asg2

February 1, 2023

0.0.1 Import library

[ ]:
```
import pandas as pd
```

0.0.2 01FFx.txt decode

[ ]:
```
df01 = pd.read_csv("assign2_data/01FFx.txt", sep="\t", header=None)
df01.columns = ["IV", "c[0]"]
```

[ ]:
```
df01["x"] = [int(x[-2:], 16) for x in df01["IV"]]
df01["c"] = [int(x, 16) for x in df01["c[0]"]]
df01["m"] = [f'{i:x}' for i in df01["c"] ^ (df01["x"] + 2)]
```

[ ]:
```
df01.head()
```

[ ]:

	IV	c[0]	x	c	m
0	01FF00	22	0	34	20
1	01FF01	11	1	17	12
2	01FF02	41	2	65	45
3	01FF03	1c	3	28	19
4	01FF04	9c	4	156	9a

[ ]:
```
df01["m"].value_counts().nlargest(1)
```

[ ]:
```
45    46
Name: m, dtype: int64
```

Obtain m0

[ ]:
```
m0 = df01["m"].value_counts().idxmax()
m0
```

[ ]:
```
'45'
```

0.0.3 03FFx.txt decode

```
[ ]: df03 = pd.read_csv("assign2_data/03FFx.txt", sep="\t", header=None)
     df03.columns = ["IV", "c[0]"]
```

Try k0 = 0

```
[ ]: k0 = 0
```

```
[ ]: df03["c"] = [int(x, 16) for x in df03["c[0]"]]
     df03["x"] = [int(x[-2:], 16) for x in df03["IV"]]
```

Increase k0 by 1 until m0 matchs

```
[ ]: while (True):
         df03["m"] = [f'{i:x}' for i in df03["c"] ^ (df03["x"] + 6 + k0)]
         if df03["m"].value_counts().idxmax() == m0:
             break
         k0 += 1
```

```
[ ]: df03.head()
```

```
[ ]:        IV c[0]    c  x   m
     0  03FF00   a2  162  0  82
     1  03FF01   d7  215  1  f6
     2  03FF02   05    5  2  27
     3  03FF03   6a  106  3  49
     4  03FF04   4e   78  4  6a
```

```
[ ]: df03["m"].value_counts().nlargest(1)
```

```
[ ]: 45    18
     Name: m, dtype: int64
```

Obtain k0

```
[ ]: k0h = f'{k0:x}'
     k0h
```

```
[ ]: '1a'
```