PANEVROPSKI UNIVERZITET APERION

FAKULTET INFORMACIONIH TEHNOLOGIJA

Vandredne studije

Predmet:

OBJEKTNO ORJENTISANO PROGRAMIRANJE U JAVA PROGRAMSKOM JEZIKU

PROGRAM ZA SINHRONO ŠIFROVANJE I DEŠIFROVANJE PORUKE

(seminarski rad)

Predmetni nastavnik:

Doc. Dr Saša Salapura

Student:

Boris Blagojević

Indeks br. : 58-16 /RPI

Datum i mjesto: 30.10.2019 Banja Luka

SADRŽAJ

UVOD

Tema ovog seminatskog rada je bila kriptografski algoritmi u Java programskom jeiku kao desktop aplikacija. Algoritam se temelji na načinu sifrovanja pomoću Viženere metode. Zadatak ovog programa je da učita ključ i poruku iz txt datoteka, sifruje te zatim desifruje poruku i da iste zapiše u nove txt datoteke.

U ovom seminarskom radu biće opisana način rada Viženere metode, sadržaj programa i kratak opis rada ovog programa.

VIŽENEROVA ŠIFRA

Viženeorva šifra je metoda sifrovanja ili prekrivanje poruke pomocu ključa. Ova metoda je nadogradnja Cezarove metode, gdje se kod Cezarovog šifrovanja koristi kljuc kao kao jedan broj sa kojim se pomjera slova za taj broj, kod Viženerovog šifrovanja se koristi rječ kao ključ.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Slika 1 Tabela Viženerovog sifrovanja

Prema tabeli sa slike 1 možemo vidjeti da ako je poruka slovo A i na nju dodamo kljuc slovo X, dobijemo šifrovanu poruku slovo X.

Ali kada povecamo poruku za jedno slovo B i iskoristimo isti kljuc X dobijemo šiforvanu poruku Y.

Ako imamo pravu poruku koju bi neka osoba poslala kao na primjer :

OVA PORUKA CE BITI TAJNA[1]

I ovu poruku šifrujemo Viženerovom metodom sa ključem:

ZDRAVO

Potrebno je da rječ ključa produžimo za onoliko mjesta koliko je dugačka poruka, izuzevši prazna mjesta:

KLJUČ: ZDRAVOZDRAVOZDRAVO
PORUKA: OVAPORUKACEBITITAJNA

SIFROVANA PORUKA:

NYRPJFTNRCZPHWZTVXMD

Ovaj proces se može opisati formulom:

Ei = (Pi + Ki) mod 26

Gdje je P poruka, K je kljuc a E je sifrovana poruka.
I je indeks, pozicija slova u poruci, kljuci i sifrovanoj poruci.

Desifrovanje je ista metoda samo unazad, jer kada smo sifrovalji poruku vrijednost kljuca smo dodavali na vrijednost poruke, a kod desifrovanja vrijednost sifrovane poruke oduzmemo za vrijednost kljuca.

KLJUČ : ZDRAVOZDRAVOZDRAVO
ŠIFROVANA PORUKA

NYRPJFTNRCZPHWZTVXMD

PORUKA: OVAPORUKACEBITITAJNA

Metoda je izvršena prema formuli:

Pi = (Ei – Ki +26) mod 26

[1] U poruci se ne nalazi slovo Ć zato što se u programu koristi ASCII tabela karaktera u kojoj ovo slovo i slićna ne postoje.

SADRŽAJ PROGRAMA

Program se sadrži od jedne klase i pet metoda uključujuči i main metodu. Takođe sadrži i jednu biblioteku za ulazno izlazne operacije. Unastavku cu ukratko opistati rad metoda koje koristim u programu.

Metoda sifrovanje

U ovoj metodi primamo dva stringa, prvi string je poruka koju ćemo šifrovati a drugi string je staticka, ne promjenjiva varijabla koja je ključ.

U ovoj metodi pomocu formule koju smo opisali u tekstu gore sifrujemo poruku sa kljucem. Veoma je bitno da se kljuc ponavlja to jeste da se svaki karkter poruke poveća za vrijednost karaktera ključa. Kada dođemo do kraja rječi ključa potrebno je da se vratimo na prvi karakter ključa.

Ova metoda na kraju vraća jedan string u kojoj se nalazi sifrovana poruka.

Potpis metode:

Static String sifrovanje (String text, final String kljuc)

Metoda desifrovanja

Kao i kod metode sifrovanja, ova metoda vraca jedan string, desifrovan tekst. Prima dva stringa, prvi je sifrovana tekst, a drugi je kljuc isto kao i kod prve on je fiksan.

Koristi se druga formula iz prethodnog teksta o metodi viženerovog šifrovanja. Kao i u prehodnoj metodi bitno je da se karakteri rječi ključa ponavljaju onoliko puta koliko imamo karaktera u sifrovanoj poruci.

Na kraju ova metoda vraca string sa desifrovanom porukom.

Potpis metode:

Static String desifrovanje (String text, final String kljuc)

Metoda ucitavanja teksta iz txt datoteke.

Ova metoda ima ulazan jedan string i izlazan jedan string.

Koristimo try i catch sintaksu u ovoj metodi. U try tjelu inicijališemo Scanner objekat sa imenom ucitaj. U tom objektu ce se nalaziti lokacija datoteke iz kojecemo ucitavati tekst koji želimo da se sifruje. Takodje ova metoda ce ucitati tekst kljuca.

U while petlja ce provjeravati da li ima linija u txt datoteci, i sve dok ima ucitavaće text u lokalni string koji je deklarisan prije try i catch sintakse.

Catch sintaksa će ispisati poruku korisniku ako try ne može pronaći datoteku.

Na kraju ova metoda vraća učitani tekst kao string.

Potpis metode:

Static string ucitajTxt(String lokacija)

Metoda pisanja teksta

Ova metoda je void, ne vraća nista. Ucitava dva stringa, prvi je sifrovani ili desifrovni tekst, a drugi sting je lokacija datoteke. Treba napomenuti da u ovoj metodi lokacije koje prime ne postoje, to jeste ne postoje txt datoteke. Program će zahvaljujući I/O biblioteci i njenm metodama napraviti txt datoteku onoliko puta koliko bude pozvan.

U try sintaksi se inicijalizuje objekat pisi u kojem se nalazi lokacija gdje ce se napraviti nova datoteka.
Metoda koja se poziva pisi.println(txt) će pisati u datoteku primljeni string. Bitno je zatvoriti datoteku pomoću pozivanja metode pisi.close() da bi se saćuvala poruka koja je primljena u ovoj metodi. Ako ne zatvorimo datoteku doicemo samo praznu txt datoteku.

Potpis metode:

Static void pisiTxt(Strig txt, String lokacija)

Main metoda

U main metodi imamo četiri stringa u kojima se nalaze lokacije (postojeće i one koje će biti napravljene) txt datoteka. Stringovi su sledeći

- kljuc
- orginalniText
- sifrovaniText
- desifrovaniText

Nalaze se takođe i dva stringa koji će privremeno držati sifrovane i desifrovane poruke, stringovi sif i des (skraceno).

Pozivaju se dve metode sifrovanje i desifrovanje u kojima se salju poruka i kljuc.
Na kraju će biti ispisano u terminalu korisniku poruka Gotovo, kao bi se znalo da je program zavrsio sa radom.

KRATAK OPIS RADA PROGRAMA

Kao što smo rekli u main metodi se nalazi šest stringova od kojih prva četiri kao vrijednost imaju lokaciju datoteka u kojima se cita poruka i kljuc, te u druga dva stringa se nalazi lokacija u kojima će se kreirati nove datoteko u kojim će se upisati sadržaj sifrovane i dešifrovane poruke. Ti stringovi su kljuc (lokacija txt datoteke sa ključem), orginalniText (lokacija txt datoteke sa porukom), sifrovaniText (željena lokacija sa imenom datoteke u kojoj će se upisati sifrovani tekst) i desifrovaniText (željena lokacija sa imenom datoteke u kojoj će se upisati desifrovani tekst).

Dva stringa u kojima će se privremeno sačuvati šifrovani i dešifrovani tekst (imena varijabli su sif i des.

Prvo se poziva metoda sifrovanje u kojima se salje vrijednost lokacije orginalnog teksta kao i lokacija kljuc. Ova metoda ce po opisu rada viženere sifrovanja, šifrovati tekst i vratiti vrijednost u main koja će se sačuvati u varijabli sif.

Zatim se poziva metoda pisiTxt kojoj se salje sifrovani tekst iz varijable sif i lokacija sifrovanog teskta iz varijable sifrovaniText.
Metoda pisi kreira novu datoteku sa zeljenim imenom koji je dat u lokaciji datoteke. Piše sifrovani tekst i zatvara tu novo kreiranu datoteku.

Poziva se metoda desifrovanje koja uzima sifrovani tekst iz varijable sif i kljuc. Desifruje tekst i vraca string desifrovanog teksta u main metodu.

Poziva se pisiTxt metoda, uzima dva stringa, desifrovani string i lokaciju zeljene datoteke.
Pise u datoteku i zatim je zatvara.

Na kraju poziva se metoda println koj će ispisati korisniku u terminalu poruku da je program završio.

ZAKLJUČAK

Kao što možemo vidjeti ovo je kratak program, cija je jedina namjena da učita kljuc i poruku iz datoteke, sifruje poruku i upise u novu datoteku taj sadržaj, zatim desifruje poruku i takođe upise u još jednu novu datoteku sadržaj. Pošto koristimo isti ključ za šifrovanje i dešifrovanje poruke možemo vidjeti da je ovo sinhroni algoritam.
Pokušano je u ovome seminarskom radu da se sto je moguće bolje opise rad samog algoritma sifrovanja i desifrovanja na teoretski način i da se opise sadržaj programa i njegov rad.

IZVORI

Wignere cipher. (2019, Oktobar 20). Preuzeto sa Wikipedia: https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

SPISAK SLIKA