UNESP - BAURU Bacharelado em Sistemas de Informações

Sistema de Criptografia

Avaliação - João Milone (BSI)

1) Introdução:

O sistema utilizado para criar a criptografia foi de chave simétrica, onde a chave consiste em uma sequência de caracteres desejados para serem criptografados e esta sequência será revertida para criar uma outra sequência que possui os mesmos caracteres. Ou seja, cada caracter tem sua referência na sequência invertida. Este método de criptografia foi pensado para ser utilizado em trocas de mensagens pela internet. Onde a mensagem seria criptografada e enviada por um dos mensageiros e quando chegar no destino ser descriptografada pelo mensageiro para o outro usuário conseguir entender. Ou seja, caso a mensagem seja interceptada no meio do caminho ela seria incompreensível aos olhos de quem capturou.

2) A sequência escolhida:

Foi escolhida uma sequência de caracteres comuns de usos em mensagens e textos online. Onde ficaria praticamente impossível de se decifrar uma mensagem caso ela fosse interferida sem conhecimento prévio de como ocorreu a criptografia.

A sequência em questão é essa:

abcdefghijklmnopqrstuvwxyzáàãâéèêíìîóòôãÁÀÂÁÉÈÊÍÌÎÓÒÕÔABCDEFGHIJKLMNOPQRS TUVWXYZ0123456789-= ,.!?#()

E sua inversa por consequência:

)(#?!.,

=-9876543210ZYXWVUTSRQPONMLKJIHGFEDCBAÔÕÒÓÎÌÍÊÈÉÃÂÀÁõôòóîìíêèéâãàázyx wvutsrqponmlkjihgfedcba

3) Algoritmo:

O algoritmo funciona de forma bem simples, na hora de criptografar, irá passar de letra em letra no texto e irá pegar a posição de cada uma na sequência normal para ver qual a sua equivalente na sequência invertida. Como um exemplos de textos criptografados temos abaixo:

Texto normal:

Salve galera, onde que eu boto o saco de batata?

DESLIGA O FREEZER A NOTCHE!

Texto criptografado:

à)8Y!h,)8!2)gh56?!h3Z!h!Zh(505h5h1)#5h?!h()0)0)d ÂÀàìòõÈhèhÁãÀÀuÀãhÈhêèáÃôÀe

4) Código fonte:

```
public partial class frmDecripto : Form
        string chaveNormal =
"abcdefghijklmnopqrstuvwxyzáàãâéèêíìîóòôõÁÀÂÃÉÈÊÍÌÎÓÒÕÔABCDEFGHIJKLMNOPQ
RSTUVWXYZ0123456789-= ,.!?#()", chaveCripto = ")(#?!.,
=-9876543210ZYXWVUTSRQPONMLKJIHGFEDCBAÔÕÒÓÎÌÍÊÈÉÃÂÀÁÕôÒÓÎÌÍêèéâãàázyxwvu
tsrqponmlkjihgfedcba";
        public frmDecripto()
        {
            InitializeComponent();
        }
        private void btnCripto_Click(object sender, EventArgs e)
            Criptografar();
        }
        private void btnDecripto Click(object sender, EventArgs e)
            Descriptografar();
       void Descriptografar()
        {
            if (txtTextoDescripto.Text.ToString() == string.Empty)
                return;
            string textoParaCriptografar = "" , txtTextoCriptografado =
txtTextoDescripto.Text.ToString();
            for (int i = 0; i < txtTextoCriptografado.Length; i++)</pre>
                textoParaCriptografar +=
DescriptografarLetra(txtTextoCriptografado[i]);
            txtTextoCriptografar.Text = textoParaCriptografar;
            txtTextoDescripto.Text = "";
        void Criptografar()
```

```
if (txtTextoCriptografar.Text.ToString() == string.Empty)
                return;
            string textoParaCriptografar =
txtTextoCriptografar.Text.ToString(), txtTextoCriptografado = "";
            for (int i = 0; i < textoParaCriptografar.Length; i++)</pre>
            {
                txtTextoCriptografado +=
CriptografarLetra(textoParaCriptografar[i]);
            txtTextoCriptografar.Text = "";
            txtTextoDescripto.Text = txtTextoCriptografado;
        }
        char CriptografarLetra(char letraRef)
        {
            char letra = letraRef;
            int idNaChave = -1;
            for (int i = 0; i < chaveNormal.Length; i++)</pre>
                if (chaveNormal[i] == letra)
                    idNaChave = i;
            }
            if (idNaChave == -1)
                return letra;
            else
                return chaveCripto[idNaChave];
        char DescriptografarLetra(char letraRef)
            char letra = letraRef;
            int idNaChave = -1;
            for (int i = 0; i < chaveCripto.Length; i++)</pre>
            {
                if (chaveCripto[i] == letra)
                    idNaChave = i;
            }
            if (idNaChave == -1)
```

```
return letra;
else
    return chaveNormal[idNaChave];
}
```