ASPECTOS ALGÉBRICOS DA SEGURANÇA DA INFORMAÇÃO

Antonio Euclides da Rocha Vieira
CPD/IBICT

RESUMO
O uso da criptografia na segurança e privacidade da informação vem gradativamente assumindo papel de relevância à medida que se firma a tendência ao processamento distribuído, com as bases de dados compartilhadas através de redes de comunicação. Identificado esse fato, surge a preocupação de se abordar a/gebricamente a criptografia, desenvolvendo-a como ferramenta aplicável a sistemas de informação automatizados e, em particular, para processamento em equipamentos orientados para caracteres de 8 bits.

Descrítores:
Criptografia; Privacidade da Informação; Processamento de Dados; Processamento Distribuído; Segurança da Informação; Sistema de Informação.

I - INTRODUÇÃO

A computação centralizada foi um conceito amplamente utilizado que incentivou o aparecimento de equipamentos cada vez mais potentes para os nodos centrais das redes de teleprocessamento.

Em decorrência da centralização, as bases de dados requeriam capacidade de armazenamento sempre maior e, em situações envolvendo teleprocessamento, os dados podiam não ser obtidos por problemas de comunicações ou sobrecarga no sistema anfitrião.

Os usuários remotos passaram a questionar a validade de se separar de seus próprios dados, delegando os controles de segurança *e* privacidade e se submetendo a uma estrutura operacional externa.

Várias soluções foram propostas, mas a solução mais adequada foi obtida através da criação de um novo conceito: o processamento distribuído.

Existem duas conseqüências imediatas da aplicação desse conceito. Primeiro, as bases de dados do usuário ficam disponíveis em sua própria instalação e próximas aos locais onde ocorrem as transações, reduzindo ou eliminando os problemas de comunicações de dados. Segundo, os sistemas de computador de grande porte e de alto custo tornam-se desnecessários, dando lugar à utilização de mini-computadores de baixo custo.

O processamento distribuído também afeta o conceito de banco de dados. Um banco de dados centralizado gerencia um conjunto de bases de dados múltiplas e logicamente relacionadas com informações inter-relacionadas e não redundantes. Um banco de dados distribuído é uma integração lógica de banco de dados que gerenciam bases de dados, potencialmente redundantes, em instalações individuais.

O problema da segurança e privacidade da informação ganha nova dimensão.

Um banco de dados em um nodo da rede de teleprocessamento pode se comunicar com outro banco de dados em outro nodo, ou com um programa desenvolvido com a intenção de burlar as proteções instaladas.

Nesse ponto é importante tornar clara a distinção entre segurança e privacidade.

Segurança se refere à proteção de informações contra a revelação acidental ou intencional a pessoas não autorizadas, ou modificações não autorizadas e destruição.

Privacidade se refere aos direitos de indivíduos ou organizações determinarem por eles próprios quando, como e até que ponto uma informação de sua propriedade pode ser transmitida a terceiros.

Na maioria dos bancos de dados existentes, as proteções cobrem apenas os aspectos de segurança. A preocupação com a privacidade é algo que vem surgindo a medida que se toma consciência das implicações sociais do uso dos computadores.

A segurança pode ser facilmente implantada através

de uma estrutura de autorização por senhas a nível de arquivos ou campos, mas a privacidade tem características mais dinâmicas e é assunto de competência individual ou interna a uma organização.

Em bancos de dados centralizados vem sendo amplamente empregada a técnica de proteção por senhas, tendo dado lugar ao aparecimento da figura do Gerente de Senhas.

Uma gerência central desse tipo pode desagradar aos órgãos satélite — perda de prestígio e perda de "controle" devido a dependência na definição e manutenção das bases de dados sob sua responsabilidade. Se não se evitar que tais atritos se transformem em conflitos políticos o projeto todo poderá ser aliado, chegando mesmo a fracassar.

Uma forma de se eliminar ou restringir a atuação de uma gerência central consiste na aplicação da criptografia como ferramenta alternativa ou conjugada a uma estrutura de autorização por senhas.

Essas ferramentas são de fato complementares. A proteção por senhas é extrínseca aos dados, podendo ser a nível de arquivos ou campos. A proteção por criptografia é intrínseca aos dados.

A característica da criptografia ser intrínseca à informação traz duas importantes conseqüências. Primeiro, torna viável se estender a proteção ao nível de privacidade, além do nível puro e simples de segurança. Segundo, outros processos intrínsecos â informação, tais como compactação de dados, podem ser embutidos nos algoritmos do processo de proteção por criptografia.

Aliás, a possibilidade de se embutir um processo de compactação de dados no de criptografia, a torna particularmente atrativa para armazenamento e transmissão de dados.

Reconhecendo o papel de relevância que vem assumindo a criptografia na segurança e privacidade da informação, à medida que se firma a tendência aos bancos de dados distribuídos, surge, de forma natural, a preocupação de se abordar algebricamente essa ferramenta de proteção de dados.

2 - CRIPTOGRAFIA

A seguinte notação será usada neste trabalho para representar aqueles subconjuntos do conjunto N dos números naturais, de interesse para a construção proposta.

NOTAÇÃO:

(i) $N_+ = \{ n \in N \mid n \geqslant 0 \}$

(ii) $N_+^* = N_+ - \{0\}$

(iii) $N_- = \{ n \in N \mid n \leqslant 0 \}$

(iv) $N_-^* = N_- - \{0\}$

Seja o conjunto A. Para toda bijeção g de A em A, vamos definir a operação $<>$ de composição sucessiva da g com ela própria e sua inversa, que será necessário à definição de criptografia.

CONVENÇÃO:

$g : A \to A$ é bijeção

DEFINIÇÃO:

a composição sucessiva é a jeção

$<> : \{ g, g^{-1} \} \times N \to F_g^A$ tal que

$\forall (\gamma, n) \in \{ g, g^{-1} \} \times N$ associa

$<> (\gamma, n) = \gamma^{<n>} \in F_g^A$ tal que:

(i) $\gamma^{<n>} = i_A$, se $n = 0$

(ii) $\gamma^{<n>} = \gamma^{<n-1>} \circ \gamma$, se $n > 0$

(iii) $\gamma^{<n>} = \gamma^{-1 <-n>}$, se $n < 0$

Essa operação de composição das bijeções g e g^{-1} tem como contradomínio o conjunto de bijeções

$F_g^A = \{ i_A, g, g^{-1}, g \circ g, g^{-1}, g \circ g \circ g,$

$g^{-1} \circ g^{-1}, \ldots \}$, que não aparece explicitamente na definição por ser irrelevante para a construção aqui proposta.

A seguir vamos demonstrar algumas propriedades da aplicação da $<>$ na g e g^{-1}.

TEOREMA:

$<> : \{ g, g^{-1} \} \times N \to F_g^A$ é injeção

PROVA:

seja $(\gamma_1, n_1), (\gamma_2, n_2) \in \{ g, g^{-1} \} \times N$ tal que

$(\gamma_1, n_1) = (\gamma_2, n_2)$; então $\gamma_1 = \gamma_2$ e $n_1 = n_2$;

(i) seja $n_1 = n_2 = 0$; então $\gamma_1^{<n_1>} = \gamma_1^{<0>} =$

$= i_A$; então $\gamma_2^{<n_2>} = \gamma_2^{<0>} = i_A$; então $\gamma_1^{<n_1>} =$

$= \gamma_2^{<n_2>}$;

(ii) seja $n_1 = n_2 > 0$;

prova por indução:

seja $n_1 = n_2 = 1$; então $\gamma_1^{<n_1>} = \gamma_1^{<0>} \circ \gamma_1 =$

$= i_A \circ \gamma_1 = \gamma_1$; então $\gamma_2^{<n_2>} = \gamma_2^{<0>} \circ \gamma_2 =$

$= i_A \circ \gamma_2 = \gamma_2$; mas $\gamma_1 = \gamma_2$; então

$\gamma_1^{<n_1>} = \gamma_2^{<n_2>}$;

- hipótese: o resultado é válido para

$n_1 = n_2 = k$; seja $n_1 = n_2 = k + 1$; então

$\gamma_1^{<n_1>} = \gamma_1^{<k+1>} = \gamma_1^{<k>} \circ \gamma_1$; então

$\gamma_2^{<n_2>} = \gamma_2^{<k+1>} = \gamma_2^{<k>} \circ \gamma_2$; mas $\gamma_1 = \gamma_2$

e $\gamma_1^{<k>} = \gamma_2^{<k>}$; então $\gamma_1^{<k>} \circ \gamma_1 =$

$= \gamma_2^{<k>} \circ \gamma_2$; então $\gamma_1^{<n_1>} = \gamma_2^{<n_2>}$;

(iii) seja $n_1 = n_2 < 0$;

então $\gamma_1^{<n_1>} = \gamma_1^{-1<-n_1>}$;

então $\gamma_2^{<n_2>} = \gamma_2^{-1<-n_2>}$; mas $(-n_1) = (-n_2) > 0$

e γ_1^{-1}; $\gamma_2^{-1} \in \{ g_1, g_2 \}$; então, por (ii),

$\gamma_1^{-1<n_1>} = \gamma_2^{-1<n_2>}$; então $\gamma_1^{<n_1>} = \gamma_2^{<n_2>}$;

então, por (i), (ii) e (iii), $\gamma_1^{<n_1>} = \gamma_2^{<n_2>}$;

então $<>(\gamma_1, n_1) = <>(\gamma_2, n_2)$; então

$<>: \{ g, g^{-1} \} \times N \rightarrow F_g^A$ é injeção. Q.E.D.

A partir desse teorema podemos obter o seguinte resultado.

COROLÁRIO:

$\forall (\gamma, n_1), (\gamma, n_2) \in \{ g, g^{-1} \} \times N$,

se $n_1 = n_2$ então $\gamma^{<n_1>} = \gamma^{<n_2>}$

PROVA:

seja

$(\gamma_1\ n_1), (\gamma_1\ n_2) \in \{ g, g^{-1} \} \times N$; seja $n_1 = n_2$;
então $(\gamma_1\ n_1) = (\gamma_1\ n_2)$;
mas $<>: g, g^{-1} \times N \rightarrow F_g^A$
é injeção; então $<>(\gamma, n_1) = <>(\gamma, n_2)$; então
$\gamma^{<n_1>} = \gamma^{<n_2>}$.

Q.E.D.

É interessante observar que $<>$ não é sobrejeção. Por exemplo, pela definição da $<>$, se tem que $g^{<-2>} = g^{-1<2>}$ e no entanto $(-2) \neq 2$ e a g somente seria igual a g^{-1} se fosse a identidade sobre A.

TEOREMA:

$\gamma^{<n>}: A \rightarrow A$ é bijeção,

$\forall (\gamma, n) \in \{ g, g^{-1} \} \times N$

PROVA:

(i) seja $n = 0$;

então $\gamma^{<n>} = \gamma^{<0>} = i_A$; mas

a identidade sobre A é bijeção de A em

A; então $\gamma^{<n>} : A \rightarrow A$ é bijeção;

(ii) seja $n > 0$;
prova por indução:

- seja $n = 1$; então $\gamma^{<n>} = \gamma^{<1>} = \gamma^{<0>} \circ \gamma =$

$= i_A \circ \gamma = \gamma$; mas $g : A \rightarrow A$ é bijeção;

então $\gamma^{<n>} : A \rightarrow A$ é bijeção;

- hipótese: o resultado é válido para

$n = k$; seja $n = k + 1$; então $\gamma^{<n>} =$
$= \gamma^{<k+1>} = \gamma^{<k>} \circ \gamma$;

mas a composição de bijeções de A em A é uma bijeção de A em A; então $\gamma^{<n>} : A \rightarrow A$ é bijeção;

(iii) seja $n < 0$; seja $\gamma = g$; então $\gamma^{<n>} = g^{<n>} =$

$= g^{-1<-n>}$; mas $(-n) > 0$; então, por (ii),

$g^{-1<-n>} : A \rightarrow A$ é bijeção; então $\gamma^{<n>} : A \rightarrow A$

é bijeção; seja $\gamma = g^{-1}$; então $\gamma^{<n>} =$

$= g^{-1<n>} = (g^{-1})^{-1<-n>}$; mas $g : A \rightarrow A$ é bijeção;

então $(g^{-1})^{-1} = g$; então $\gamma^{<n>} = g^{<-n>}$;

mas $(-n) > 0$; então, por (ii), $g^{<-n>} : A \rightarrow A$

é bijeção; então $\gamma^{<n>} : A \rightarrow A$ é bijeção.

Q.E.D.

A propriedade de composição sucessiva à direita foi estabelecida por definição. Vejamos agora a de composição sucessiva à esquerda.

TEOREMA:

$\gamma^{<n>} = \gamma \circ \gamma^{<n-1>}$, $\forall (\gamma, n) \in g, g^{-1} \times N_+^*$

PROVA:
por indução:

- seja $n = 1$; então $\gamma^{<n>} = \gamma^{<1>} = \gamma^{<0>} \circ \gamma =$

$= i_A \circ \gamma = \gamma \circ i_A = \gamma \circ \gamma^{<0>} = \gamma \circ \gamma^{<n-1>}$;

• hipótese : o resultado é válido para

$n = k$; seja $n = k + 1$; então $\gamma^{<n>} = \gamma^{<k+1>} =$

$= \gamma^{<k>} \circ \gamma = \gamma \circ \gamma^{<k-1>} \circ \gamma = \gamma^{<k>} =$

$= \gamma \circ \gamma^{<n-1>}$.

Q.E.D.

Como $g^{<n>}$ é bijeção, ela admite inversa. A seguir vamos provar dois lemas que serão usados na demonstração de que $g^{-1<n>}$ é essa inversa à direita e a esquerda.

LEMA:

$g^{<n>} \circ g^{-1<n>} = i_A, \forall n \in N_+$

PROVA:

(i) seja $n = 0$;

$=$ então $g^{<n>} \circ g^{-1<n>} =$

$= g^{<0>} \circ g^{-1<n>} \circ g^{-1<0>} =$

$= i_A \circ i_A = i_A$;

(ii) seja $n > 0$;

prova por indução:

• seja $n = 1$;

$=$ então $g^{<n>} \circ g^{-1<n>} = g^{<1>} \circ g^{-1<1>} =$

$= g^{<0>} \circ g \circ g^{-1} \circ g^{-1<0>} =$

$= i_A \circ i_A \circ i_A = i_A$;

• hipótese: o resultado é válido para

$n = k$; seja $n = k + 1$; então $g^{<n>} \circ g^{-1<n>} =$

$= g^{<k+1>} \circ g^{-1<k+1>} =$

$= g \circ g^{<k>} \circ g^{-1<k>} \circ g^{-1} =$

$= g \circ i_A \circ g^{-1} = g \circ g^{-1} = i_A$.

Q.E.D.

LEMA:

$g^{-1<n>} \circ g^{<n>} = i_A, \forall n \in N_+$

PROVA:

(i) seja $n = 0$;

$=$ então $g^{-1<n>} \circ g^{<n>} = g^{-1<0>} \circ g^{<o>} =$

$= i_A \circ i_A = i_A$;

(ii) seja $n > 0$;

prova por indução:

• seja $n = 1$;

$=$ então $g^{-1<n>} \circ g^{<n>} = g^{-1<1>} \circ g^{<1>} =$

$= g^{-1<0>} \circ g^{-1} \circ g \circ g^{<0>} = i_A \circ i_A \circ i_A = i_A$;

• hipótese: o resultado é válido para

$n = k$; seja $n = k + 1$; então $g^{-1<n>} \circ g^{<n>} =$

$= g^{-1<k+1>} \circ g^{<k+1>} =$

$= g^{-1} \circ g^{-1<k>} \circ g^{<k>} \circ g =$

$= g^{-1} \circ i_A \circ g = g^{-1} \circ g = i_A$.

Q.E.D.

Vejamos agora que $g^{-1<n>}$ é a inversa de $g^{<n>}$ à direita.

TEOREMA:

$g^{<n>} \circ g^{-1<n>} = i_A, \forall n \in N$

PROVA:

(i) seja $n \geqslant 0$; então, por lema anterior,

$g^{<n>} \circ g^{-1<n>} = i_A$;

(ii) seja $n < 0$;

então $g^{<n>} \circ g^{-1<n>} = g^{-1<-n>} \circ (g^{-1})^{-1<-n>}$;

mas $(g^{-1})^{-1} = g$; então $g^{<n>} \circ g^{-1<n>} =$

$= g^{-1<-n>} \circ g^{<-n>}$; mas $(-n) > 0$; então,

por lema anterior, $g^{-1<-n>} \circ g^{<-n>} = i_A$;

então $g^{<n>} \circ g^{-1<n>} = i_A$.

Q.E.D.

Falta mostrar que $g^{-1<n>}$ é a inversa de $g^{<n>}$ à esquerda.

TEOREMA:

$g^{-1<n>} \circ g^{<n>} = i_A, \forall n \in N$

PROVA:

(i) seja $n \geqslant 0$;

então, por lema anterior,

$g^{-1}<n> \circ g<n> = i_A$;

(ii) seja $n<0$; então $g^{-1}<n> \circ g<n> =$

$= (g^{-1})^{-1}<-n> \circ g^{-1}<-n>$; mas $(g^{-1})^{-1} = g$;

então $g^{-1}<n> \circ g<n> = g<-n> \circ g^{-1}<-n>$;

mas $(-n) > 0$; então, por lema anterior,

$g<-n> \circ g^{-1}<-n> = i_A$;

então $g^{-1}<n> \circ g<n> = i_A$.

Q.E.D.

A bijeção $g : A \to A$ assim construída, é um dos elementos usados na definição de criptografia. Um outro elemento, convencionado a seguir, é a injeção h.

CONVENÇÃO:

(i) $N \subseteq N$

(ii) $M \subseteq N$

(iii) $h : N \to M$ é injeção

Vamos agora estabelecer o que é criptografia.

DEFINIÇÃO: f é criptografia sobre $\{A, N, g, h\}$

se e somente se

$f : A \times N \to A \times N$ é jeção tal que

$\forall (a, n) \in A \times N, \exists f(a, n) \in A \times N$

tal que $f(a, n) = (g^{<h(n)>}, n)$

Evidentemente, tão importante quanto cifrar uma informação é decifrá-la oportunamente. Em conseqüência é mandatório que a criptografia admita inversa e que se conheça essa inversa.

Inicialmente provemos que a criptografia é uma bijeção.

CONVENÇÃO:

f é criptografia sobre $\{A, N, g, h\}$

TEOREMA:

$f : A \times N \to A \times N$ é bijeção

PROVA:

basta provar que a jeção

$f : A \times N \to A \times N$ é injetiva e sobrejetiva;

(i) sejam $(a_1, n_1), (a_2, n_2) \in A \times N$ tais que

$(a_1, n_1) \neq (a_2, n_2)$; então $a_1 = a_2$ e $n_1 = n_2$;

mas $h : N \to M$ é injeção; então $h(n_1) = h(n_2)$;

mas $<> : \{g, g^{-1}\} \times N \to F_g^A$ é injeção;

então $g^{<h(n_1)>} = g^{<h(n_2)>}$; então

$g^{<h(n_1)>}(a_1) = g^{<h(n_2)>}(a_1)$; mas

$g^{<h(n_2)>} : A \to A$ é injeção; então

$g^{<h(n_2)>}(a_1) = g^{<h(n_2)>}(a_2)$; então

$(g^{<h(n_1)>}(a_1), n_1) = (g^{<h(n_2)}(a_2), n_2)$;

então $f(a_1, n_1) = f(a_2, n_2)$; então

$f : A \times N \to A \times N$ é injeção;

(ii) sejam $(a_1, n_1), (a_2, n_2) \in A \times N$ tais que

$f(a_1, n_1) = f(a_2, n_2)$; então $(g^{<h(n_1)>}(a_1), n_1) =$

$= (g^{<h(n_2)>}(a_2), n_2)$; então $n_1 = n_2$ e

$g^{<h(n_1)>}(a_1) = g^{<h(n_2)>}(a_2)$; mas $h : N \to M$

é injeção; então $h(n_1) = h(n_2)$; mas

$<> : \{g, g^{-1}\} \times N \to F_g^A$ é injeção;

então $g^{<h(n_1)>} = g^{<h(n_2)>}$; então

$g^{<h(n_1)>}(a_1) = g^{<h(n_1)>}(a_2)$; mas

$g^{<h(n_1)>} : A \to A$ é sobrejeção; então

$a_1 = a_2$; então $f : A \times N \to A \times N$ é sobrejeção.

Como a criptografia é uma bijeção, ela admite inversa. O teorema a seguir identifica essa f^{-1}.

TEOREMA: $f^{-1} : A \times N \to A \times N$ é tal que

$\forall (a, n) \in A \times N, \exists f^{-1}(a, n) \in A \times N$

tal que $f^{-1}(a, n) = (g^{-1<h(n)>}(a), n)$

PROVA: basta mostrar que a f^{-1} é inversa à esquerda e à direita da f;

seja $(a, n) \in A \times N$;

(i) $f^{-1} \circ f(a, n) = f^{-1}(f(a, n))$

$= f^{-1}\ (g^{<h(n)>}(a),\ n)$

$= (g^{-1<h(n)>}\ (g^{<h(n)>}(a)),\ n)$

$= (g^{-1<h(n)>} \circ g^{<h(n)>}(a),\ n)$

$= (i_A\ (a),\ n)$

$= (a,\ n);$

então $f^{-1} \circ f = i_{A \times N}$; então f^{-1} é inversa à

(ii) $f \circ f^{-1}\ (a,\ n) = f(f^{-1}\ (a,\ n))$

$= f(g^{-1<h(n)>}(a),\ n)$

$= (g^{<h(n)>}\ (g^{-1<h(n)>}(a)),\ n)$

$= (g^{<h(n)>} \circ g^{-1<h(n)>}\ (a),\ n)$

$= (i_A\ (a),\ n)$

$= (a,\ n);$

então $f \circ f^{-1} = i_{A \times N}$; então f^{-1} é inversa à direita da f.

Q.E.D.

É interessante observar que a f^{-1} atende à definição de criptografia sobre $\{A, N, g^{-1}, h\}$.

TEOREMA: f é criptografia sobre $\{A, N, g, h\}$ se e somente se f^{-1} é criptografia sobre $\{A, N, g^{-1}, h\}$

PROVA:

(i) seja f criptografia sobre $\{A, N, g, h\}$;
então $f^{-1} : A \times N \to A \times N$ é tal que
$\forall (a, n) \in A \times N, \exists f^{-1}(a, n) \in A \times N$
tal que $f^{-1}(a, n) = (g^{-1<h(n)>}(a), n)$;
então f^{-1} é criptografia sobre $\{A, N, g^{-1}, h\}$;

(ii) seja f^{-1} criptografia sobre $\{A, N, g^{-1}, h$;
então $(f^{-1})^{-1} : A \times N \to A \times N$ é tal que
$\forall (a, n) \in A \times N, \exists (f^{-1})^{-1}(a, n) \in A \times N$
tal que $(f^{-1})^{-1}(a, n) = ((g^{-1})^{-1<h(n)>}(a), n)$;
mas f e g são bijeções, então
$(f^{-1})^{-1} = f$ e $(g^{-1})^{-1} = g$; então f é
criptografia sobre $\{A, N, g, h\}$.

Geralmente se confunde a criptografia f sobre $\{A, N, g, h\}$ com o valor de $g^{<h(n)>}(a)$ que, em última análise, é a informação cifrada ou decifrada.

3 – EXEMPLO

Criptografar, sob o código 341057, o texto "$\alpha\alpha\gamma\beta\delta\alpha\beta\alpha$" definido sobre o conjunto de caracteres $\alpha, \beta, \gamma, \delta$.

Designando $A = \{\alpha, \beta, \gamma, \delta\}$,

seja a bijeção $g : A \to A$ definida por : $g(\alpha) = \beta$

$g(\beta) = \gamma$

$g(\gamma) = \delta$

$g(\delta) = \alpha.$

Designando $N = \{1, 2, 3, 4, 5, 6, 7, 8\}$ e

$M = 3, 4, 1, 0, 5, 7$,

seja a injeção $h : N \to M$ definida por : $h(1) = h(7) = 3$

$h(2) = h(8) = 4$

$h(3) = 1$

$h(4) = 0$

$h(5) = 5$

$h(6) = 7.$

Seja a criptografia $f : A \times N \to A \times N$
tal que $\forall (a, n) \in A \times N, \exists f(a, n) \in A \times N$
tal que $f(a, n) = (g^{<h(n)>}(a), n)$.

Para se obter o texto criptografado basta determinar

$f(\alpha, 1) = (g^{<h(1)>}(\alpha), 1) = (g^{<3>}(\alpha), 1) =$

$= (\delta, 1)$

$f(\alpha, 2) = (g^{<h(2)>}(\alpha), 2) = (g^{<4>}(\alpha), 2) =$

$= (\alpha, 2)$

$f(\gamma, 3) = (g^{<h(3)>}(\gamma), 3) = (g^{<1>}(\gamma), 3) =$

$= (\delta, 3)$

$f(\beta, 4) = (g^{<h(4)>}(\beta), 4) = (g^{<0>}(\beta), 4) =$

$= (\beta, 4)$

$f(\delta, 5) = (g^{<h(5)>}(\delta), 5) = (g^{<5>}(\delta), 5) =$

$= (\alpha, 5)$

$f(\alpha, 6) = (g^{<h(6)>}(\alpha), 6) = (g^{<7>}(\alpha), 6) =$

$= (\delta, 6)$

$f(\beta, 7) = (g^{<h(7)>}(\beta), 7) = (g^{<3>}(\beta), 7) =$

$= (\alpha, 7)$

$f(\alpha, 8) = (g^{<h(8)>}(\alpha), 8) = (g^{<4>}(\alpha), 8) =$

$= (\alpha, 8)$

Dessa forma o texto cifrado correspondente será "$\delta\ \alpha\ \delta\ \beta\ \alpha\ \delta\ \alpha\ \alpha$".

4 – FORMULAÇÃO DE UMA CRIPTOGRAFIA PARA APLICAÇÕES EM PROCESSAMENTO DE DADOS

Com base no desenvolvimento algébrico apresentado, vamos formular uma criptografia que, através da escolha adequada de seus elementos, poderá ser aplicada em transmissão de dados ou em sistemas de informação automatizados.

Inicialmente vamos caracterizar o que é um conjunto de caracteres e o que é uma tabela circular destes caracteres.

Embora esses conceitos sejam freqüentemente empregados, é necessário caracterizá-los rigorosamente uma vez que serão elementos básicos na formulação aqui proposta.

CONVENÇÃO:

(i) $m \in N_+^*$

(ii) $K = \{ k \in N_+ \mid k < m \}$

DEFINIÇÃO:

A é conjunto de caracteres se e somente se

$A = \{ a_i \mid i \in N_+^* \text{ e } i \leqslant m \}$ tal que

$\forall a_i\ a_j \in A,\ a_i = a_j \text{ sss } i = j$

CONVENÇÃO:

A é conjunto de caracteres

DEFINIÇÃO:

t é tabela sobre $\{A, K\}$

se e somente se

$t : A \times K \to A \times K$ é jeção tal que

$\forall (a_i, k) \in A \times K, \exists\ t(a_i, k) \in A \times K$

tal que:

(i) $t(a_i, k) = (a_{i+k}, k)$ se $i + k \leqslant m$

(ii) $t(a_i, k) = (a_{i+k-m}, k)$ se $i + k > m$

CONVENÇÃO:

t é tabela sobre $\{A, K\}$

Vamos agora iniciar todo um processo de identificação da tabela t sobre $\{A, K\}$ com a bijeção $g : A \to A$ da construção algébrica apresentada na seção 2. Em conseqüência, o conjunto A daquela construção será identificado com o conjunto $A \times K$, domínio e contradomínio da t.

Dentro desse processo, vamos provar inicialmente que t é bijeção.

TEOREMA:

$t : A \times K \to A \times K$ é bijeção

PROVA:

basta provar que a jeção
$t : A \times K \to A \times K$ é injetiva e sobrejetiva:

(i) sejam $(a_i, k_1), (a_j, k_2) \in A \times K$ tais que $(a_i, k_1) = (a_j, k_2)$; então $a_i = a_j$ e $k_1 = k_2$; mas A é conjunto de caracteres, então $i = j$ e $i, j \in N_+^*$; mas $k_1, k_2 \in K$, então $k_1, k_2 \in N_+$; então $i + k_1 = i + k_2$ e $i + k_1, i + k_2 \in N_+^*$; seja $i + k_1 \leqslant m$; então $j + k_2 \leqslant m$; então $a_{i+k_1}, a_{j+k_2} \in A$; então $a_{i+k_1} = a_{j+k_2}$; então $(a_{i+k_1}, k_1), (a_{j+k_2}, k_2) \in A \times K$ e $(a_{i+k_1}, k_1) = (a_{j+k_2}, k_2)$; mas $t(a_i, k_1) = (a_{i+k_1}, k_1)$ e $t(a_j, k_2) = (a_{j+k_2}, k_2)$; então $t(a_i, k_1) = t(a_j, k_2)$; seja $i + k_1 > m$; então $j + k_2 > m$; então $i + k_1 - m, j + k_2 - m \in N_+^*$; então $a_{i+k_1-m}, a_{j+k_2-m} \in A$; mas $i + k_1 - m = j + k_2 - m$, então $a_{i+k_1-m} = a_{j+k_2-m}$; então $(a_{i+k_1-m}, k_1), (a_{j+k_2-m}, k_2) \in A \times K$

e $(a_{i+k_1-m}, k_1) = (a_{j+k_2-m}, k_2)$; mas

$t(a_i, k_1) = (a_{i+k_1-m}, k_1)$ e $t(a_j, k_2) =$

$= (a_{j+k_2-m}, k_2)$; então $t(a_i, k_1) = t(a_j, k_2)$;

então $t : A \times N \to A \times N$ é injeção;

(ii) sejam $(a_i, k_1), (a_j, k_2) \in A \times K$ tais que

$t(a_i, k_1) = t(a_j, k_2)$; então $(a_{i+k_1}, k_1) =$

$= (a_{j+k_2}, k_2)$ ou $(a_{i+k_1}, k_1) = (a_{j+k_2-m}, k_2)$

ou $(a_{i+k_1-m}, k_1) = (a_{j+k_2}, k_2)$ ou

$(a_{i+k_1-m}, k_1) = (a_{j+k_2-m}, k_2)$; então

$k_1 = k_2$; suponhamos, por absurdo,

que $a_i \neq a_j$; mas A é conjunto de caracteres, então $i \neq j$; então

$i + k_1 \neq j + k_2$ e $i + k_1 - m \neq j + k_2 - m$;

então, se $a_{i+k_1}, a_{j+k_2} \in A$ então $a_{i+k_1} \neq$

$\neq a_{j+k_2}$ então $(a_{i+k_1}, k) \neq (a_{j+k_2}, k_2)$;

então, se $a_{i+k_1-m}, a_{j+k_2-m} \in A$ então

$a_{i+k_1-m} \neq a_{j+k_2-m}$ então $(a_{i+k_1-m}, k_1) \neq$

$\neq (a_{j+k_2-m}, k_2)$; então $(a_{i+k_1}, k_1) =$

$= (a_{j+k_2-m}, k_2)$ ou $(a_{i+k_1-m}, k_1) =$

$= (a_{j+k_2}, k_2)$; então, se a_{i+k_1},

$a_{j+k_2-m} \in A$ então $a_{i+k_1} = a_{j+k_2-m}$

então $i + k_1 = j + k_2 - m$ então $i = j - m$,

ou se $a_{i+k_1-m}, a_{j+k_2} \in A$ então

$a_{i+k_1-m} = a_{j+k_2}$ então $i + k_1 - m =$

$= j + k_2$ então $j = i - m$; então

$i = j - m$ ou $j = i - m$; mas $i, j \in N_+^*$,

então $i > m$; então $a_i \notin A$

ou $a_j \notin A$; absurdo; então $a_i = a_j$;

então $(a_i, k_1) = (a_j, k_2)$; então

$t : A \times K \to A \times K$ é sobrejeção. Q.E.D.

Como a tabela é uma bijeção, ela admite inversa t^{-1} que chamaremos de tabela inversa sobre $\{A, K\}$.

TEOREMA: $t^{-1} : A \times K \to A \times K$ é tal que

$\forall (a_i, k) \in A \times K,$

$\exists\, t^{-1}(a_i, k) \in A \times K$ tal que:

(i) $t^{-1}(a_i, k) = (a_{i-k}, k)$ se $i > k$

(ii) $t^{-1}(a_i, k) = (a_{m-k+i}, k)$ se $i \leqslant k$

PROVA:

basta mostrar que a t^{-1} é inversa à esquerda e à direita da t;
seja $(a_i, k) \in A \times K$

(i) seja $i + k \leqslant m$; então $t(a_i, k) = (a_{i+k}, k)$;

mas $i \in N_+^*$, então $i + k > k$; então

$t^{-1} \circ t(a_i, k) = t^{-1}(t(a_i, k)) = t^{-1}(a_{i+k}, k) =$
$= (a_{i+k-k}, k) = (a_i, k)$; então $t^{-1} \circ t =$

$= i_{A \times k}$;

seja $i + k > m$; então $t(a_i, k) = (a_{i+k-m}, k)$;

mas $a_i \in A$, então $i \leqslant m$; então

$i + k \leqslant m + k$; então $i + k - m \leqslant k$; então
$t^{-1} \circ (a_i, k) = t^{-1}(t(a_i, k)) =$

$= t^{-1}(a_{i+k-m}, k) = (a_{m-k+i+k-m}, k) =$

$= (a_i, k)$; então $t^{-1} \circ t = i_{A \times k}$;

(ii) seja $i > k$; então $t^{-1}(a_i, k) = (a_{i-k}, k)$;

mas $a_i \in A$, então $i \leqslant m$; então

$i - k + k \leqslant m$; então $t \circ t^{-1}(a_i, k) =$

$= t(t^{-1}(a_i, k)) = (a_{i-k}, k) = (a_{i-k+k}, k) =$

$= (a_i, k)$; então $t \circ t^{-1} = i_{A \times k}$;

seja $i \leqslant k$; então $t^{-1}(a_i, k) = (a_{m-k+i}, k)$;

mas $i \in N_+^*$, então $m + i > m$; então

$m - k + i + k > m$; então

$t \circ t^{-1}(a_i, k) = t(t^{-1}(a_i, k)) =$

$= t(a_{m-k+i}, k) = (a_{m-k+ik-m}, k) =$

$= (a_i, k)$; então $t \circ t^{-1} = i_{A \times k}$.

Q.E.D.

A seguir vamos transportar a definição da operação de composição sucessiva dada na construção algébrica

apresentada na seção 2, adaptando-a às tabelas sobre $\{A, K\}$.

DEFINIÇÃO:

a composição sucessiva é a jeção

$<>: \{t, t^{-1}\} \times N \rightarrow F_t^{A \times k}$ tal que

$\forall (\gamma, n) \in \{t, t^{-1}\} \times N$ associa

$<>(\gamma, n) = \gamma <n> \in F_t^{A \times k}$ tal que:

(i) $\gamma <n> = i_{A \times k}$, se $n = 0$

(ii) $\gamma <n> = \gamma <n-1> \circ \gamma$, se $n > 0$

(iii) $\gamma <n> = \gamma^{-1} <-n>$, se $n < 0$

A tabela t, a tabela inversa t^{-1} e a operação de composição $<>$ dessas tabelas serão elementos usados na construção da criptografia objeto desta seção. Dois outros elementos, código e seleção sobre esse código, serão caracterizados a seguir.

CONVENÇÃO:

$\ell \in N_+^*$

DEFINIÇÃO:

N é código sob ℓ

sss

$N = \{ n_i \in N_+^* \mid i \in N_+^* \text{ e } i \leqslant \ell \}$

CONVENÇÃO:

N é código sob ℓ

DEFINIÇÃO:

η é seleção sobre o código N

sss

$\eta : N_+^* \rightarrow N$ é jeção tal que $\forall j \in N_+^*$,

$\exists \eta(j) \in N$ tal que $\eta(j) = n_{1 + \text{resto}\,(\frac{j-1}{\ell})}$

CONVENÇÃO:

η é seleção sobre o código N

Pretendemos identificar a seleção η sobre N com a injeção h da construção algébrica apresentada na seção 2. Dessa forma, provemos que η é injeção.

TEOREMA:

$\eta : N_+^* \rightarrow N$ é injeção

PROVA:

sejam $i, j \in N_+^*$ tais que $i = j$, então

$\eta(i) = n_{1+\text{resto}\,(\frac{i-1}{\ell})} = n_{1+\text{resto}\,(\frac{j-1}{\ell})} = \eta(j)$. Q.E.D.

Dispomos agora de todos os elementos necessários à construção da seguinte criptografia c sobre $\{A \times K, N_+^*, t, \eta\}$.

CONVENÇÃO:

$c : A \times K \times N_+^* \rightarrow A \times K \times N_+^*$ é jeção

tal que $\forall (a_i, k, j) \in A \times K \times N_+^*$

$\exists\, c(a_i, k, j) \in A \times K \times N_+^*$ tal que

$c(a_i, k, j) = (t^{<\eta(j)>}(a_i, k), j)$

De resultado anterior, sabemos que a criptografia c é uma bijeção e conhecemos sua inversa c^{-1}.

COMENTÁRIO:

$c^{-1} : A \times K \times N_+^* \rightarrow A \times K \times N_+^*$

é tal que $\forall (a_i, k, j) \in A \times K \times N_+^*$

$\exists\, c^{-1}(a_i, k, j) \in A \times K \times N_+^*$ tal que

$c^{-1}(a_i, k, j) = (t^{-1<\eta(j)>}(a_i, k), j)$

Como geralmente se tem interesse especificamente no valor cifrado ou decifrado da informação, podemos criar uma injeção υ que aplicada a c ou c^{-1} forneça esse valor.

DEFINIÇÃO:

υ é valor sobre $A \times K \times N_+^*$

sss

$\upsilon : A \times K \times N_+^*$ é jeção tal que

$\forall (a_i, k, j) \in A \times K \times N_+^*$

$\exists\, \upsilon(a_i, k, j) \in A \times K \times N_+^*$ tal que

$\upsilon(a_i, k, j) = a_i$

Dessa forma, o elemento de informação cifrado se obtém através da composição $\upsilon \circ c$ e, o decifrado, através da $\upsilon \circ c^{-1}$.

5 – EXEMPLO EM EQUIPAMENTOS ORIENTADOS PARA CARACTERES DE 8 BITS.

Considerando a formulação apresentada na seção 4, vamos propor uma criptografia passível de implantação em equipamentos de processamentos de dados orientados para caracteres de 8 bits.

CONVENÇÃO:
números representados na base hexadecimal

Fazendo m = 100, temos $\{ K = k \in N_+ \mid k < 100 \}$.

Considerando o conjunto de caracteres definido por

$a_i = i - 1$, temos $A = \{ i - 1 \mid i \in N_+^* \text{ e } i \leqslant 100 \}$.

Em conseqüência, a tabela t e a tabela

inversa t^{-1} sobre $\{ A, K \}$ são tais que

$\forall\ (i-1, k) \in A \times K,\ \exists\, t(i-1, k)$,

$t^{-1}\ (i-1, k)$

$\in A \times K$ tais que:

$$\text{(i)}\quad t(i-1,k) = \begin{cases} (i-1+k, k), & \text{se } i-1+k \leqslant 100 \\ (i-1+k-100, k), & \text{se } i-1+k > 100 \end{cases}$$

$$\text{(ii)}\quad t^{-1}(i-1,k) = \begin{cases} (i-1-k, k), & \text{se } i-1 > k \\ (100-k+i-1, k), & \text{se } i-1 \leqslant k \end{cases}$$

Trabalhando apenas com 8 bits, podemos concluir que, por efeito de truncamento é esquerda,

$i - 1 \pm k \pm 100 = i - 1 \pm k$, e, portanto:

$t(i-1, k) = (i-1+k, k)$;

$t^{-1}(i-k, k) = (i-1-k, k)$.

Dessa forma, para um dado código N sob ℓ e para uma seleção η sobre esse código, os valores dos elementos de informação cifrados e decifrados são obtidos através de:

$$\upsilon \circ c\,(i-1, k, j) = \upsilon\,(t^{<\eta(j)>}(i-1, k), j)$$

$$= \upsilon\,(i-1+k \cdot \eta\,(j), k, j)$$

$$= i-1+k \cdot \eta\,(j)$$

$$\upsilon \circ c^{-1}(i-1, k, j) = i-1-k \cdot \eta\,(j)$$

Para efeito de programação podemos substituir i – 1 por i, ou seja,

$\upsilon \circ c\,(i, k, j) = i + k \cdot \eta\,(j)$

$\upsilon \circ c^{-1}(i, k, j) = i - k \cdot \eta\,(j)$,

onde : $0 \leqslant i \leqslant FF$ é o elemento de informação a ser cifrado ou decifrado; $0 \leqslant k \leqslant FF$ é uma constante de deslocamento na tabela; $j \geqslant 1$ representa a posição do elemento de informação no texto; e a seleção η sobre o código N é definida de acordo com o algoritmo selecionado.

ABSTRACT

Cryptography as information security and privacy tool is getting a relevant position at the same rate scattered data processing environment becomes the most attractive solution for data bases shared via communication networks.
The scope of this work is an algebraical sight of cryptography as an applicable tool for automatic information systems and, specially, in 8 bits character oriented equipments.