Roopesh R SRN : PES1201802353

Rajat P Rayadurg SRN : PES1201802455

RABIN KARP STRING MATHCHER

RSA ENCRYPTION

Advanced Algorithms(UE18CS553)

8th May 2019

Overview

This document covers the implementation/design details, screenshots , statistics like timing, memory usage and finally it covers learning outcomes of this project.

System Specifications (On which the program was tested)

Model name:	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
CPU(s):	4
Architecture:	x86_64
CPU op-mode(s):	``32-bit, 64-bit
Byte Order:	Little Endian
CPU MHz:	1197.576
CPU max MHz:	3600.0000
CPU min MHz:	1200.0000

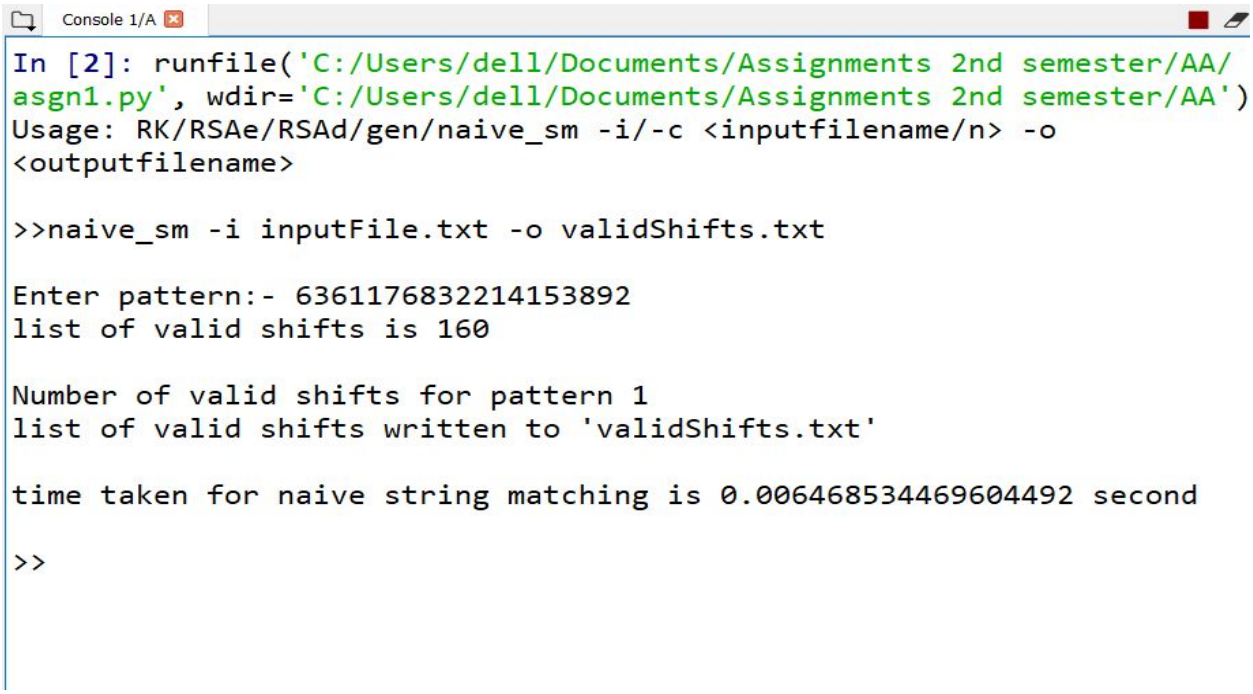
2

L1d cache:	32K
L1i cache:	32K
L2 cache:	256K
L3 cache:	4096K
Thread(s) per core:	2

Screenshot 1 : Rabin-karp pattern matching demo

```
In [4]: runfile('C:/Users/dell/Documents/Assignments 2nd semester/AA/asgn1.py', wdir='C:/Users/dell/Documents/
Assignments 2nd semester/AA')
Usage: RK/RSAe/RSAd/gen -i/-c <inputfilename/n> -o <outputfilename>

>>RK -i inputFile.txt -o validShifts.txt

Enter the pattern:- 6361176832214153892
Pattern P found at index 160
Number of valid shifts for pattern 1
list of valid shifts written to 'validShifts.txt'

time taken is 0.04592251777648926 second

>>RK -i sample.txt -o validShifts.txt
```

Screenshot 2: Comparison of Rabin-Karp with Naive String Matcher

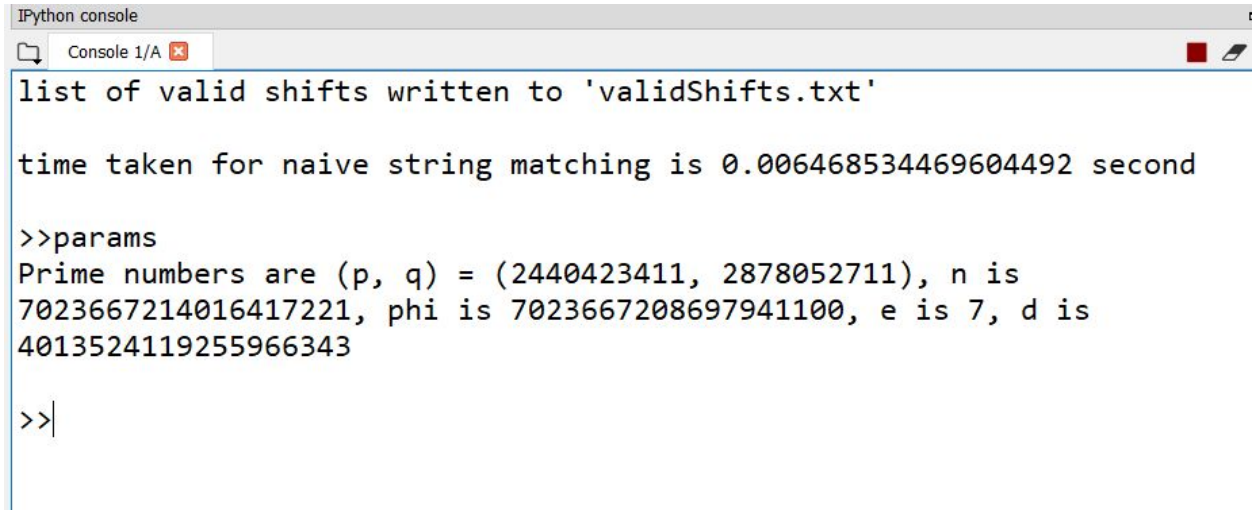


Screenshot3 : RSA Encryption-Decryption demo

```
>>RSAe -i inputFile.txt -o outputFile.txt
cipher text written to outputFile.txt
time taken is 1.3840913772583008 second

>>RSAd -i outputFile.txt -o outputConfirm.txt
decrypted msg stored in outputConfirm.txt
time taken is 0.1705915927886963 second

>>
```

Screenshot 4:- Input file,ciphertext,Decrypting the ciphertext

Screenshot 5:-Parameters used in RSA Encryption



Operations	Input Size	Timing
Rabin Karp	14981 words/101854 characters	0.047s
Naive String Matcher	14981 words/ 101854 characters	0.312s
RSA Encryption	5000 credit card numbers	1.378s
RSA Decryption	5000 encrypted credit card numbers	1.687s

Implementation Details

It is implemented in Python.

Learning Outcome

We learnt how to implement Rabin-Karp string matcher for Text search and also to implement RSA-Encryption with 32-bit primes for asymmetric encryption.

Comments About Assignment

Was a fun assignment, considering the fact that 2014-2018 was not as fun as this year.