E-fólio A | Folha de resolução para E-fólio

UNIDADE CURRICULAR: Segurança em Redes e Computadores

CÓDIGO: 21181

DOCENTE: Professor Henrique São Mamede

A preencher pelo estudante

NOME: Francisco José Pinto de Amaral

N.º DE ESTUDANTE: 1802876

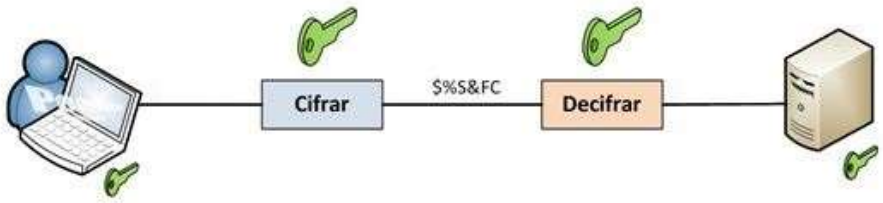
CURSO: Licenciatura em Engenharia Informática

DATA DE ENTREGA: 23-11-2021

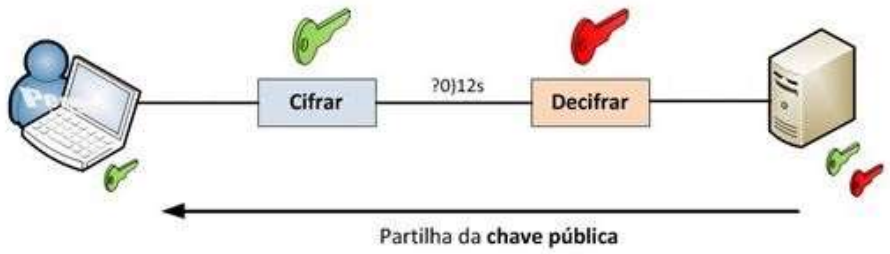
TRABALHO / RESOLUÇÃO:

RELATÓRIO:

Designa-se por cifra simétrica um sistema convencional de chave única (ou chave secreta) usada por ambos interlocutores e na premissa que esta seja conhecida apenas por eles de forma a privacidade e a autenticidade. A desvantagem para este método é a troca da chave entre os dois interlocutores, o processo deve ser feito em segurança de forma que uma terceira pessoa não tenha conhecimento da mesma, toda a segurança é refletida na chave.

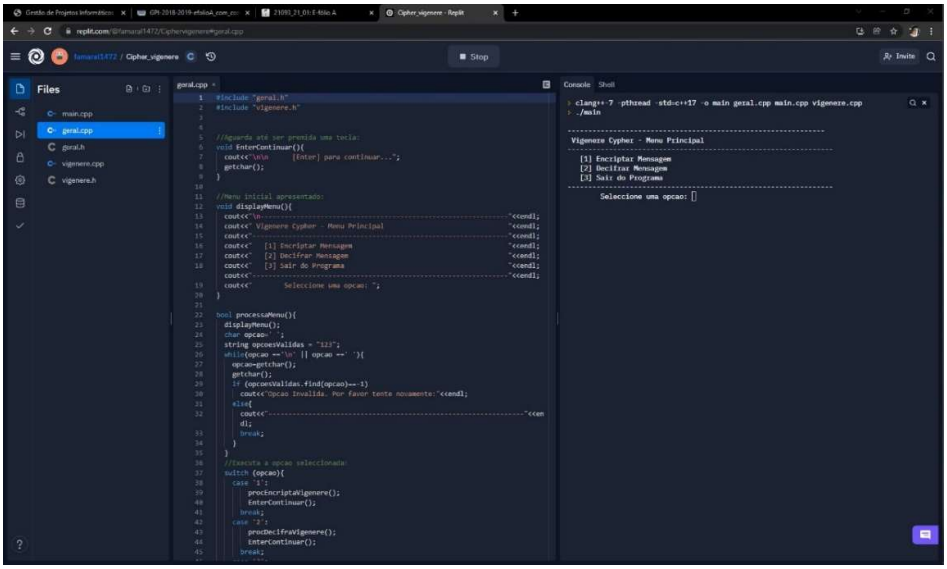


Designa-se por cifra assimétrica aquela que utiliza duas chaves: uma chave privada e uma chave pública. Esta é a cifra mais utilizada por ser mais prática, a chave pública é distribuída livremente para todos os correspondentes via email ou outras formas enquanto a chave privada é para uso exclusivo do criador dos pares de chaves para cifrar decifrar mensagens de forma segura. O uso desta cifra surge como uma parte fundamental da segurança da internet (p.e. Blockchain) permitindo que haja sigilo de informação e que a mensagem/conteúdo não foi alterada.

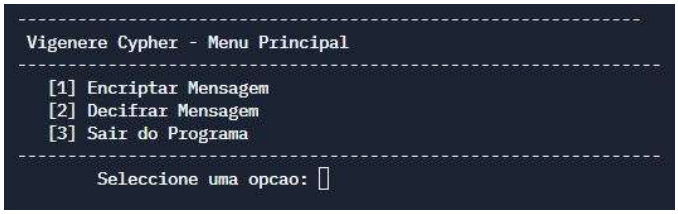


Para implantação das cifras solicitadas neste trabalho escolhi a linguagem de programação **C++** no qual o código foi desenvolvido em um **IDE Web – www.replit.com** que tem como Sistema Operativo base o **ubuntu0.18.04.1 ~ clang version 7.0.0-3.**

Para a **Cifra Simétrica** escolhi a mais simples e mais conhecida dentro das Cifras Polialfabeticas de Substituição – a ***Vigenère Cipher*** – de acordo com a página 102 do manual adotado - Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. 7th Edition (Global Edition), Prentice Hall.



O Menu inicial tem 3 opções: “[1] Encriptar Mensagem”, “[2] Decifrar Mensagem” e “[3] Sair do Programa”. Pedindo para selecionar uma das três opções.



O domínio do texto compreende todos os caracteres pela constante “DOM_INF” e “DOM_SUP” que são todos os caracteres visíveis da tabela ASCII Standard do caracter 32 ao 126. Os restantes caracteres da tabela foram ignorados devido a questões de acentuação nas diferentes linguagens/teclado a nível internacional (p.e. ñ).

Na Encriptação cada caracter do texto cifrado é obtido deslocando o respetivo caracter do texto original (*plaintext*) um determinado número de posições ao longo da tabela ASCII. O número de posições a deslocar é determinado a partir do código ASCII de um dos caracteres da chave secreta.

De acordo com a equação para encriptação da página 103 (3.3): $Ci = (pi + ki \ mod \ m) \bmod 26$, o mod 26 são as 26 letras em maiúsculo. Neste caso específico como utilizei mais

do que os 26 caracteres será *mod 94* sendo que vai do código ASCII 32 ao 126 conforme supra explicado.

No caso da chave ser mais curta do que a mensagem (texto original – *plaintext*) o programa repete a chave, no caso da chave ser mais longa que a mensagem ele ignora os caracteres adicionais. ($ki \ mod \ m$) em que *m* é o comprimento de caracteres da chave.

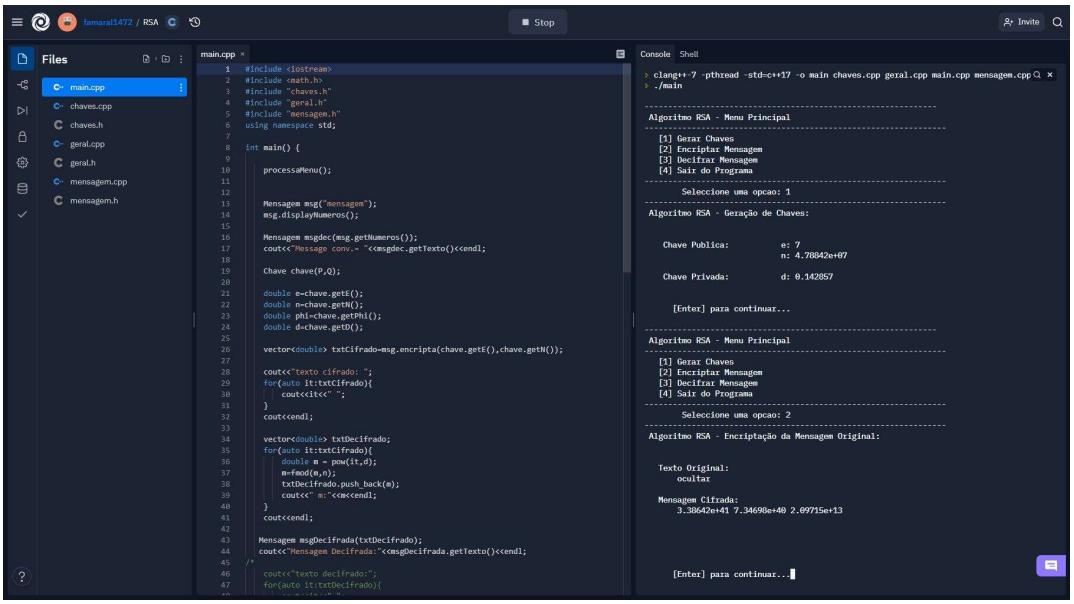
Se a chave tiver apenas um caracter, todos os caracteres do texto cifrado irão ser obtidos aplicando o mesmo deslocamento ao texto original, isto é, o algoritmo comporta-se como a cifra de César.

Para decifrar a mensagem o programa comporta-se da mesma forma á exceção do deslocamento ser feito no sentido contrário, em vez da uma soma temos uma subtração conforme as próprias equações demonstram:

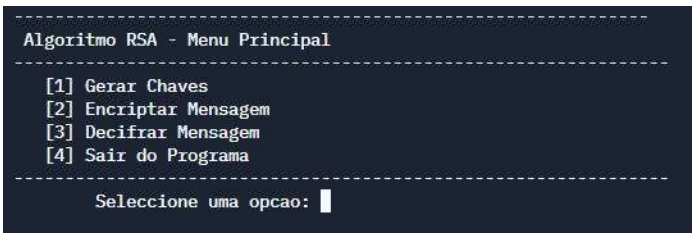
$$C_i = (p_i + k_{i \bmod m}) \bmod 26 \qquad \text{e} \qquad p_i = (C_i - k_{i \bmod m}) \bmod 26.$$

NOTA – Apesar da bibliografia adotada mencionar equações, por exemplo a (3.3) fugi um pouco ao mencionado para mostrar domínio sobre o assunto em questão, usar apenas letras maiúsculas (mod 26) seria uma cópia do que está no manual.

Para a **Cifra Assimétrica** escolhi o Algoritmo RSA criado por Ron **R**ivest, Adi **S**hamir e Len **A**dleman, as iniciais de cada apelido dão nome á cifra em questão – RSA – de acordo com a secção 9.2 (página 294) do manual adotado - Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. 7th Edition (Global Edition), Prentice Hall.



O Menu inicial, neste caso de cifra assimétrica tem 4 opção tendo em conta que existe a necessidade de gerar as chaves Pública e Privada, sendo: “[1] Gerar Chaves”, “[2] Encriptar Mensagem”, “[3] Decifrar Mensagem” e “[4] Sair do Programa”. Pedindo para selecionar uma das quatro opções.



A organização que vai receber a(s) mensagem(s) é que vai fornecer as chaves para encriptar a mensagem. Por exemplo: https://www.cncs.gov.pt/pt/chave-pgp/

Escolhem-se os números primos *p* e *q*, quanto maior for o número mais difícil será de fatorizar fazendo com que haja uma menor probabilidade de sofrer um ataque por força bruta. Ambos os valores de *p* e *q* multiplicados obtem-se o valor de *n* que é um valor que faz parte das duas chaves.

De seguida calculamos o totiente de *pq* (que lhe dou o nome de phi no programa) através da formula $\phi(pq) = (p-1)(q-1)$ de acordo com o manual adotado.

De formas prática, para preparar a mensagem para ser cifrada existe um trabalho de preparação que passa por transformar a mensagem em números. Esta transformação passa por obter o código ASCII de cara caracter da mensagem a encriptar e subtrair-lhe 32, após termos a nossa mensagem transformada em números dividimos a cadeia de caracteres em blocos de 3 considerando da direita para a esquerda o caracter mais á direita é multiplicado por 10^0, o do meio multiplicado por 10^2 e o da esquerda multiplicado por 10^4, somando os três múltiplos dá origem a um número de 6 números prontos a ser cifrados, aplicando de seguida o algoritmo.

Deste modo, na decifragem conseguimos aplicar o mesmo método no sentido inverso sem perder o caminho até á mensagem original.

REFERÊNCIAS BIBLIOGRÁFICAS:

Stallings, William (2007) *Cryptography and Network Security: Principles and Practice.* 7th Edition (Global Edition), Prentice Hall.

Imagens - https://pplware.sapo.pt/tutoriais/networking/criptografia-simetrica-e-assimetrica-sabe-a-diferenca/

Conteúdo fórum: Modulo 2 – Encriptação de Dados e Infraestrutura de Chave Pública, Curso Especialização em Cibersegurança – Edição 2019/2020, Universidade Aberta.

FIM