

Криптографија - Домашна задача 1

Михајло Крагујевски

183002

Шифрирање на текст

Текстот кој што ќе го криптирам е:

*Кога се обидуваме да го решиме проблемот со компјутер или некое парче технологија за таа работа, првото нешто што треба да го направиме е да утврдиме дали проблемот е со хардверот или со софтверот. Како ќе ја направиме таа определба зависи од проблемот што го доживуваме, но честопати се подразбира исклучување на еден или на друг преку тестирање. Без оглед на тоа како ќе стигнете до тој одговор, јас често сум навистина изненаден за тоа колку голема конфузија е таму кога станува збор за хардверски софтвер. Уште полошо е кога споменувам *firmware*. Еве повеќе за тоа како секоја од овие "производи" се разликува, знаење кое треба да го имате ако планирате да направиме дури и наједноставно отстранување на проблеми на било кој од вашите огромен број на технолошки уреди: Хардверот е "вистински материјал" што можете да го видите со очите и со допир со вашите прсти. За жал, како физичка ствар, исто така, понекогаш може да ја мирисате како што умира огнена смрт, или да слушнете како што физички се распаѓа во последните последици. Бидејќи хардверот е дел од "вистинскиот" свет, сето тоа на крајот избледува. Како физичка работа, исто така е можно да се скрши, да се удави, прегрее, и на друг начин да се изложи на елементите. Вашиот паметен телефон е парче хардвер, иако исто така содржи софтвер и фирмвер (повеќе за оние подолу). Вашиот таблет, лаптоп или десктоп компјутер исто така е хардвер, и содржи многу индивидуални хардверски компоненти, исто така, како матична плоча, процесор, мемориски стапчиња и друго. Овој флеш диск во вашиот џеб е хардвер. Модемот и рутерот во плакарот дома се и парчиња хардвер. Иако тоа не е секогаш така лесно, со користење на едно од вашите пет сетила (освен вкус ... немојте да пробате некој дел од вашиот компјутерски систем) е често вашиот најдобар начин да се каже дали хардверот е причина за проблем. Дали е пушењето? Дали е разбиена? Дали недостасува парче? Ако е така, хардверот веројатно е извор на проблемот. Како чувствителна како што сум направил хардвер да биде во она што сте го прочитале, една голема работа за хардверот е тоа што обично може лесно да се смени. Софтверот што го изгуби може да биде незаменлив, но повеќето хардверски се "неми" - замена која често е исто толку вредна како и оригиналот. Погледнете ја мојата листа на компјутерски хардверски уреди за повеќе за некои од вообичаените делови на компјутерскиот систем и за што се користат. Софтверот е Виртуелен: може да се копира, измени и уништи. Софтверот е сè за вашиот компјутер што не е хардвер. Вашиот оперативен систем или апликација на вашиот паметен телефон, се софтверски. Бидејќи софтверот е информација, а не физичка работа, постојат неколку бариери за постоењето.*

Објаснување на програмата ClearedText.java:

Најпрво овој текст морав да го средам со тоа што ќе ги избришам празните места и специјалните карактери (-+*/()?! итн.) Напишав код во Java (ClearedText.java), кој што тоа ќе ми го прави, додека па оригиналниот текст го ставив во датотека Uncleared-Text.txt. Во кодот направив нова датотека Cleared-Text.txt и направив функција која ќе ми го зема текстот од Uncleared-Text.txt, со помош на regex ќе ги избришам специјалните карактери и празните места, па средениот текст сместен во еден String, ќе го ставам во новата датотека Cleared-Text.txt. Со ова го имам средено текстот кој што треба да го криптирам.

Шифрирање

Јас одлучив текстот да го криптирам користејќи го Афин шифрувачот. Имам клуч кој што е поделен во два дела $k = (a, b)$, формулата за криптирање гласи:

$$E_k(x) = y = ax + b \bmod 31$$

Додека па a, b, x, y припаѓаат на множеството од бројот на букви (31) во македонската азбука $\{0, 1, 2, \dots, 30\}$

Нека $k = (5, 7)$

со тоа што:

$$A = 0 = (0 \cdot 5) + 7 = 7 \bmod 31 \rightarrow \text{Ж}$$

$$B = 1 = (1 \cdot 5) + 7 = 12 \bmod 31 \rightarrow \text{К}$$

$$B = 2 = (2 \cdot 5) + 7 = 17 \bmod 31 \rightarrow \text{Њ}$$

.

.

.

$$\text{Ш} = 30 = (30 \cdot 5) + 7 = 157 \bmod 31 \rightarrow \text{В}$$

и со ова добивам супституција за секоја буква во азбуката.

Објаснување на програмата CipherText.java:

Најпрво започнав со креирање празна датотека Ciphred-Text.txt во која ќе го внесам шифрираниот текст. Направив функција TextCipher во која иницијализирам две променливи a и b , кои ми го претставуваат клучот поделен на два дела, и го читам текстот од датотеката Cleared-Text.txt, како една цела линија, и го внесувам во еден String text. Правам loop со почеток од 0 до крајот на текстот (text.length()) се со цел да можам да го изминам стрингот, карактер по карактер. Иницијализирам две променливи, x – позицијата на буквата во азбуката почнувајќи од 0 - 30 и y – резултатот од горе наведената функција, во овој случај остатокот од модуло операцијата. Правам проверка за карактерот на i -тата позиција од текстот (со text.charAt()), која буква е во азбуката, на тој начин доделувам соодветна позиција x , оваа проверка ја правам за секоја буква. Бидејќи во текстот имам големи и мали букви па и за двете ја правам проверката.

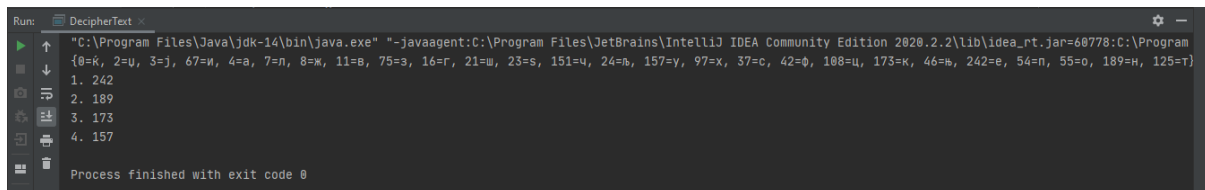
Наредно ја впишав функцијата, бидејќи сите променливи ги имам, и го добивам y .

у ми е резултатот од функцијата но воедно и позицијата на буквата која што е супституција за буквата од оригиналниот текст. Следно само правам append на буквата, во фајлот каде што го криптирам текстот, и така за секоја наредна буква од оригиналниот текст. На крај само ги затворам стримовите, да ослободат простор во меморија, и печатам порака дека текстот е успешно шифриран.

Со ова, во датотеката CipheredText.txt, го добив шифрираниот текст на оригиналната порака, користејќи Афин шифрувач со клуч k(5 , 7).

Дешифрирање на текст

Колешката Ангела Сотировска 183115 ми прати шифриран текст, во датотека kriptiran-tekst.txt, кој што треба да го дешифрирам. Најпрво најдов фреквенција на честота на буквите. Тоа го направив со HashMap, каде што за секој карактер од текстот ќе ми брои колку е неговото појавување, и ќе ми прави countArray[i]++ за секоја буква од азбуката. Тоа може да се види тука, дел извадок од програмата DecipherText.java



```
Run: DecipherText
"C:\Program Files\Java\jdk-14\bin\java.exe" "-javaagent:C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 2020.2.2\lib\idea_rt.jar=68778:C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 2020.2.2\bin" -classpath C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 2020.2.2\bin\classes;C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 2020.2.2\lib\idea_rt.jar DecipherText
{0=k, 2=u, 3=j, 67=n, 4=a, 7=p, 8=ж, 11=b, 75=s, 16=r, 21=ш, 23=s, 151=ч, 24=ь, 157=y, 97=x, 37=c, 42=0, 108=ц, 173=к, 46=ь, 242=e, 54=п, 55=о, 189=н, 125=т}
1. 262
2. 189
3. 173
4. 157
Process finished with exit code 0
```

Застапеноста на најкористените букви во енкриптираниот текст имаше сличност со табелата на распределба на фреквенциите што значеше дека првите 4 букви се тие, односно тие се самогласките, но не се знае распоредот. По некоја претпоставка, првата буква има најголема застапеност, од мапата видов дека во енкриптираниот текст тоа е “ Е ” и си ја зададов како “ А ”, поттик за ова беше и самата табела, која што беше поставена на курсот, каде А имаше најголема застапеност. После низа комбинации и brute force пробувања, приметив дека ако вредноста на втората најзастапена буква, тоа е “ Н ”, и ја зададам третата на застапеност по табелата, тоа е “ И ”, нивното растојание е 6 букви една од друга. Ова ми беше стартот за дешифрирање на кодот. Увидов дека колешката ја шифрирала пораката со Цезар шифрувач со клуч k = 6 букви напред. Ја направив супституцијата за секоја буква, и ги append во празниот фајл Deciphered-Text.txt, и го добив следниот текст:

серијатаигранатроновигрубојаследиприказнатаодпесназамразиогандејствиетосеодвиваво
измислениеседумкралстванавестеросасеријатагиприказуваборбитенаводечкитесемејст
вазаконтроланажелезниотпрестолкакоштотечеприказнатасепојавувадополнителназака
наоддалечниотсевериисточниотконтинентесоспратасезонаевернаадаптацијанаистои
мениотроманпонатамошнитесезонисевеќеоддалечуваатодизворниотматеријалспореда
ејвидбениофсеријатаадаптацијаовоцелинакојајаследимапаташтоџоријапоставилгиприка
жуваглавнитеточкинонеиситепопатнистаницидејствиетонасеријатаиликовитесепотти
кнатиодисторискинастанивоевропаглавнатаинспирацијаеанглискатавојанарозитекојасе
одвиваламеѓудинастиителанкастеријоркотсликанивосудиритемеѓудинастиителанистери
старкпоголемиотделодвестероссозамоцитеивитешкитетурнирипотсетуваатнасредниот
твекодзападнаевропакралицатасерсиланистерпотсетувананаизабеланареченаволчицатаод
францијаженатанаедвардвторивпрочемтааинејзинотосемејствоонакакакоштосеприкажа

нивосеријатароманинаморисдруонпроколнатикралевиноголемамерагоинспириралемартин
останатитеисторискиинспирациизанекоиодементитевосеријатасесидотнахадријангол
емиотсидлегендитезаатлантидадревнатавалиријавизантискиотгрчкиогандивитоганисл
андскатасагазавикинитесемејствотогрејџојимонголскитехордиплеметодотракикакоиеле
ментиодстогодишнатавојнаииталијанскатааренесансаголематапопуларностнасериијатав
онајголемделсеприпишуванаवेशтинатанамартиндагивткаеситеовиеелементивоеднород
нацелинакојаеверодостојнаворамкитенаеднаалтернативнаисторијадејвидбениофпредлож
илсериијатадасерекламиракакосопрановивосреднатаземјаукажувајќинамрачнитенастани
фантастичниотсветвокојсеслучувааттиспроведенаестудијаспоредкојасериијатасенаоѓан
автороместоодчетиридесеттелевизискиамериканскидрамскисериииспоредбројотнаубиств
апросечночетиринаесетвоеднаепизода