MSIN-4212 Deciphering Bitcoin

Cryptography Assignment

Programming Exercise

Daniel Felipe Carrillo Vanegas – Cod. 201215750
Javier Peniche – Cod. 201716772

Universidad de los Andes Colombia | Departamento de Ingeniería de Sistemas y Computación

JUNE 2022

Next, tables containing inputs of size n will be presented, with the respective time it took for the brute force algorithm to find the original input.

Tables

Length = 2

RecoveredWord	Time (ms)
aaa	105
bbb	133
ccc	152
ddd	144
eee	213
fff	290
ggg	297
hhh	315
iii	327
jjj	352
Avg.	**2328**

Length = 3

RecoveredWord	Time (ms)
aaaa	674
bbbb	809
cccc	840
dddd	927
eeee	1094
ffff	1076
gggg	1040
hhhh	1097
iiii	1278
jjjj	1570
Avg.	**10405**

Length = 4

RecoveredWord	Time (ms)
aaaaa	3130
bbbbb	6407
ccccc	8953
ddddd	13244
eeeee	18624
fffff	15277
ggggg	16186
hhhhh	22012
iiiii	28565
jjjjj	31109
Avg.	**163507**

Length = 5

RecoveredWord	Time (ms)
aaaaa	3130
bbbbb	6407
ccccc	8953
ddddd	13244
eeeee	18624
fffff	15277
ggggg	16186
hhhhh	22012
iiiii	28565
jjjjj	31109
Avg.	**163507**

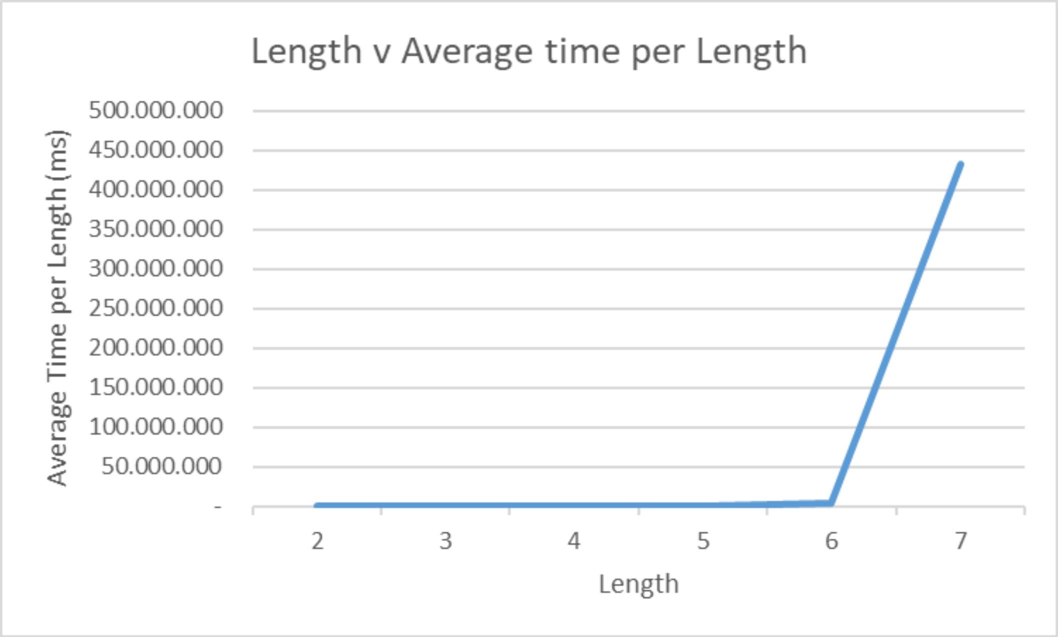
Length = 6

RecoveredWord	Time (ms)
aaaaaa	78300
bbbbbb	114867
cccccc	236785
dddddd	242876
eeeeee	322110
ffffff	355890
gggggg	428425
hhhhhh	498744
iiiiii	553096
jjjjjj	612007
Avg.	**3443100**

Length = 7

RecoveredWord	Time (ms)
aaaaaaa	1410304
bbbbbbb	3572780
ccccccc	7403012
ddddddd	12478956
eeeeeee	19982112
fffffff	35894470
ggggggg	48314405
hhhhhhh	66900456
iiiiiii	87736904
jjjjjjj	148709421
Avg.	**432402820**

Figure



To conclude, as can be seen in the graph, as we increase the size of the input for the realization of the dictionary attack (or brute force attack), the time it takes the program to find the input increases exponentially, so an attack of this style when the size of the original input is very high, it’s not really viable.

Used libraries

```
java.security.MessageDigest;
java.util.Scanner;
```

How to run the program

The program runs successfully with JavaSE-16 (jre). When running the program, it asks to enter a number by a console message to choose between the 2 possible operations that the program can execute

1 - > Get the Hash code of a message entered by parameter

2 - > Identify the original input

Remark: When importing the .java for the first time, make sure to correct the error resulting from the package name where the file is located.