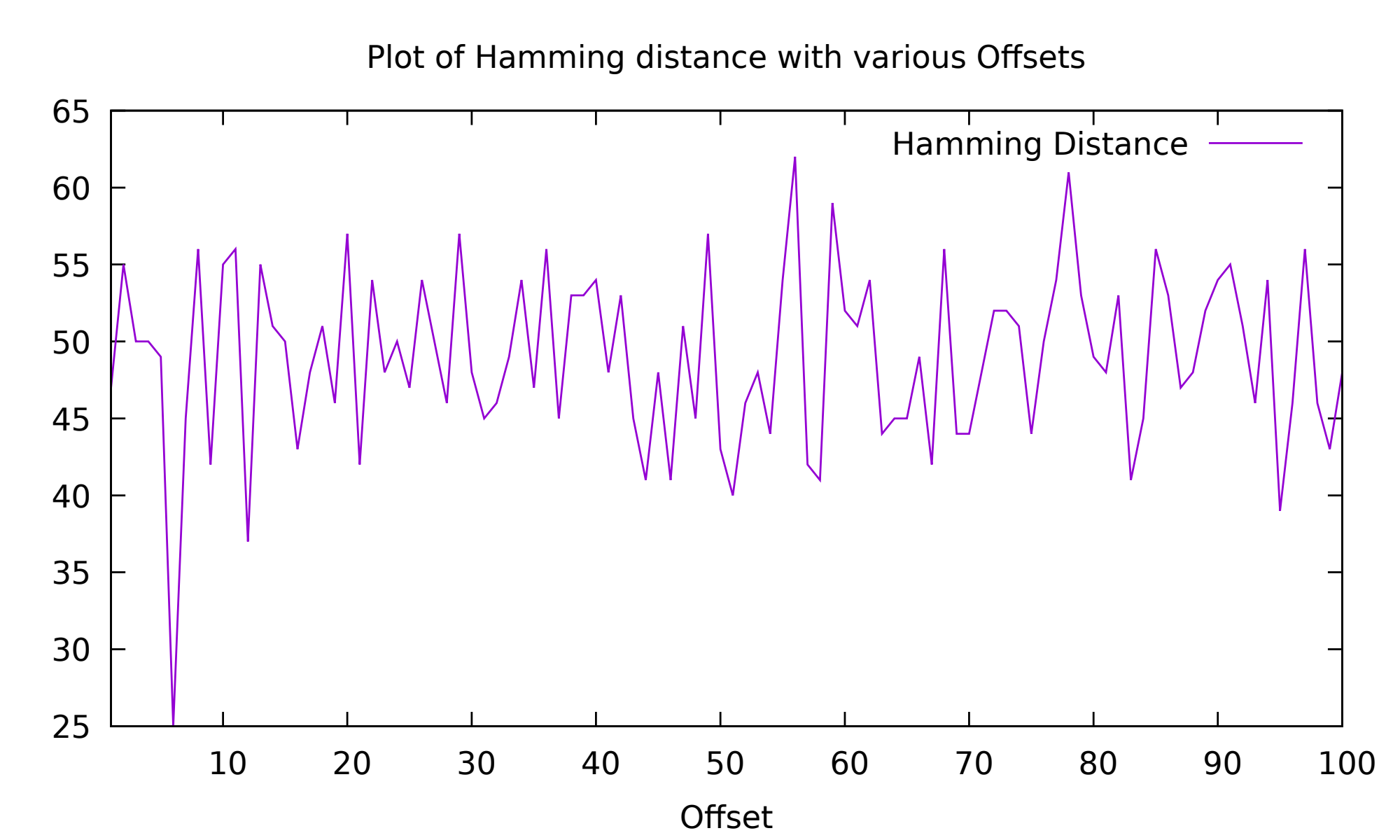
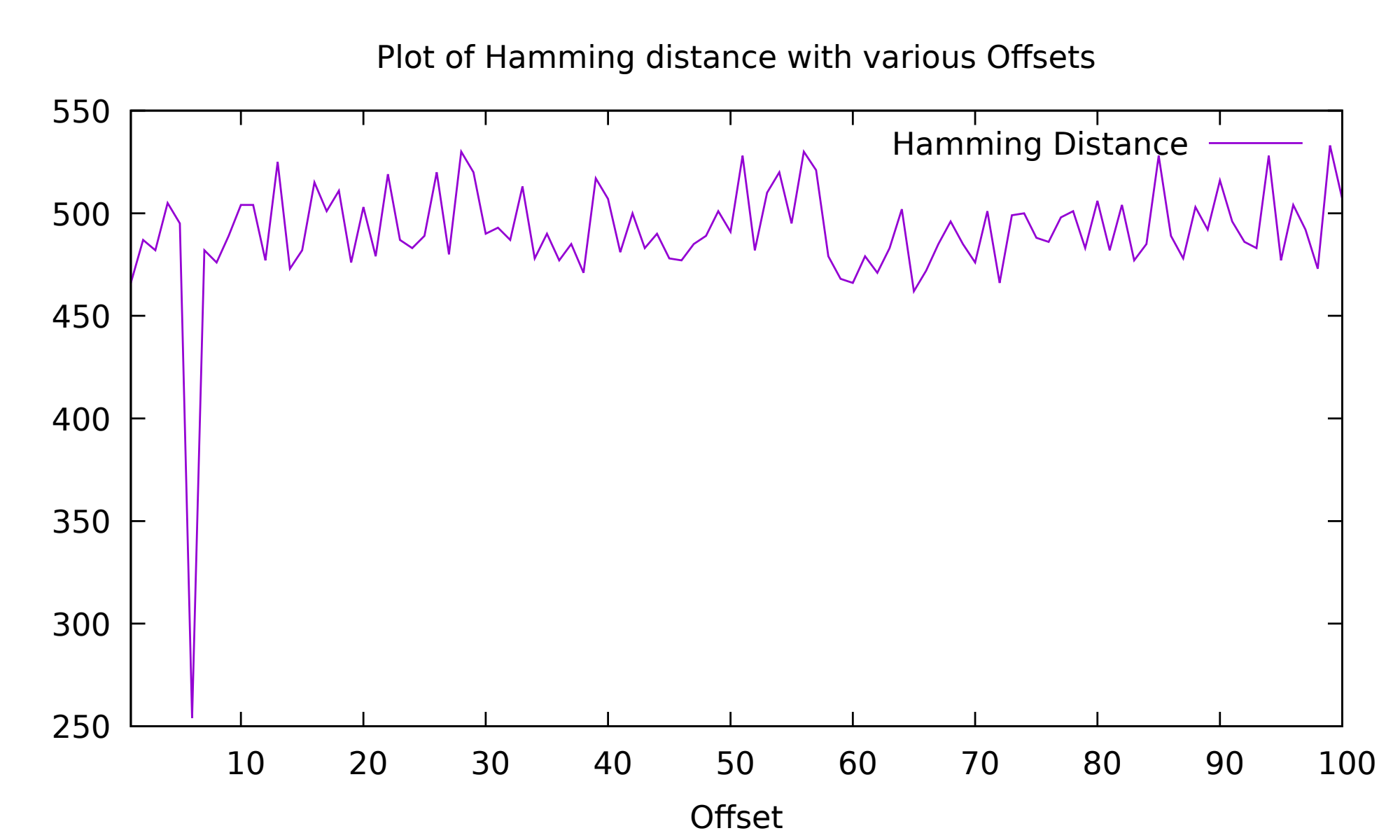
Report of Assignment: Hamming Distance

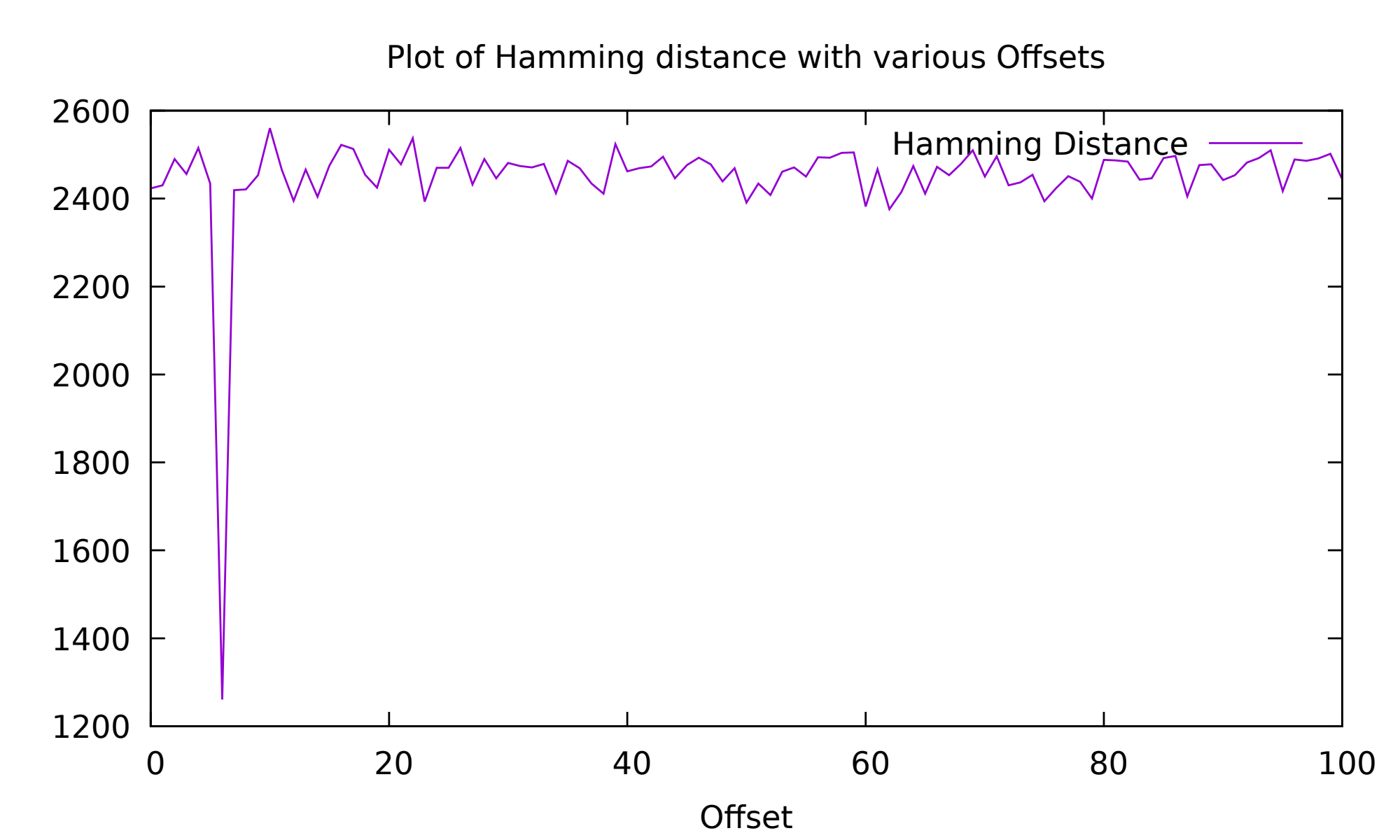
Done by Group 2A: Santosh, Gagan Deep, Manikandan

- The initial bitstream is generated based on the input of number of bits from the user. It is generated randomly using the rand() function as rand()%2 gives a value of 0 or 1.
- Now to randomly pick up the locations and bit values, a number is being generated between 0 and 1; if that number turns out to be less the fraction of bits to be picked up, that bit/character is selected into the next array. Since the rand() function generates numbers with equal probability, the number of values picked up are approximately the fraction required i.e., if 100 numbers are generated between 0 and 1, nearly 25 of them will be less than 0.25.
- From the input taken on the fraction of the bitstream that is to be revealed, we calculate the hamming distance (or the number of bits that are different) using **XOR** operator (bit operator).
- We find the offset by using the minimum hamming distance and **plotting the graph** of hamming distance vs offsets.
- The following are results to show that as the fraction of the bits revealed increases the accuracy of prediction increases.
- The following is the graph generated for the inputs: N = 1000000, Fraction of values picked = 0.1, Fraction of values that have an error = 0.25 and the Fraction revealed to Alice = 0.2
- **Disclaimer** : The values generated are random, this graph might not be generated again for the same set of inputs.


Plot of Hamming distance with various Offsets
Hamming Distance
35
30
25
20
15
10
5
781400
781420
781440
781460
781480
781500
Offset


Plot of Hamming distance with various Offsets
Hamming Distance
65
60
55
50
45
40
35
30
25
10
20
30
40
50
60
70
80
90
100
Offset


Plot of Hamming distance with various Offsets
Hamming Distance
550
500
450
400
350
300
250
10
20
30
40
50
60
70
80
90
100
Offset


Plot of Hamming distance with various Offsets
Hamming Distance
2600
2400
2200
2000
1800
1600
1400
1200
0
20
40
60
80
100
Offset