Cifra QWERTY – Método criptográfico

Abordagem teórica e apreciação de resultados

Bruno Gabriel Nunes Martins – **45206**

Pedro Pinto - **40204**

Pedro Rodrigues - **30156**

Licenciatura em Engenharia Informática

Criptografia

Orientador: Professor Doutor António Santos

Lisboa, 2022

Cifra QWERTY – Método criptográfico

Abordagem teórica e apreciação de resultados

Bruno Gabriel Nunes Martins – **45206**

Pedro Pinto - **40204**

Pedro Rodrigues – **30156**

Trabalho apresentado(a) ao **ISTEC – Instituto Superior de Tecnologias Avançadas**, na área de estudos de **Criptografia**, como requisito parcial para a avaliação contínua da cadeira (40%), sob a orientação do Professor Doutor António Santos.

Lisboa, 2022

Índice

1. Introdução

Programadores e Profissionais na área de desenvolvem software e ferramentas para a solução de um ou mais problemas expostos a partir dos Clientes que as solicitam. Muitos desses problemas estendem algumas dificuldades do nosso dia-a-dia e, por conseguinte, cada vez mais o crescimento de soluções se verificam.

Contudo, estes profissionais nunca tiveram como um dos focos principais: a implementação da segurança, seja no levantamento de requisitos ou na própria codificação devido ao facto de muitos consumidores não se importarem com este assunto.

Para muitas empresas, agregar segurança significa um maior investimento para a criação de recursos, o que por sua vez não agregava nada no aumento de vendas e valor comercial.

Em 16 de fevereiro de 2000, o Federal *Bureau of Investigation* afirma que em 1999 havia mais de 100 milhões de utilizadores na Internet nos Estados Unidos. (*Criptografia e Segurança: O Guia Oficial RSA - STEVEN BURNETT - Google Livros*, n.d.).

Pegando no dado anterior, conclui-se que para aquela data, já existia uma grande base de utilizadores expostos na Internet, o que facilmente faria com que estes utilizadores já estariam expostos a possíveis crimes cibernéticos.

Conclui-se, portanto, que o cibercrime deixou há muito de ser uma palavra desconhecida para a generalidade da população mundial, sendo cada vez mais comum a execução dos mesmos por parte de indivíduos ou mesmo nações. (André & Gonçalves, 2016)

Após este fundamento teórico, fica claro que a Segurança deve ser um dos princípios base para a construção de qualquer produto ou serviço.

A segurança deve estar presente em todo o processo da empresa, desde o planeamento até à concretização do produto em si.

As organizações devem implementar um conjunto de regras e diretrizes para as ações que são executadas nas mesmas.

Segundo normas como: **Norma ISO/IEC 27002** e a **Norma ISO/IEC 17799** (*Segurança Da Informação - Normas ISO*, 2020), dão ênfase a uma orientação e documentação necessária de acordo com os requisitos do negócio e com as leis regulamentares que definem parte do(s) processo(s) que as organizações executam.

Regras essas que definem alguns pontos importantes a ter em conta como: formas de acesso e de utilização às infraestruturas e a informações que todos os colaboradores necessitam de ter acesso para executarem as suas funções, utilização correta de equipamentos, planeamento e aceitações dos sistemas, cópias de segurança, trocas de informações, definição de controlos de acesso, treinamento e educação especializada a todos os colaboradores das organizações sobre a segurança nas mesmas e outras regras, pontos e ações a serem seguidos.

A criptografia, portanto, é uma das formas de garantir a segurança na informação, tendo como base princípios da segurança da informação, a partir de cifras (algoritmo que compreende a encriptação e a desencriptação) em que um dos **princípios fundamentais**

sublinha que, o funcionamento interno do sistema criptográfico é completamente conhecido pelo invasor, e o único segredo é a chave utilizada no processo. (Khalid et al., 2012)

No fundo, garante a **confidencialidade**, **integridade, autenticidade** e **não-repúdio** das informações. (Khalid et al., 2012)

(*Segurança Da Informação - Proteção*, 2020)

Neste relatório, será abordado um dos métodos de Cifras de Substituição - Cifra de QWERTY, também conhecido como uma das variantes da cifra de *Julio Cesar* ou *Caesar Cypher*. (QWERTY).

A cifra de QWERTY também tem outro nome, denominada de **Keyboard Shift**, sendo um método das cifras de substituições.

2. Desenvolvimento

2.1 Resumo Histórico do Modelo

Tendo em vista as questões: militares, religiosas e comerciais, promoveram-se desde os tempos remotos o uso de escritas secretas. No antigo egípcio usavam a escrita hierática, que era claramente incompreensível para o resto da população, o que podemos estar perante abordagem a metodologia criptográfica, devido a estarem a trocar o alfabeto egípcio pelos hieróglifos.

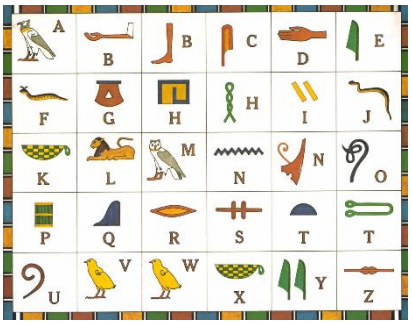


Figura 1. Representação simbólica associado a letras.

Várias formas de comunicação secreta foram extensamente usadas, como, por exemplo, a utilizada pelo **Imperador Romano Júlio César** para se comunicar com os seus generais.

César usava um sistema simples de substituição de letras, em que cada letra do alfabeto era trocada por outra letra do mesmo alfabeto, **deslocada por um x número**, onde, por exemplo, **se o x = 3**, ou seja, se for trocado no alfabeto o "a", no alfabeto encriptado seria o caracter "**d**".
A ideia da cifra de César e da sua generalização sob a forma de cifra afim, basearam, durante muitos séculos, diversos sistemas de segurança.

Hoje em dia, **denomina-se por cifra de César qualquer encriptação** que envolva substituição de cada letra original por uma letra deslocada de um número fixo de posições que não necessariamente três. Talvez a cifra de substituição mais simples seja a **cifra de César**, batizada em homenagem ao homem que a usou.

As cifras de substituição são, portanto, todas aquelas que criptografam texto simples, trocando cada letra presente no texto indicado por outro texto/símbolo conforme está indicado

na chave utilizada. (*Substitution Cipher - an Overview | ScienceDirect Topics*, n.d.)

Se eliminarmos qualquer restrição relativa à ordem dos caracteres do alfabeto cifrado, o número de potenciais chaves dispara. Se tivermos em conta o alfabeto português, pode contar-se no total:

$26! = 403291461126603635584000000$

tipos de alfabetos cifrados possíveis. (Santos, 2019).

Sabendo o método em questão, torna-se fácil fazer a sua descodificação. As seis primeiras letras do alfabeto cifrado darão uma pista para essa descoberta.

2.2 Explicação do modelo (Método QWERTY)

Vejamos este exemplo:

Texto a ser encriptado: "**OLA MUNDO"**.

$T = \text{OLA MUNDO}$

1. Montar uma matriz de 2x26 em que:
   a. Na **primeira linha** é indicado os 26 caracteres do Alfabeto de A → Z.
   b. Na **segunda linha** é indicado os caracteres com a ordem baseada no padrão de teclado QWERTY.

   c. Visualização da cifra gerada

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

Y	Z
N	M

$C = QWERTYUIOPASDFGHJKLZXCVBNM$

2. Encriptação do texto "**OLA MUNDO"**

   $C = QWERTYUIOPASDFGHJKLZXCVBNM$

   $T = \text{OLA MUNDO}$

   Para cada letra de **T**, procura-se a letra no alfabeto na **primeira linha** e**, na mesma coluna**, utiliza-se a letra na **segunda linha.**

   OLA MUNDO → GSQ DXFRG

   Portanto, $E = \text{GSQ DXFRG}$

3. Processo de desencriptação da palavra "**OLA MUNDO"**

   O processo inverso torna-se relativamente simples. Sabendo que: $E = \text{GSQ DXFRG}$, para cada letra em **E**, procura-se a letra na **segunda linha** e**, na mesma coluna**, utiliza-se a letra na **primeira linha.**

   GSQ DXFRG → OLA MUNDO

   Portanto, $D = \text{OLA MUNDO}$

2.2 Explicação do modelo (Método Palavra-chave customizada)

Existe uma variante na cifra de QWERTY que apresenta uma abordagem mais simplificada e customizada.

Dá a possibilidade de a cifra gerada ser baseada a partir de uma **palavra-chave**. Esta palavra-chave fará parte da cifra, colocada no princípio da mesma, deixando os restantes caracteres concatenados à dita palavra. Este método permite gerar um grande porte de cifras. (Santos, 2019).

Vejamos outro exemplo:

$T = \text{ISTEC}$

Palavra-Chave = **CRIPTOGRAFIA**

1. Montar uma matriz de 2x26 em que:

   a. Na **primeira linha** é indicado os 26 caracteres do Alfabeto de A → Z.
   b. Na **segunda linha** os primeiros caracteres da **palavra-chave**, seguindo os restantes caracteres com a ordem baseada no padrão de teclado QWERTY. É importante verificar se o caracter já se encontra presente na palavra. Se não existir, o caracter é inserido.

   A **palavra-chave** Criptografia tem os caracteres: **"i"**, **"a" e "r"** repetidos. Nestes casos, a partir de cada segunda ocorrência, os caracteres repetidos serão removidos.

   CRIPTOGRAFIA → CRIPTOGAF

   c. Visualização da cifra customizada gerada

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

Y	Z
B	M

Portanto, a cifra gerada**:**

$C = CRIPTOGAFQWEYUSDHJKLZXVBNM$

2. Encriptação do texto **"ISTEC"**

   Para cada letra de **T**, procura-se a letra no alfabeto na **primeira linha** e**, na mesma coluna**, utiliza-se a letra na **segunda linha.**

   ISTEC → FKLTI

   Portanto, $E = \text{FKLTI}$

3. Processo de desencriptação da palavra **"ISTEC"**

   O processo inverso torna-se relativamente simples e igual ao método de QWERTY padrão.
   Novamente, para cada letra em **E**, procura-se a letra na **segunda linha** e**, na mesma coluna**, utiliza-se a letra na **primeira linha.**

   FKLTI → ISTEC

   Portanto, $D = \text{ISTEC}$

3. Desenvolvimento

3.1 Algoritmo em Linguagem Natural

Para a componente prática desde projeto, foi feito a codificação deste método criptográfico. Para representar os algoritmos em linguagem natural, foi utilizado a abordagem de pseudocódigos. (DEITEL & DEITEL, 1986)

O pseudocódigo consiste em frases curtas em inglês usadas para explicar tarefas específicas dentro de um programa. Idealmente, o pseudocódigo não deve incluir palavras-chave em nenhuma linguagem de computador específica. (*Pseudocode - an Overview | ScienceDirect Topics*, n.d.)

Pseudocódigos criados:

1. QWERTY – Encriptação
2. QWERTY customizada – Encriptação
3. QWERTY – Desencriptação

3.2 Algoritmo – QWERTY Encriptação

```
VARIÁVEIS
alfabeto, cifra, frase, texto_encriptado: vetor[caracter];

INICIO
      alfabeto ← "abcdefghijklmnopqrstuvwxyz"
      cifra ← "qwertyuiopasdfghjklzxcvbnm"

      ESCREVER ("Indique a frase a ser encriptada pelo método QWERTY")
      LER(frase)

      PARA posicao_letra = 0 ATÉ tamanho(frase) FAZ

        PARA i posicao_cifra = 0 ATÉ tamanho(cifra) FAZ
              SE alfabeto[posicao_cifra] = frase[posicao_letra] ENTÃO
                    texto_encriptado ← cifra[posicao_cifra]
              SENÃO
                   SE frase[posicao_letra] = " "
                       texto_encriptado ← " "
                  FIM SE
              FIM SE
        FIM PARA

    FIM PARA
FIM
```

3.3 Algoritmo – QWERTY customizada - Encriptação

```
VARIÁVEIS
alfabeto, cifra_qwerty, cifra_customizada, frase, texto_encriptado:
vetor[caracter];

FUNCAO gerar_cifra (palavra: literal): literal
      // Declarar uma variável local para o processo de gerar cifra
      vetor[caracter] qwerty_aux;

      qwerty_aux ← cifra_qwerty
      palavra ← removerCaracteresDuplicados(palavra) // ex. antonio -> antoi

       // Remover caracteres existentes na palavra inserida da cifra qwerty
       PARA posicao = 0 ATÉ tamanho(palavra) FAZ
            qwerty_aux = qwerty_aux.trocar(palavra[posicao], "")
       FIM PARA

        // exemplo → antoi com qweryupsdfghjklzxcvbm =
antoiqweryupsdfghjklzxcvbm
        Retornar concatenar_strings(palavra, qwerty_aux)
FIM FUNCAO
```

```
INICIO
      alfabeto ← "abcdefghijklmnopqrstuvwxyz"
       cifra_qwerty ← "qwertyuiopasdfghjklzxcvbnm"

      ESCREVER("Indique a frase a ser encriptada pelo método QWERTY")
      LER(frase)

      ESCREVER("Indique o texto da cifra a ser considerado para a
encriptação.")
      LER(cifra_customizada)

       cifra_customizada = gerar_cifra(cifra_customizada)

 PARA posicao_letra = 0 ATÉ tamanho(frase) FAZ
      PARA i posicao_cifra = 0 ATÉ tamanho(cifra_customizada) FAZ
            SE alfabeto[posicao_cifra] = frase[posicao_letra] ENTÃO
                  texto_encriptado ← cifra_customizada[posicao_cifra]
            SENÃO
                  SE frase[posicao_letra] = " "
                       texto_encriptado ← " "
                   FIM SE
            FIM SE
       FIM PARA
```

3.4 Algoritmo – QWERTY Desencriptação

```
VARIÁVEIS
alfabeto, cifra, frase, texto_encriptado, texto_normal: vetor[caracter];

INICIO
      alfabeto ← "abcdefghijklmnopqrstuvwxyz"
      cifra ← "qwertyuiopasdfghjklzxcvbnm"
      texto_encriptado ← "gsq dxfrg"

      PARA posicao_letra = 0 ATÉ tamanho(frase) FAZ

        PARA i posicao_cifra = 0 ATÉ tamanho(cifra) FAZ
              SE cifra[posicao_cifra] = frase[posicao_letra] ENTÃO
                    texto_normal ← alfabeto[posicao_cifra]
              SENÃO
                   SE frase[posicao_letra] = " "
                        texto_normal ← " "
                   FIM SE
              FIM SE
        FIM PARA

    FIM PARA

    // texto_normal = ola mundo
FIM
```

3.5 Demonstração de resultados com o programa codificado

Para construção do programa, foi utilizado a linguagem de Programação **Python**, contendo as seguintes funcionalidades:

1. QWERTY Método de Encriptação
2. QWERTY Método customizado de Encriptação

Na simulação, o programa interpreta e processa o texto que será encriptado, aplicando a função. lower(), que transforma cada caracter para a sua forma minúscula.

Este processo é essencial para garantir a consistência entre as cifras e evitar possíveis bugs.

O programa também está preparado para reconhecer e inserir *whitespaces* de forma automática. Em bom rigor, os *whitespaces* também são inseridos na cifra.

Os dados foram os seguintes:

3.5.1 QWERTY Método de Encriptação

Texto a ser encriptado: Projeto Criptografia

```
----------------- LEI Turma B -----------------

Realizado por: Pedro Pinto, Bruno Martins e Pedro Rodrigues


Shift/Keyboard Cipher - selecione uma das opções abaixo:

1 - Qwerty method
2 - Alphabet with custom cypher method
0 - Finish the program

>> 1

Write your text to be encoded using QWERTY cypher:
>>
```

Escolhendo a opção **1** e colocando o texto pretendido, o resultado gerado apresenta-se da seguinte forma:

```
>> 1

Write your text to be encoded using QWERTY cypher:
>> Projeto Criptografia
----------------- Results ----------------

Text encrypted:  hkgptzg ekohzgukqyoq
Text decrypted:  projeto criptografia

Press ENTER to return to menu
```

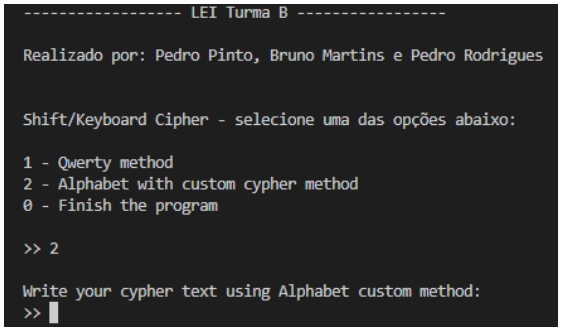
$C = QWERTYUIOPASDFGHJKLZXCVBNM$

$E = HKGPTZG\ EKOHZGUKQYOQ$

Pressionando a tecla ENTER, é possível reiniciar a aplicação e testar, por exemplo a segunda alternativa/proposta deste projeto.

3.5.2 QWERTY Método customizado de encriptação

Escolhendo a opção **2** e colocando o texto pretendido, o resultado gerado apresenta-se da seguinte forma:



O primeiro input solicitado ao utilizador será a **palavra-chave** a ser considerada para a construção.

Importante reforçar que frases/palavras como:

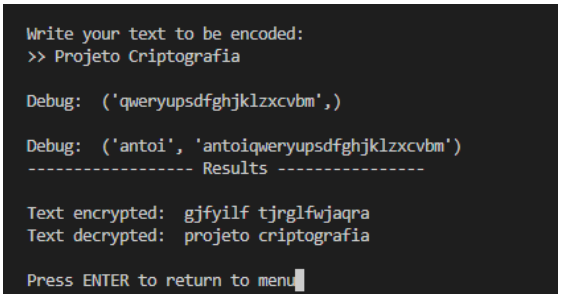
- ANTONIO
- CRIPTOGRAFIA
- OLA ANA
- PROJETO CRIPTOGRAFIA
- HELLO WORLD

Terão, como critério, a remoção de caracteres repetidos, conforme mencionado acima. Ficam, portanto:

- ANTOI
- CRIPTOGAF
- OLA N
- PROJET CIGAF
- HELO WRD

Ainda na simulação, a palavra-chave indicada foi: “antonio” e o texto a ser encriptado foi **“**Projeto Criptografia”.

Vejamos os resultados:



Após a análise de resultados, comprova-se o processamento correto da palavra-chave “antonio”.

A palavra-chave não poderá conter caracteres repetidos.

$C = ANTOIQWERYUPSDFGHJKLZXCVBM$

$E = GJFYILF\ TJRGLFWJAQRA$

4. Conclusão

TBD

5. Bibliografia

André, J., & Gonçalves, P. (2016). Enquadramento legal da Cibersegurança em Portugal e no Mundo [EN - Escola Naval]. In *EN - TMI - Curso Marinha*. https://comum.rcaap.pt/bitstream/10400.26/15040/1/ASPOF EN-M Pinto Gonçalves 2016.pdf

Criptografia e segurança: o guia oficial RSA - STEVEN BURNETT - Google Livros. (n.d.). Retrieved December 23, 2022, from https://books.google.pt/books?hl=pt-PT&lr=&id=DIskNhcTUNoC&oi=fnd&pg=PR11&dq=Criptografia&ots=H1rrWFlpJj&sig=5V9AlMhw_4yLp46YDV1Gm8e--5g&redir_esc=y#v=onepage&q=Criptografia&f=false

DEITEL, H. M., & DEITEL, B. (1986). Structured Programming. *An Introduction to Information Processing*, 184–217. https://doi.org/10.1016/B978-0-12-209005-9.50015-1

Khalid, M., Rahmani, I., Wadhwa, N., & Malhotra, V. (2012). ALPHA-QWERTY CIPHER: AN EXTENDED VIGENÈRE CIPHER. *Advanced Computing: An International Journal (ACIJ)*, *3*(3). https://doi.org/10.5121/acij.2012.3311

Pseudocode - an overview | ScienceDirect Topics. (n.d.). Retrieved January 7, 2023, from https://www.sciencedirect.com/topics/engineering/pseudocode

Santos, A. (2019). *Criptografia - Segurança e Vulneralidade - Vulnerabilidades* (p. 217). https://drive.google.com/drive/u/1/folders/105-Cpfvs3tlHZ-1BBm1qtfIcOYOCvdtJ

Segurança da Informação - Normas ISO. (2020). 09/11/2020. https://sway.office.com/zmeXRtfIkicKDkZ8?ref=Link

Segurança da Informação - Proteção. (2020). 03/11/2020. https://sway.office.com/tgcDY6ppSmaYbLzO?ref=Link

Substitution Cipher - an overview | ScienceDirect Topics. (n.d.). Retrieved January 7, 2023, from https://www.sciencedirect.com/topics/computer-science/substitution-cipher