MSX Article

Criptografia no MSX

Fulswrjudild qr PVZ

Resumo

O objetivo deste artigo é demonstrar algumas técnicas de criptografia no MSX.

1. Introdução

A criptografia (do grego: kryptós = escondido, graphein = escrita) é o estudo de técnicas para a transformação de uma informação de sua forma original para outra ilegível, de forma que possa ser compreendida apenas por seu destinatário, evitando assim que a informação possa a ser descoberta por pessoas não autorizadas. O receptor possui uma espécie de chave, que permite transformar o texto ilegível de volta a seu estado original.

Adaptado de: http://pt.wikipedia.org/wiki/Criptografia

2- Técnicas de Criptografia

2.1. A Cifra de César (Caesar Cipher Cryptography)

O imperador romano Júlio César (100 a.C. - 44 a.C.) já utilizava textos cifrados (criptografados) para se comunicar com os seus generais. A técnica utilizada na época recebeu seu nome.

Essa técnica é uma das mais simples e consiste na troca de uma letra do alfabeto por outra, distante dela um número fixo de vezes. No caso do Império Romano, a troca era feita por letras distantes três posições à frente.

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

Tabela 1. A cifra de César

Observando a tabela 1, a frase “o coelho come a cenoura” ficaria “R FRHOK FRPH D FHQRXUD”.

Adaptado de: http://pt.wikipedia.org/wiki/Cifra_de_Cesar

2.2. Deslocamento da Tabela ASCII

A técnica da Cifra de César pode ser extendida para a tabela ASCII, utilizada para representar letras, números e símbolos em computação.

Do mesmo modo que é feito na Cifra César, um caractere é substituído por outro da tabela ASCII (não necessáriamente outra letra), distante n posições adiante ou para trás.

Por exemplo, a palavra “casa” possui os seguintes códigos ASCII:

Caractere	c	a	s	a
Código ASCII	99	97	115	97

Ao deslocarmos os caracteres de “casa” 64 posições para trás, o resultado seria:

Texto Original	c	a	s	a
Código ASCII	99	97	115	97
Deslocamento	-64	-64	-64	-64
Novo Código ASCII	35	33	51	33
Texto Cifrado	#	!	3	!

A palavra “casa” cifrada torna-se “#!3!”, no qual é ilegível.

Para se obter de volta a palavra original, deve-se realizar a operação inversa da cifragem, ou seja, somar 64 posições a cada caractere. O ato de “somar 64” é a chave para o receptor decifrar o texto.

Esta técnica pode ser utilizada para esconder textos de jogos e aplicações. Entretanto, não deve ser aplicada ao código de máquina do programa, pois ele se tornaria “ilegível” também para o computador.

Código em Basic para cifrar um texto:

```
10 M$="mensagem a ser cifrada"
20 D=2
30 MC$=""
40 FOR C=1 TO LEN(M$)
50 CC = (ASC(MID$(M$,C,1)) + D) MOD 256
60 MC$ = MC$ + CHR$(CC)
70 NEXT C
80 PRINT "Original: ";M$
90 PRINT "Cifrada: ";MC$
```

Saída:
Original: mensagem a ser cifrada
Cifrada: ogpucigo"c"ugt"ekhtcfc

A variável *D* é a chave e controla o deslocamento.

A instrução MOD é utilizada para realizar o deslocamento circular. Não é necessário, caso o tipo de variável seja inteiro não-sinalizado de 1 byte apenas. No MSX, a variável inteira possui 2 bytes, a de simples precisão 4 e dupla precisão 8 bytes.

Para decodificar a mensagem cifrada anteriormente, basta aplicar o mesmo deslocamento, só que no sentido inverso. Acrescente as seguintes linhas ao programa anterior:

```
100 IF D<0 THEN END
110 M$ = MC$ : D=-D
120 GOTO 30
```

Esse tipo de criptografia é simples e relativamente fácil de ser quebrada. Basta descobrir o valor do deslocamento, que é um número de 0 a 255, e a mensagem é decifrada. Hoje em dia, o uso de computadores para tal fim tornam essa tarefa ainda mais fácil.

Em vista disso, atualmente utilizam-se técnicas mais complexas e chaves bem maiores, no intuito de dificultar ao máximo a decodificação de um texto por uma pessoa não autorizada.

3- Créditos

Este artigo foi escrito por Marcelo Silveira em Março de 2004 e revisado em Julho de 2017.

e-mail: flamar98@hotmail.com
homepage: http://marmsx.msxall.com