Criptoanálise da Cifra de Vigenère

Gabriel Frigo Petuco

Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
Porto Alegre – RS – Brazil

Resumo. *Este relatório descreve o desenvolvimento de um programa para a criptoanálise da cifra de Vigenère, cujo objetivo é decifrar um texto cifrado e encontrar o texto claro correspondente. O método empregado envolve a estimativa do comprimento da chave utilizada na criptografia, utilizando o Índice de Coincidência. Além disso, o programa analisa a frequência das letras para identificar a chave correta, aplicando frequências conhecidas da língua portuguesa e inglesa.*

1. Introdução

A cifra de Vigenère é um método de criptografia clássica que utiliza uma sequência de letras (chave) para cifrar o texto claro. A segurança dessa cifra reside na complexidade da chave; no entanto, técnicas de criptoanálise, como o Índice de Coincidência e o Teste de Kasiski, podem ser utilizadas para revelar o texto claro. Este trabalho detalha a implementação de um programa que, dada uma string cifrada, determina o texto claro correspondente.

2. Estrutura do Código

O programa é estruturado em várias funções, que incluem:

1. **Índice de Coincidência**: Calcula a frequência de coincidências entre as letras de um texto cifrado, fornecendo uma indicação do comprimento da chave.
2. **Determinação do Comprimento da Chave**: Através do Índice de Coincidência, o programa avalia diferentes comprimentos de chave e seleciona aquele que apresenta o maior índice, indicando a maior probabilidade de corresponder à chave utilizada na cifragem.
3. **Análise de Frequência**: Para cada parte do texto cifrado, a frequência das letras é comparada com as tabelas de frequência de letras em português e inglês, permitindo a identificação da chave utilizada na cifra.
4. **Descriptar**: Após determinar a chave, o programa utiliza essa informação para decifrar o texto cifrado, convertendo os valores ASCII do texto cifrado de volta ao texto claro.

3. Implementação

O programa começa com a importação das bibliotecas necessárias, como o Flask, e a definição de variáveis globais, incluindo as tabelas de frequência das letras em português e inglês, além de constantes como o tamanho máximo da chave.

A função indiceCoincidencia(cifrado) calcula o Índice de Coincidência para um texto cifrado dado. O Índice de Coincidência é uma métrica que quantifica a probabilidade de

duas letras aleatórias escolhidas do texto serem iguais. Isso é útil para estimar o comprimento da chave.

A função tamanhoChave(cifrado) determina o comprimento da chave mais provável, dividindo o texto cifrado em partes com base em comprimentos de chave hipotéticos e calculando a média do Índice de Coincidência para cada comprimento.

As funções frequenciaPortugues(sequencia) e frequenciaIngles(sequencia) realizam a análise de frequência para identificar a letra da chave correspondente a cada parte do texto cifrado. Essas funções utilizam a tabela de frequência conhecida para comparar e calcular a diferença em relação à sequência deslocada.

As funções chavePortugues(cifrado, key_length) e chaveIngles(cifrado, key_length) constroem a chave ao iterar sobre as sequências de letras do texto cifrado, utilizando as funções de análise de frequência.

A função decifrar(cifrado, key) converte o texto cifrado de volta ao texto claro utilizando a chave encontrada. Para cada letra do texto cifrado, o código ASCII é ajustado de acordo com a letra correspondente na chave.

O programa utiliza o Flask para criar uma API que permite enviar um texto cifrado e receber o texto claro em resposta. A rota /decifrar processa a requisição e retorna as chaves e textos claros em formato JSON.

4. Lógica Geral

O fluxo do programa pode ser resumido nas seguintes etapas:

1. **Recepção do Texto Cifrado**: O usuário envia um texto cifrado.
2. **Limpeza do Texto**: O texto é processado para remover caracteres não alfabéticos.
3. **Cálculo do Comprimento da Chave**: O Índice de Coincidência é usado para estimar o comprimento da chave.
4. **Análise de Frequência**: O texto cifrado é dividido em partes e comparado com as tabelas de frequência para determinar a chave.
5. **Decifrar**: A chave identificada é usada para decifrar o texto cifrado, retornando o texto claro ao usuário.

6. Estrutura do Projeto

- app.py: Código principal que contém a lógica de criptoanálise e as rotas.
- index.html: Interface HTML e CSS simples para interação com o usuário.

Para utilizar a aplicação:

pip install Flask

python app.py

Acessar em http://127.0.0.1:5000/

6. Resultados

A aplicação foi testada com textos cifrados em português e inglês. Para um texto cifrado fornecido, o programa foi capaz de descobrir a chave correta e produzir o texto claro correspondente. Os resultados indicam que a análise de frequência, combinada com o Índice de Coincidência, é eficaz na criptoanálise da cifra de Vigenère.

6.1 Língua Inglesa

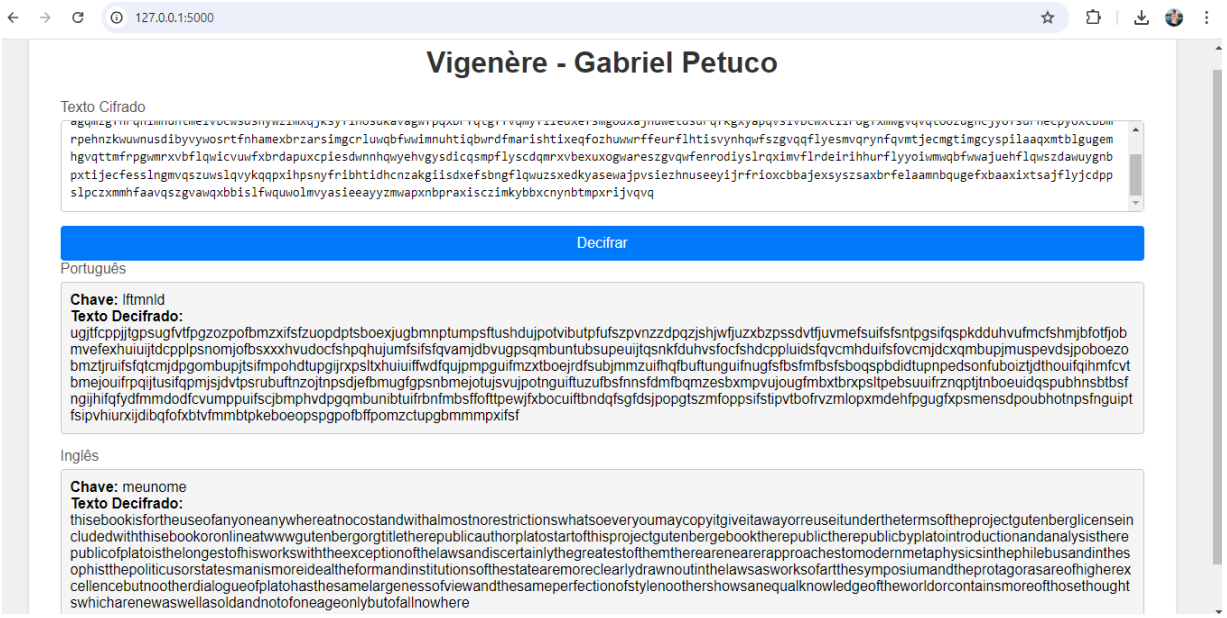
Texto Cifrado:

flcfsnsaocftavflyhgqsrehlczimrsjvqvqenacosexuarimfluyaawfriesexdmwgwareabnhesqz
yemayyespcbcuxavjqmfeqnmavdiofsuxgrxrfflqxyeaesrxbrddsviwgugxqrvrfspugyagqmz
gfhrqhimnuhtmeivbcwsdshywzimxqjksyfihosdkavagwfpqxbrfqtgffvqmyfliedxefsmgodx
ajnuwetdsdrqfkgxyapqvsivbcwxtilrdgfxmwgvqvqtoozugncjyofsurnecpyoxcbbmrpehnzk
wuwnusdibyvywosrtfnhamexbrzarsimgcrluwqbfwwimnuhtiqbwrdfmarishtixeqfozhuww
rffeurflhtisvynhqwfszgvqqflyesmvqrynfqvmtjecmgtimgcyspilaaqxmtblgugemhgvqttmfr
pgwmrxvbflqwicvuwfxbrdapuxcpiesdwnnhqwyehvgysdicqsmpflyscdqmrxvbexuxogwar
eszgvqwfenrodiyslrqximvflrdeirihhurflyyoiwmwqbfwwajuehflqwszdawuygnbpxtijecfes
slngmvqszuwslqvykqqpxihpsnyfribhtidhcnzakgiisdxefsbngflqwuzsxedkyasewajpvsiezh
nuseeyijrfrioxcbbajexsyszsaxbrfelaamnbqugefxbaaxixtsajflyjcdppslpczxmmhfaavqszgv
awqxbbislfwquwolmvyasieeayyzmwapxnbpraxisczimkybbxcnynbtmpxrijvqvq

Chave: meunome

Texto Claro:

thisebookisfortheuseofanyoneanywhereatnocostandwithalmostnorestrictionswhatsoever
youmaycopyitgiveitawayorreuseitunderthetermsoftheprojectgutenberglicenseincludedwi
ththisebookoronlineatwwwgutenbergorgtitletherepublicauthorplatostartofthisprojectgute
nbergebooktherepublictherepublicbyplatointroductionandanalysistherepublicofplatoisthe
longestofhisworkswiththeexceptionofthelawsandiscertainlythegreatestofthemtherearenea
rerapproachestomodernmetaphysicsinthephilebusandinthesophistthepoliticusorstatesma
nismoreidealtheformandinstitutionsofthestatearemoreclearlydrawnoutinthelawsasworks
ofartthesymposiumandtheprotagorasareofhigherexcellencebutnootherdialogueofplatohas
thesamelargenessofviewandthesameperfectionofstylenoothershowsanequalknowledgeoft
heworldorcontainsmoreofthosethoughtswhicharenewaswellasoldandnotofoneageonlybut
ofallnowhere



6.2 Língua Portuguesa

Texto Cifrado:

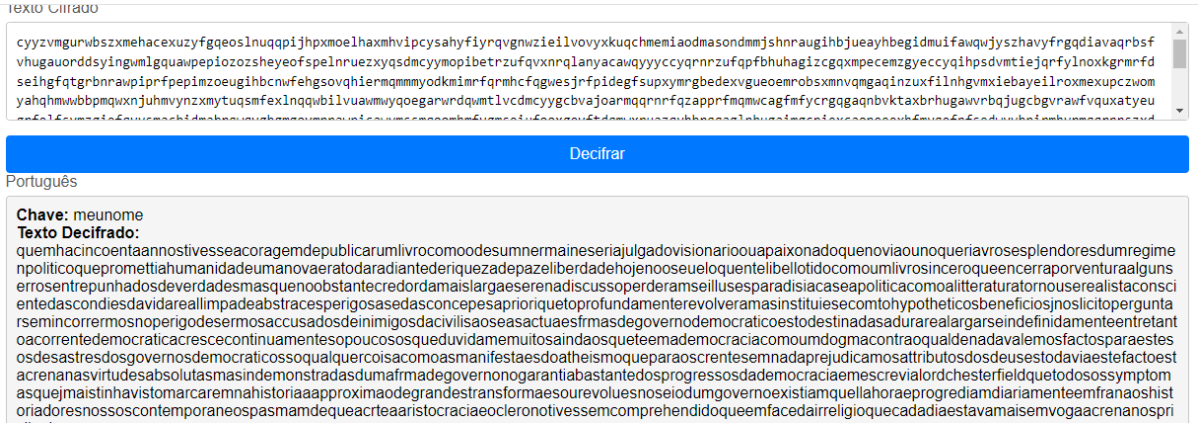
cyyzvmgurwbszxmehacexuzyfgqeoslnuqqpijhpxmoelhaxmhvipcysahyfiyrqvgnwzieilvo
vyxkuqchmemiaodmasondmmjshnraugihbjueayhbegidmuifawqwjyszhavyfrgqdiavaqrbs
fvhugauorddsyingwmlgquawpepiozozsheyeofspelnruezxyqsdmcyymopibetrzufqvxnrqla
nyacawqyyyccyqrnrzufqpfbhuhagizcgqxmpecemzgyeccyqihpsdvmtiejqrfylnoxkgrmrfds
eihgfqtgrbnrawpiprfpepimzoeugihbcnwfehgsovqhiermqmmmyodkmimrfqrmhcfqgwesjr
fpidegfsupxymrgbedexvgueoemrobsxmnvqmgaqinzuxfilnhgvmxiebayeilroxmexupczwo
myahqhmwwbbpmqwxnjuhmvynzxmytuqsmfexlnqqwbilvuawmwyqoegarwrdqwmtlvcd
mcyygcbvajoarmqqrnrfqzapprfmqmwcagfmfycrgqgaqnbvktaxbrhugawvrbqjugcbgvrawf
vquxatyeugrfelfsymzgiefqvysmacbidmabrqwqvgbgmgoymnrawpicawymssmqoomhmfv
gmseiufooxgeyftdqmwxruazqvhbrqqaglnhugaimgcpiexcaopeeexhfmvqefnfsedwyvbpir
mhvrmqqrnrszxdinnbfsmgiefqrfixraagdenvqmgdimpsoszxcaimqqrnrgataywbgawcyyqih
mpegragmfsmnwzhmsmdiqxqignrqqaglnqueosgbiyhakgnqarfvubegexhyaopehefraawre
wgcetmvurgfiesmqseeexlrgpsekiisdrawxraagdenvqaweskhoxugilpcuwmgizcmwyehvtqw
feyfraeflyvgyscyycodeawweszxqwyzbmhmtlrxghuguzceefxlvpgxawxbgpigwyfhahmzcn
sexqjuphaiexupfqrmrufjuvfyxrgmfesfhhmwyemvbpiyshfhdepemqiyervgnrqkazyebaraku
eozxuevngfezxyqcetdsaesewawxnrqqaglnqueqqyfqdihmuycdholyfhqvrmyyrcyqxiqcese
wszdfsyemdiqnyecfhurtepvgfsyelpodiyruuwexavcnomtbvikwyeahytfmrpimgfmrejieami
esoeshsxyyfbawqmiqiykazyebaijmmgwmqcyyyzmlavurddssvyqwmqpmuewmqqrnrsyjd
ehnceluwnbfuepslrgzsewifqarfigccdeziifdmwyegqscyqewehqemvcfhagdewvoqsopyeczsf
mprgeiygizdditihqwpscyyrareoixnwdvqpctwaugiwnrmhueyfhmzmquvgqqhsanoovqruac
etdmpvzqkusm

Chave: meunome

Texto Claro:

quemhacincoentaannostivesseacoragemdepublicarumlivrocomoodesumnermaineseriajul
gadovisionarioouapaixonadoquenoviaounoqueriavrosesplendoresdumregimenpoliticoqu

epromettiahumanidadeumanovaeratodaradiantederiquezadepazeliberdadehojenooseuelo
quentelibellotidocomoumlivrosinceroqueencerraporventuraalgunserrosentrepunhadosde
verdadesmasquenoobstantecredordamaislargaeserenadiscussoperderamseillusesparadisi
acaseapoliticacomoalitteraturatornouserealistaconscientedascondiesdavidareallimpadeab
stracesperigosasedasconcepesaprioriquetoprofundamenterevolveramasinstituiesecomtoh
ypotheticosbeneficiosjnoslicitoperguntarsemincorrermosnoperigodesermosaccusadosdei
nimigosdacivilisaoseasactuaesfrmasdegovernodemocraticoestodestinadasadurarealargars
eindefinidamenteentretantoacorrentedemocraticacrescecontinuamentesopoucososquedu
vidamemuitosaindaosqueteemademocraciacomoumdogmacontraoqualdenadavalemosfa
ctosparaestesosdesastresdosgovernosdemocraticossoqualquercoisacomoasmanifestaesdo
atheismoqueparaoscrentesemnadaprejudicamosattributosdosdeusestodaviaestefactoestac
renanasvirtudesabsolutasmasindemonstradasdumafrmadegovernonogarantiabastantedos
progressosdademocraciaemescrevialordchesterfieldquetodososymptomasquejmaistinha
vistomarcaremnahistoriaaapproximaodegrandestransformaesourevoluesnoseiodumgover
noexistiamquellahoraeprogrediamdiariamenteemfranaoshistoriadoresnossoscontempora
neospasmamdequeacrteaaristocraciaeocleronotivessemcomprehendidoqueemfacedairreli
gioquecadadiaestavamaisemvogaacrenanosprivilegios



7. Conclusão

O desenvolvimento deste programa demonstra a viabilidade de técnicas de criptoanálise para decifrar textos cifrados usando a cifra de Vigenère. A utilização do Índice de Coincidência e a análise de frequência permitiram a recuperação bem-sucedida do texto claro, evidenciando a importância dessas metodologias na segurança da informação. Futuros trabalhos podem explorar a otimização do algoritmo e a implementação de métodos alternativos, como o Teste de Kasiski, para comparação de eficácia.