Problem2

Method :

1. Use SHA-3 (256 bits) to generate hash code, later used d bits (MSB) for d-bit hash code.
2. Generate random strings of n (10) length and compute hash code.
3. Check for string1 and string2 ,
   string1 != string2 and hashCode(string1) == hashCode(string2).
4. Calculate comparison,memory required to reach step.
5. To get average comparison and memory run the algorithm M (50) times.

Run Command : python birthdayattack.py

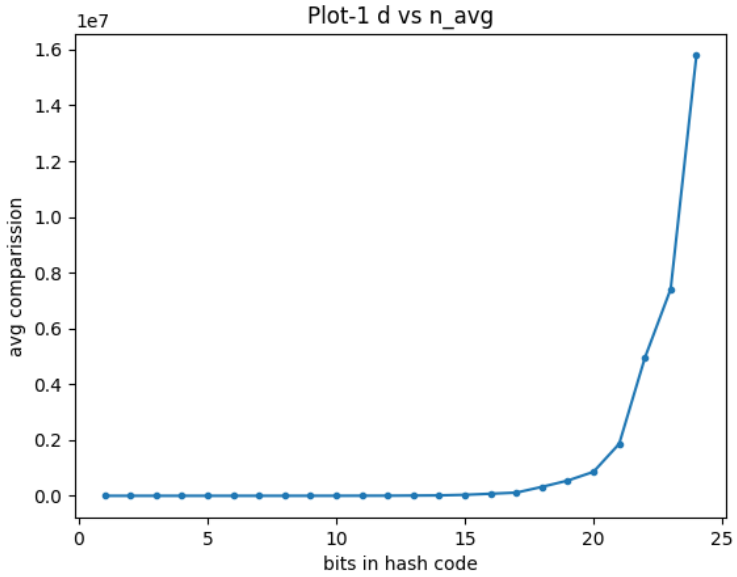
Output Window

```
(venv) C:\SEM2\NSS\problem_2>python birthdayAttack.py
Hash Bits, string1, string2, hashCode, Largest Memory in Bits, comparission
1       ('tfnqnudygq', 'qffcdbyxnt', '1', 2, 2)
2       ('vyhhfefwtj', 'raorkinntj', '10', 4, 2)
3       ('proutoacwb', 'mbdfqgjgoo', '100', 12, 12)
4       ('sbqiqmtuzz', 'tepturbufs', '1000', 8, 2)
5       ('yoztsfposj', 'nxsocdwmon', '11101', 30, 30)
6       ('aexeigadtm', 'tzgoltrgjt', '110001', 42, 42)
7       ('fqkolxguio', 'undbrwdjfd', '1000011', 112, 240)
8       ('hvqtinhafk', 'fbbkdsugrg', '10010011', 216, 702)
9       ('uqyubnvuot', 'usapbogpis', '111010101', 135, 210)
10       ('apxqblxucd', 'jwkkuyqbxc', '1111100111', 60, 30)
11       ('sarclgeedv', 'qsbxnzfijm', '11000101010', 726, 4290)
12       ('pqkdkoubnz', 'xixvjmsrdb', '111010100110', 480, 1560)
13       ('rpidcjliuz', 'ivqbwzkwnm', '1011110101000', 1144, 7656)
14       ('vertoasdpk', 'iqlbiriqgh', '11111011000111', 1736, 15252)
15       ('criloawygq', 'xogwfzuxap', '100110010111101', 1410, 8742)
16       ('ztdqczeabf', 'rklehjvloq', '1011001010001110', 1888, 13806)
17       ('xfptgqdclo', 'vdiyhaqyou', '10010001010001010', 6188, 132132)
18       ('flhypzbfbp', 'cfpvtdwkgg', '100111110001101111', 4392, 59292)
19       ('wszkkwotzo', 'aeguihrpnq', '1101100001110010100', 11837, 387506)
20       ('eqoolubfeh', 'ahrywnxzcf', '10010111000100100111', 27060, 1829256)
21       ('imbxasnhcv', 'xucbwsstii', '101011111010101001011', 11340, 291060)
22       ('ukatgikako', 'lhkcxmlkvo', '1110011101111000000101', 68728, 9756252)
23       ('bsrfqpdlsm', 'hkmzfauokp', '10011000000110110000011', 80017, 12099962)
24       ('ocyqckhpnu', 'nqhnasdclt', '10011010000011001011111', 63912, 7088906)
```

Observation :

The Average memory and average comparisons increases with number of hash bits.
The behavior can be observed in below graphs.

Plot : Bits Vs Average Comparison



Plot : Bits Vs Average Memory