**UNIVERSITETI I PRISHTINËS "HASAN PRISHTINA"**

**FAKULTETI I SHKENCAVE MATEMATIKO-NATYRORE**

**DEPARTAMENTI I MATEMATIKËS**

**PROGRAMI: SHKENCA KOMPJUTERIKE**

# PUNIM SEMINARIK

Lënda: Siguria e të dhënave

TEMA: Vigenere Cipher

**Punuar nga:** Auron Ismajli

Florida Kurtaj

Laureta Durguti

**Mars 2023**

# Përmbajtja

**Historiku** ..... 3
**Përshkrimi** ..... 4
**Algoritmi** ..... 6
**Kodi** ..... 7

## Historiku

Vigenere Cipher, ose "kodi i Vigenerit" , është një sistem enkriptimi që u zhvillua në fillim të shekullit të 16-të nga një diplomat dhe kriptograf francez, Blaise de Vigenère. Ky sistem enkriptimi u përdor nga shumë komandantë ushtarakë, diplomatë dhe agjentë sekretë në shekujt pasardhës, duke bërë që të jetë një nga metodat më të njohura dhe të përdorura të enkriptimit.

Ideja e kësaj metode enkriptimi është e ngjashme me atë të Caesar Cipher.

Caesar Cipher ishte një metodë enkriptimi që përdorte një shifër fikse për të shkëputur mesazhet. Kjo metodë ishte e thjeshtë për tu zbuluar, pasi shifra e përdorur për të shkëputur mesazhin ishte gjithmonë e njëjtë, dhe kishte vetëm 25 mundësi. Vigenère e kuptoi se nëse ai mund të përdorte një seri shifrash të ndryshme për secilën shkronjë në mesazh, kodi do të ishte shumë më i sigurt dhe do të ishte më vështirë për tu zgjidhur.

Kjo bëri që metoda e kodi i Vigenerit të jetë një prej metodave më të njohura dhe të përdorura të enkriptimit. Megjithatë, kodi i Vigenerit u zbulua dhe u zgjidh në fund të shekullit të 19-të, kur u zhvilluan metoda të reja të enkriptimit.

Sistemi i enkriptimit Vigenere është një sistem enkriptimi të cilin shumë njerëz e konsiderojnë si një prej metodave më të sigurta të enkriptimit në historinë e kriptografisë. Kjo është për shkak se ai përdor një seri shifrash të ndryshme për secilën shkronjë në mesazh, duke bërë që të jetë shumë më vështirë për tu zgjidhur dhe për tu ndërprerë nga një person që nuk e ka shifrën e duhur.

Megjithatë, kodi i Vigenerit nuk është pa të meta dhe ka disa kufizime. Nëse shikohet me kujdes, mund të vërehet se mesazhet të cilat janë të përkthyera me këtë sistem, kanë një strukturë periodike. Kjo mund të ndihmojë një person të kuptojë se si është përdorur shifra dhe të zgjidhë mesazhin.

Për të përmbushur këto kufizime, u zhvilluan metoda të ndryshme të enkriptimit, të tilla si RSA, AES dhe DES. Këto metoda janë më të avancuara dhe më të sigurta se kodi i Vigenerit, dhe janë përdorur gjithnjë e më shumë në kohën moderne të teknologjisë së informacionit.

Megjithatë, historia dhe zhvillimi i kriptografisë nuk do të ishin të plotësuar pa këtë metodë të enkriptimit më të ndryshme dhe inovative. Sistemi i shifrës së Vigenerit është një prej metodave të enkriptimit më të njohura dhe të përdorura në

historinë e kriptografisë, dhe është një simbol i inovacionit dhe zhvillimit të teknologjisë së informacionit.

## Përshkrimi

### Si përdoret Vigenere Cipher?

Për të përdorur këtë sistem enkriptimi, fillimisht duhet të keni një shifër që do të përdorni për të shkëputur mesazhin. Kjo shifër mund të jetë një fjali ose fjalë e caktuar, dhe duhet të jetë e një gjatësie të barabartë me gjatësinë e mesazhit që dëshironi të enkriptoni.

Pas kësaj, ju duhet të keni një tabelë alfabeti të ndërtuar sipas rreshtave dhe kolonave. Për të enkriptuar mesazhin, ju do të shkruani secilën shkronjë të mesazhit në një rresht, dhe secilën shkronjë të shifrës në një kolonë. Në këtë mënyrë, ju do të keni një grup të shifrave për secilën shkronjë të mesazhit.

| | 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 |

Pasi keni gjetur grupet e shifrave për secilën shkronjë, ju mund të përdorni tabelën e alfabetit për të zëvendësuar secilën shkronjë me shifrat e duhura. Për kthimin e

mesazhit në formën origjinale, ju do të përdorni shifrat e duhura nga shifrat e celesit dhe tabela alfabeti për të gjetur shkronjën e duhur.

Për shembull, nëse shkronja e parë e mesazhit është "H" dhe shkronja e parë e shifrës është "K", ju do të shkruani "K" në kolonën e parë dhe "H" në rreshtin e parë të tabelës alfabeti. Shifra e duhur do të jetë ajo që gjendet në kryqëzim të kolonës së "K" dhe rreshtit të "H".

Kodi i Vigenerit është një sistem enkriptimi i thjeshtë për t'u kuptuar, por duhet të merren parasysh disa aspekte dhe kufizime për t'u siguruar që ai të përdoret me sukses dhe me siguri.

Tabela e Vigenere Cipher mund te gjendet e gatshme por në fund do t’ju paraqesim një java code se si krijohet.

## Algoritmi

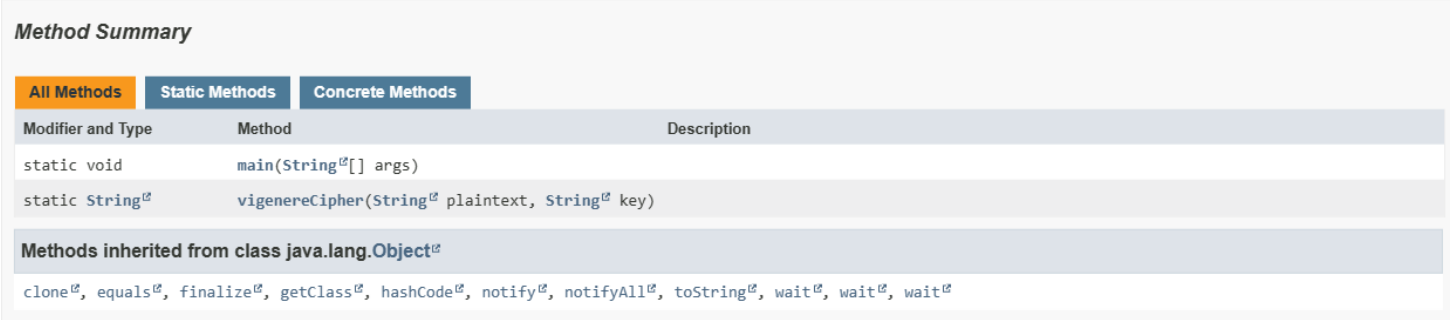
Algoritmi për Shifrën e Vigenere:

1. Inicializojeni mesazhin e tekstit të thjeshtë dhe çelësin sekret.
2. Krijoni një tabelë Vigenere që përmban alfabetin.
3. Gjeneroni çelësin e përsëritur duke zgjeruar çelësin sekret në gjatësinë e mesazhit.
4. Konvertoni mesazhin dhe çelësin në shkronja të mëdha.
5. Iterojeni përmes secilit karakter në mesazh:
   a. Përcaktoni rreshtin dhe kolonën për karakterin në tabelën Vigenere.
   b. Përcaktoni karakterin përputhës në çelësin për iterimin aktual.
   c. Përcaktoni kolonën për karakterin në tabelën Vigenere për karakterin në çelësin.
   d. Përcaktoni karakterin e cifrave duke gjetur karakterin në kryqëzim të rreshtit dhe kolonës nga hapat a dhe c.
   e. Shtoni karakterin e cifrave në rezultat.
6. Jepni tekst të shifruar.

## Kodi

Kodin e këtij algoritmi e kemi krijuar ne java.

Kodi përbëhet nga metoda “main” dhe metoda statike “vigenereCipher”.



***Method Summary***

All Methods | Static Methods | Concrete Methods

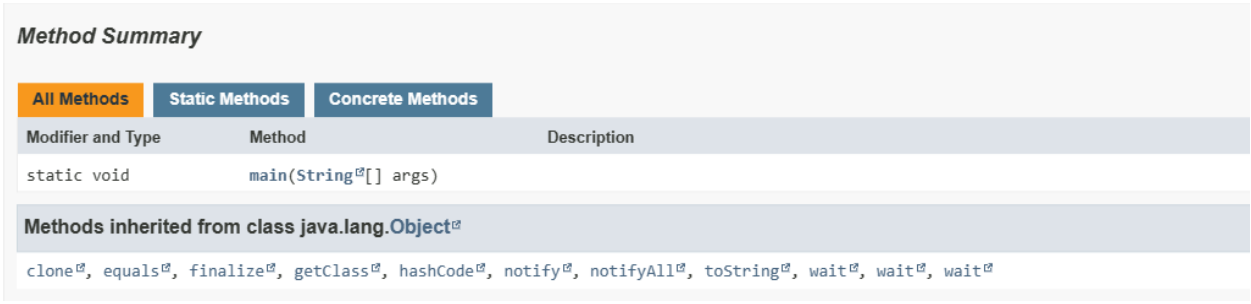
| Modifier and Type | Method | Description |
|---|---|---|
| static void | main(String[] args) | |
| static String | vigenereCipher(String plaintext, String key) | |

**Methods inherited from class java.lang.Object**

clone, equals, finalize, getClass, hashCode, notify, notifyAll, toString, wait, wait, wait

Në metodën main së pari kërkohet nga user-i që të futet teksti origjinal dhe celësii cili sic dihet në shifrën e Vigenere është tekst, më pas thirret metoda vigenereCipher e cila duke u bazuar në celës e shifron tekstin origjinal.

Për dekriptim të tekstit duhet bazuar në tabelën e Vigenere kodi I së cilës përshkruhet më poshtë.



***Method Summary***

All Methods | Static Methods | Concrete Methods

| Modifier and Type | Method | Description |
|---|---|---|
| static void | main(String[] args) | |

**Methods inherited from class java.lang.Object**

clone, equals, finalize, getClass, hashCode, notify, notifyAll, toString, wait, wait, wait

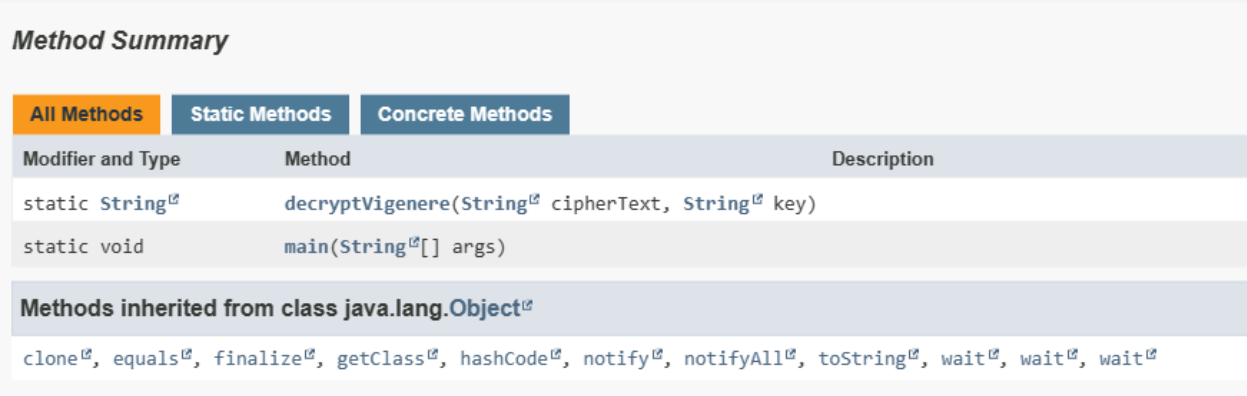
Në këtë kod, ne fillimisht krijojmë një varg dydimensional me madhësi n x n. Ne përdorim nested loops për të mbushur vargun me karakteret e tabelës Vigenere Cipher. Konkretisht, ne vendosëm tabelën[i][j] të jetë karakteri që korrespondon me shkronjën A të zhvendosur me (i + j) % n pozicione. Operacioni % n siguron që rezultati të jetë gjithmonë mes 0 dhe 25, që janë treguesit e shkronjave në alfabet.

Pas krijimit të vargut të tabelës, ne e printojmë atë.

Fillimisht shtypim rreshtin e kokës me shkronjat A deri në Z. Më pas, për çdo rresht të tabelës, shtypim shkronjën që korrespondon me indeksin e rreshtit të ndjekur nga karakteret në atë rresht.

**Vini re se ky zbatim supozon se alfabeti është alfabeti standard anglez me 26 shkronja. Nëse keni nevojë të trajtoni alfabete të tjera ose grupe karakteresh, mund t'ju duhet të modifikoni kodin në përputhje me rrethanat.**

Poashtu kemi krijuar metodën për dekriptim e cila do t'i kërkojë përdoruesit të fusë tekstin e shifrimit dhe celësin. Metoda Scanner.nextLine() përdoret për të lexuar hyrjet si vargje. Pas marrjes së hyrjes thirret metoda decryptVigenere për të deshifruar tekstin e shifrimit duke përdorur çelësin e futur nga përdoruesi. Më në fund kthehet teksti origjinal.



*Method Summary*

All Methods | Static Methods | Concrete Methods

| Modifier and Type | Method | Description |
|---|---|---|
| static String | decryptVigenere(String cipherText, String key) | |
| static void | main(String[] args) | |

**Methods inherited from class java.lang.Object**

clone, equals, finalize, getClass, hashCode, notify, notifyAll, toString, wait, wait, wait