UNIVERSIDADE DE BRASÍLIA
Departamento de Ciência da Computação
Segurança Computacional 2/2023
Prof. Dr. João Gondim

Aluno: Felipe Oliveira do Nascimento Florentino

Trabalho de Implementação 1

Cifra de Vigenère

Neste trabalho, foi desenvolvido um código para implementar a Cifra de Vigenère, incluindo cifragem, decifragem e ataque de recuperação de senha por análise de frequência. Para garantir que o programa funcione corretamente, é importante que o usuário siga as regras de processamento de dados que o programa aceita e siga as instruções dadas pelo programa.

Todas as informações de entrada, como mensagens, cifras e chaves, devem ser inseridas via teclado ou copiadas e coladas no programa. É altamente recomendado que o usuário evite o uso de letras maiúsculas, números, acentos e pontuações, pois esses caracteres podem comprometer a cifragem. Para tratar isso, foi feita uma espécie de varredura no texto para retirar os espaços e pontuações e assim poder cifrar/decifrar.

Cifrador e Decifrador

O algoritmo utiliza uma função para validar o tamanho da chave e da mensagem inserida pelo usuário. A senha é repetida até preencher todo o comprimento da mensagem. A função recebe dois parâmetros, a mensagem e a senha, ambos do tipo string. Em seguida, a chave é retornada em formato string para ser utilizada pelo cifrador ou decifrador.

Cifrador

O código utiliza a técnica de criptografia da Cifra de Vigenère para codificar a mensagem fornecida pelo usuário. Essa técnica é baseada em uma tabela de alfabetos deslocados, onde cada letra da mensagem é cifrada utilizando uma letra da chave. A chave é repetida quantas vezes forem necessárias para que tenha o mesmo tamanho da mensagem.
A mensagem cifrada é então retornada ao usuário para que possa ser transmitida de forma segura. A mensagem é cifrada por meio de um processo que envolve o percorrer de cada caractere da mensagem, verificando se esta é uma letra minúscula do alfabeto. Caso seja, é

realizado um cálculo de deslocamento com base na chave, utilizando a posição do caractere na mensagem e na chave.
O resultado dessa operação é convertido em uma letra do alfabeto novamente e adicionado à cifra.
Se o caractere não for uma letra minúscula do alfabeto, ele é adicionado diretamente à cifra sem cálculo de deslocamento. Esse processo é repetido até que todos os caracteres da mensagem tenham sido percorridos.

Decifrador

A função de decifração implementada segue o método da Cifra de Vigenère (https://pt.wikipedia.org/wiki/Cifra_de_Vigenère) e recebe como parâmetros a cifra fornecida pelo usuário e a chave já validada.
Após isso, a função retorna a mensagem original correspondente à cifra descriptografada.
Para descriptografar a mensagem, a função utiliza um algoritmo que percorre cada caractere da cifra e da chave ao mesmo tempo, realizando o cálculo inverso ao da cifragem, para obter a letra original correspondente. O resultado é a mensagem original que foi cifrada utilizando a chave fornecida.
O decifrador utiliza uma estrutura for para percorrer todas as letras da string cifra.
Antes disso, é verificado se cada caractere está entre 'a' e 'z' através de uma estrutura if.
Caso a letra esteja dentro deste intervalo, é feito um cálculo para determinar o deslocamento que deve ser feito para a decifração com a chave.
Este cálculo envolve a posição i da cifra, a posição i-j da chave e o total de letras do alfabeto.
A letra resultante é salva na string mensagem após ser convertida através da soma com 'a'.

Recuperação de senha e análise de frequência

Para decifrar uma mensagem cifrada com a técnica de Vigenère, uma das estratégias é realizar o ataque pela análise de frequência de repetição de letras, dígrafos e trigramas.
Neste projeto, foram desenvolvidas funções para quebrar a cifra por meio da análise de frequência, considerando os idiomas inglês e português, que estão disponíveis em https://pt.wikipedia.org/wiki/Frequência_de_letras.
Para utilizar o programa, o usuário deve fornecer a mensagem cifrada que deseja decifrar o idioma da mensagem e analisar as frequências para escolher um tamanho de chave.
Para executar o ataque, foram criadas funções para remover caracteres que não são minúsculos da cifra, avaliar o tamanho/frequência das letras da chave e realizar o ataque por frequência de letras.
A função estimarTamanhoChave analisa a cifra e retorna um valor para o tamanho da chave, que pode ser escolhido pelo usuário com base na análise de repetições de letras e trigramas.
Já a função ataque recebe a cifra, o tamanho da chave e o idioma da cifra e retorna a chave em potencial. Além disso, a chave e a mensagem decifrada são exibidas no terminal para o usuário.

Na implementação feita neste projeto, a cifra fornecida pelo usuário é analisada e são mostrados 10 possíveis tamanhos de chave com base na frequência de letras.
O usuário deve escolher um tamanho de chave, começando pelos maiores tamanhos até conseguir decifrar a mensagem corretamente.
Para realizar o ataque, a função ataque mapeia as frequências dos idiomas português e inglês, além da frequência da cifra recebida. Em seguida, são realizados cálculos para saber a diferença entre a frequência do idioma e a frequência da cifra recebida, a fim de determinar a chave de decifração da mensagem.

Desafios de ataque

Desafio 1

cifra

rvgllakieg tye tirtucatzoe. whvnvvei i winu mpsecf xronieg giid abfuk thv mfuty; wyenvvvr ik ij a drmg, drzzqly eomemsei in dy jouc; wyenvvvr i wied mpsvlf znmollnkarzlp palszng seworv cfffzn narvhfusvs, rnd srzngznx up khv rerr ff emeiy flnvrac i deek; aed ejpvcirlcy wyeeevvr dy hppfs gvt jucy ae upgei haed ff mv, tyat zt ieqliies r skroeg dorrl grieczplv tf prvvvnt de wrod dvliseiatvlp stvpginx ieto khv stievt, aed detyouicrlcy keotkieg geoglv's hrtj ofw--tyen, z atcolnk it yixh tzmv to xek to jer as jofn aj i tan. khzs ij mp susskitltv foi pzstfl rnd sacl. wzty a pyicosfpyicrl wlolrzsh tako tyrfws yidsecf lpoe hzs snoid; i huzetcy kakv tf thv syip. khvre zs eotyieg slrgrijieg ie tyis. zf khep blt keen it, rldosk acl mvn zn tyezr dvgiee, jode tzmv or ftyer, thvrijh merp nvarcy khe jade fvecinxs kowrrus tye fcern nity mv.

chave

arara

mensagem

regulating the circulation. whenever i find myself growing grim about the mouth; whenever it is a damp, drizzly november in my soul; whenever i find myself involuntarily pausing before coffin warehouses, and bringing up the rear of every funeral i meet; and especially whenever my hypos get such an upper hand of me, that it requires a strong moral principle to prevent me from deliberately stepping into
the street, and methodically knocking people's hats off--then, i account it high time to get to sea as soon as i can. this is my substitute for pistol and ball. with a philosophical flourish cato throws himself upon his sword; i quietly take to the ship. there is nothing surprising in this. if they but knew it, almost all men in their degree, some time or other, cherish very nearly the same feelings towards the ocean with me.

Desafio 2

cifra

tpsja kexis ttgztpb wq ssmil tfdxf vsetw ytafrttw btzf pcbroxdzo zn tqac wix, bwfd s, je ahvup sd pcbqqxff lfzed d avu ytwoxavneh sg p aznst qaghv. sfiseic f udh zgaurr dxnm rcdentv btzf nllgubsetz, wymh qfndbhqgotopl qq asmactq m prftlk huusieymi ythfdz: t tdxavict i cjs vu yts edi grzivupavnex yy pikoc wirjbko, xtw gb rvffgxa pikoc, iedp elex t gmbdr fzb sgiff bpkga; p gvgfghm t ele z xwogwko qbgmgwr adlmy bozs rtpmchv e xtme ccmo. xhmetg, hup meyqsd czgxaj o jul fsdis, eaz t tah bf iymvaxhf, mll ra roso: objqgsecl kepxqrl pgxdt sjtp emhgc v o axrfphvunh. huic zseh, ijewiet tw pjoj hzkee so kacwi pt ida dxbfp-tvict ha bsj dp tkahhf dp 1869, ge yxbya mxpm rvrclke pt qrtfffu. iwehl nre hsjspgxm t elaeks mccj, rtcse t diodiiddg, vrl lsxiszrz, isehiza nxvop rv tcxdqchfs nhrfdg v ffb eodagayaepd of cpfmftfzo ahv acnv axbkah. cezp tquvcj! vpkhmss v qfx rmd vfugx gmghrs yxq mciecthw. mrfvsnx ugt qyogbe — btbvictzm jar csnzucvr mtnhm, ifzsex i odbjtlgxq, iof czgwfpbke p mea ifzsex, ugt zvvzn yy sohupeie uwvid we gahzml asdp o znexvopzrr plxm tbxeyasep wuett ra swjcfkwa fiv pchjqgwl a mxmdp rv mtglm rcma: — “ghw, cjs f czglqrsjtpl, qqjg jeyasdtg, mod isptwj dtsid rcdirh ugt o eaenvqoo gacxgq tgkac vlagoedz t tqgrr ickibpfrvpe hq ja uod feuh pvlzl gmgottpkie fiv tpf lacfrdz t lgboeiothq. tgke lk wabpiiz, xwfpg xoetw pd qvu, ljyqaoj nfoizh sjcfkee fiv czuvqb c rzfe gabc lm nkibt tlnpkia, iiuo tlwa t o uoc vvgp s da bni xws iot t rmiiiekt ee bozs tgxuboj eymvmcvrs; enha xgjo p nq ejpcixx pajjfr lh rahgf iwnwfgs wiytha.” qcd e qbix pazgz! gea, cof mp tvdtdvnoh hmh jznex ebdzzcpl ugt zye oxmjtw. v fzb eehwd qfx gttulet t gxpijuwt hah avud wmmh; tfi llwub ele xx izrodiyaiu eoia z nrpxgtogxvqs qfuymvk ss yaxeif, hsd ad âgwupg eex tw pjjzdll ha bcto akmzrwge,

xtw bpijaoh i fgcgerh gabc hupf wq gskict xmgrv dz xwbthrcfes. fpfue p tfagfvctws. hxfrmxx md jars yhzq di uek iiehcrs, pgxdt scad mvqh gvnshvmh, aznst mdbo jambrm, rojaot gab c toekmy, p tzlst, — yy awiiz ws hpzv, — e... exrtpa ganbizrwr! dljyu p dfunh pttg uicxm cjsd ect e ftftetke etbyoct. gachvnexq-et rv sluid fiv edle mcceixt, eucrr qfx rmd drrpgxm, eouenxy ypwj dz jyq pg gacxrfpg. v vpkhmss, gaoxgqj arid. gea swxo bni et qrrabwet, bro obka fiv sp wiumojsp ksxpf gewh gtpc, toyoyxho. eex h qqj csieh idp qfidt exiodeymi pgodaebgm... ja jowmiugof qfx ijewia lhw etgjeyme q firtch ezdg, eaz iedtqv qfx vqjbr ex lm fdrfs zl ixtavnehw pt ida ekestrza. p wepd ele dbq, a fiv mpgse rcevtglm p sjsl tracwda pke meoieyme-xd. rv pp, t gmqstetke pp qrml, vsy dg flshw qhhlptwse, p pfcl xrfgsrbpkxm, p hiidmi etbyoct qma dfdtt gdtf ea xbrtp sottggmd.

chave

temporal

mensagem

algum tempo hesitei se devia abrir estas memorias pelo principio ou pelo fim, isto e, se poria em primeiro lugar o meu nascimento ou a minha morte. suposto o uso vulgar seja comecar pelo nascimento,
duas consideracoes me levaram a adotar diferente metodo: a primeira e que eu nao sou propriamente um autor defunto, mas um defunto autor, para quem a campa foi outro berco; a segunda e que o escrito ficaria assim mais galante e mais novo. moises, que tambem contou a sua morte, nao a pos no introito, mas no cabo: diferenca radical entre este livro e o pentateuco. dito isto, expirei as duas horas da tarde de uma sexta-feira do mes de agosto de 1869, na minha bela chacara de catumbi. tinha uns sessenta e quatro anos, rijos e prosperos, era solteiro, possuia cerca de trezentos contos e fui acompanhado ao cemiterio por onze amigos. onze amigos! verdade e que nao houve cartas nem anuncios. acresce que chovia — peneirava uma chuvinha miuda, triste e constante, tao constante e tao triste, que levou um daqueles fieis da ultima hora a intercalar esta engenhosa ideia no discurso que proferiu a beira de minha cova: — “vos, que o conhecestes, meus senhores, vos podeis dizer comigo que a natureza parece estar chorando a perda irreparavel
de um dos mais belos caracteres que tem honrado a humanidade. este ar sombrio, estas gotas do ceu, aquelas nuvens escuras que cobrem o azul como um crepe funereo, tudo isso e a dor crua e ma que lhe roi a natureza as mais intimas entranhas; tudo isso e um sublime louvor ao nosso ilustre finado.” bom e fiel amigo! nao, nao me arrependo das vinte apolices que lhe deixei. e foi assim que cheguei a clausula dos meus
dias; foi assim que me encaminhei para o undiscovered country de hamlet, sem as ânsias nem as duvidas do moco principe, mas pausado e tropego como quem se retira tarde do espetaculo. tarde e aborrecido. viramme ir umas nove ou dez pessoas, entre elas tres senhoras, minha irma sabina, casada com o cotrim, a filha, — um lirio do vale, — e... tenham paciencia! daqui a pouco lhes direi quem era a terceira senhora. contentem-se de saber que essa anonima, ainda que nao parenta, padeceu mais do que as parentas. e verdade, padeceu mais. nao digo que se carpisse, nao digo que se deixasse rolar pelo chao, convulsa. nem o meu obito era coisa altamente dramatica... um solteirao que expira aos sessenta e quatro anos, nao parece que reuna em si todos os elementos de uma tragedia. e dado que sim, o que menos convinha a essa anonima era aparenta-lo. de pe, a cabeceira da cama, com os olhos estupidos, a boca entreaberta, a triste senhora mal podia crer na minha extincao.

Conclusão

O código em c++ implementa funções de cifragem e decifragem usando a cifra de Vigenère, que é vulnerável a ataques de recuperação de senha por análise de frequência. Embora essa cifra tenha sido usada historicamente por sua segurança, ela é agora considerada relativamente fraca e facilmente quebrável com técnicas modernas de criptoanálise. Em relação ao código, foi um desafio fazer em c++ visto a sintaxe da linguagem e a falta de experiência do programador na linguagem. As referências dada pelo monitor e os sites procurados também ajudaram bastante na implementação.

Referências:

https://www.cs.du.edu/~snarayan/crypt/vigenere.html -> site para codificar e decodificar vigenere

https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher -> explicação da cifra

https://www.youtube.com/watch?v=SkJcmCaHqS0 -> aprofundamento da cifra

https://www.youtube.com/watch?v=LaWp_Kq0cKs&t=6s -> quebra da cifra

https://www.youtube.com/watch?v=P4z3jAOzT9I -> quebra da cifra