CRIPTOGRAFIA DE DADOS

Carlos Cristiano Cabral

O presente artigo deseja fornecer princípios elementares para a implementação de programas de computador voltados à proteção genérica de informações.

ABSTRACT

This article wishes to provide elementary principles useful to implement computer software concerning generic information protection.

1.0 — INTRODUÇÃO

Assegurar privacidade aos dados, muitas vezes obtidos sob cerrados esforços e elevados investimentos, tem conquistado, paulatinamente, destacado lugar na escala de prioridades de empresas tão preocupadas em salvaguardar o segredo de suas conquistas, quanto em estabelecer um rigido controle de suas operações nas mais diversas áreas, tais como a administrativa, a contábil e a econômica.

Notadamente, com o advento dos computadores e a alta capacidade de certos dispositivos para armazenar dados, tornou-se possível a baixíssimo custo, levar em um único disquete entre páginas de um caderno, um volume impressionante de informações. O incalculável valor destas informações passou a exigir do proprietário das mesmas, procedimentos extras de segurança que garantissem seu uso exclusivo nas tarefas para as quais foram obtidas, e somente por pessoas autorizadas.

A informação, que é obtida a partir de dados posicionados numa ordem lógica desejada, passa a obter então atenção paralela à proteção de acesso aos programas. Não mais satisfaz a garantia de que somente pessoas autorizadas terão acesso aos programas que manipulam os dados. Agora, pois, urge que seja priorizado o sigilo dos dados, mais ainda que a segurança do acesso aos programas.

Surgem, assim, processos de codificação de dados também conhecidos como criptografia, cujo objetivo mister é impossibilitar, ou senão, dificultar o acesso não autorizado a estes dados.

2 — NOÇÕES PRELIMINARES

Alguns termos especiais utilizados na extensão do texto são aqui esclarecidos, a fim de facilitar o seu entendimento.

BIT

Entende-se por **bit** (5) a menor unidade de trabalho de um computador. Um **bit** pode assumir apenas os valores 0 ou 1 e através da combinação destes valores são representados todos os números, letras e caracteres especiais (caracteres gráficos e de pontuação) utilizados pelo computador.

Em uma seqüência de 8 **bits** chamada de **byte**, o computador pode representar qualquer dos caracte-

* *Eng. Civil, professor Auxiliar da Unifor*

res supra-citados. Veja, por exemplo, como o computador representa internamente as letras "I" maiúscula e minúscula:

CARACTERE REPRESENTAÇÃO (1) (8 bits)

I	01001001
i	01101001

CHAVE

Denomina-se chave a uma seqüência específica de caracteres que sirva de base ao processo de criptografia de determinados dados. Usualmente, letras minúsculas são diferenciadas das maiúsculas durante a codificação dos dados, portanto é importante ser rigoroso nos detalhes durante a formação de uma chave. Observe que a chave "CRISTO" não decodifica os dados codificados pela chave "CRISTO", uma vez que a letra "I" foi utilizada diferentemente.

CRISTO e CRiSTO são chaves diferentes, como mostra a fig. 1 abaixo:

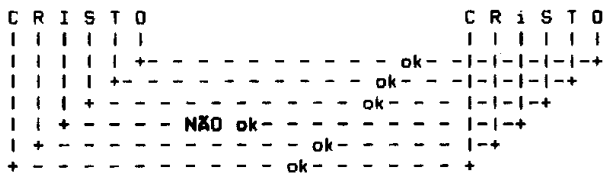


Figura 1

QUEBRA DE CÓDIGO

O fato de se conseguir decodificar plenamente os dados cuja chave e processo de criptografia são desconhecidos, é chamado de quebra de código. A facilidade de se quebrar um código é inversamente proporcional à eficiência do processo de criptografia e à complexidade da chave utilizada.

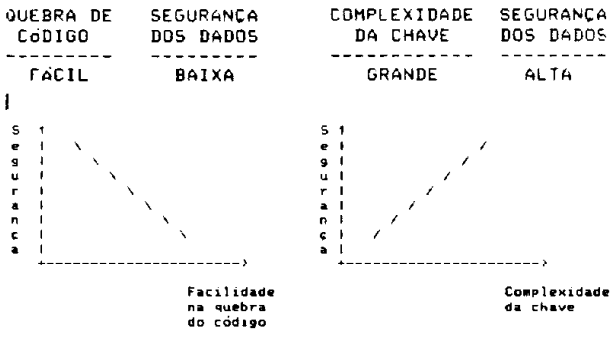


Figura 2

3.0 – TÉCNICAS DE CRIPTOGRAFIA

A seguir são comentados os modelos mais comuns utilizados para a criptografia de dados, valendo ressaltar que existe total independência entre os mesmos, sendo possível inclusive mixá-los no intuito de, oportunamente, maximizar a garantia ao sigilo dos dados.

3.1 – Substituição

Consiste em estabelecer um alfabeto referencial onde, a cada letra do alfabeto comum, corresponda um e somente um caractere do alfabeto referencial e vice-versa. Uma tabela de equivalência entre o alfabeto comum e um determinado alfabeto referencial **R**, poderia ser como se segue:

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

Conforme o alfabeto referencial acima, a frase **acesso negado**" seria criptografada como "**ZXVHHL MVTZWL**". Para retornar a frase à sua forma original, bastaria aplicar o mesmo processo em sentido inverso, isto é, pesquisar cada caractere no alfabeto referencial e encontrar seu equivalente no alfabeto comum.

Uma forma variante bastante usada na aplicação de criptografia por substituição é a do alfabeto circular, que consiste em deslocar em **N** posições, à direita ou à esquerda, o alfabeto comum. Assim, teríamos:

ALFABETO	CARACTERES
COMUM	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
REFERENCIAL	C 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

Observe que todos os caracteres foram deslocados à esquerda em duas posições, e aqueles da extrema esquerda (o "A" e o "B") foram deslocados para a extrema direita do novo alfabeto.

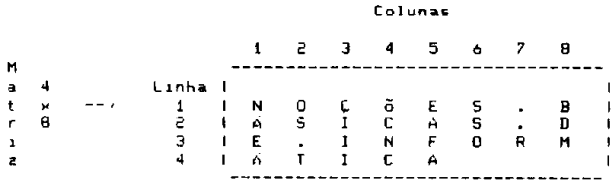
3.2 – Transposição

Permitindo maior elaboração que a substituição, a transposição consiste em tomar por base uma matriz L x C, de L linhas e C colunas, onde o texto é disposto seqüencialmente em cada linha a partir da coluna 1 até a coluna C. O texto criptografado é montado então, lendo-se seqüencialmente cada coluna, a partir da linha 1 até a linha L.

No exemplo a seguir, substituimos todos os espaços em branco por pontos, para facilitar a visualização. Supondo uma matriz 4x8, vejamos como seria criptografada uma mensagem:

Mensagem original:

NOÇÕES.BÁSICAS.DE.INFORMÁTICA



Mensagem criptografada: NÁEÁOS. TÇIIIõCN-CEAFASSO..RBDM

Formas mais complexas permitem que a transposição, fazendo uso de processos determinísticos, utilize uma chave especial de acesso ao código gerado.

3.3 — Manipulação de bits

A técnica de manipulação de **bits** (4) busca tirar proveito tanto das instruções internas do microprocessador, quanto do fato de que todo caractere é formado por uma seqüência de **bits.**

Há, desconsiderando as instruções de deslocamento de bits, quatro instruções básicas de manipulação de bits pertinentes à grande maioria dos computadores: AND, OR, XOR e NOT. A instrução NOT possui um único operando, enquanto as demais possuem dois. As tabelas a seguir, explicitam o(s) operando(s) e o resultado da operação em questão:

AND	0	1
0	0	0
1	0	1

OR	0	1
0	0	1
1	1	1

NOT	0	1
	1	0

XOR	0	1
0	0	1
1	1	0

Manipular bits significa, portanto, efetuar sobre eles operações lógicas como as supra-citadas.

Vejamos. Tomando a instrução XOR, e considerando a chave de criptografia como sendo o caractere "3", cuja representação binária é 00110011, como seria codificada a palavra "PAZ"?

Desta forma, a palavra "PAZ" criptografada com a chave "3" resulta na palavra "cri" de acordo com o padrão ASCII (2).

4 — CONCLUSÃO

Fica notório que existe um vasto universo de métodos de criptografia passivo de ser utilizado nas mais diversas aplicações.

Cabe, portanto, determinar para cada tarefa e tipo de dado a ser codificado, qual a técnica mais adequada e qual a melhor relação custo/benefício obtida (3), lembrando que, na maioria das vezes, mas nem sempre, a eficiência de um método em termos de velocidade de processamento é inversamente proporcional ao nível de segurança alcançado.

De resto cabe frisar que o assunto criptografia de dados é bem mais extenso e profundo do que nos foi possível tratar neste artigo. A comparação de performance entre os vários métodos, suas qualidades e deficiências, bem como um refinamento de tudo o que ora foi exposto, poderá vir a ser título de um artigo à posteriori.

5 — AGRADECIMENTOS

À MiniSol Informática Ltda., **software-house** local especializada em proteção de dados, por todo o apoio prestado na elaboração deste trabalho.

6 — REFERÊNCIAS BIBLIOGRÁFICAS

1. ANGERMEYER et. al. — **Tricks of the DOS masters** — The Wait Group's — s/1 — 1987.
2. BORLAND — **Turbo Pascal Reference Guide version 5.0** — Borland International — s/1 — 1988.
3. HOFFMAN, L. — **Modern Methods for Computer Security and Privacy** — Prentice Hall — s/1 — 1977.
4. SCHIELDT, H. — **Advanced Turbo Pascal** — Borland-Osborne/McGraw Hill — s/1 — 1990.
5. VELLOSO, F.C. — **Informática, Uma Introdução** — Ed. Campus — 1986.