SOBRE A ESCOLHA DE PERMUTAÇÕES PARA FINS CRIPTOGRÁFICOS

R. M. Campello de Souza, A. N. Kauffman, R. C. C. Lima
Grupo de Pesquisas em Comunicações - CODEC
Departamento de Eletrônica e Sistemas - UFPE
C.P. 7800, 50970-730, Recife PE
ricardo@npd.ufpe.br

Resumo - Permutações desempenham um papel relevante no contexto de Criptografia, uma vez que representam uma importante contribuição no sentido de incrementar a difusão gerada pelo processo de cifragem e muitos cripto-sistemas fazem uso das mesmas. Entretanto, poucas investigações foram feitas no sentido de se elucidar aspectos de uma permutação que a tornem atrativa para fins criptográficos. Neste trabalho esta temática é abordada e o problema da contagem do número de permutações sob n elementos que fixam i posições é considerado.

Abstract - Permutations play an important role in the field of data security, representing a substantial contribution to increase the diffusion of the encryption process and many cryptosystems make use of them . However, in general, the literature on the subject reports very few results concerning those aspects of a permutation that make it atractive for cryptographic purposes. In this paper the subject is considered and, in the search for cryptographically strong permutations to be used in private or public cryptosystems, the problem of counting the number of permutations of degree n that fix i elements is approached.

Palavras Chaves : criptografia, permutações, chave privada.

1. INTRODUÇÃO

Permutações são elementos de atuação vigorosa, não apenas no contexto da Matemática, mas também em muitas aplicações na Engenharia. Na área de segurança de dados, especificamente, as mesmas tem um papel importante na concepção de algoritmos de cifragem. De fato, os cripto-sistemas de chave privada mais seguros já concebidos empregam cifras do tipo produto, as quais implementam uma combinação de transformações envolvendo substituições e transposições dos caracteres do bloco de informação a ser protegido. A transposição de um bloco de n caracteres é efetuada através de uma permutação, a qual contribui para incrementar a difusão resultante da utilização de uma cifra. No projeto de cifras de bloco, os princípios de confusão e difusão, enunciados por Shannon em 1949 [1], permanecem ainda como a principal orientação a ser seguida.

As cifras de bloco mais comumente empregadas nas modernas redes de computadores de alta velocidade fazem uso de permutações no algoritmo de cifragem. Um exemplo clássico é o bem conhecido padrão de cifragem de dados DES (Data Encryption Standard), o qual faz uso de três permutações de graus diferentes [2]. Um exemplo mais recente é o cripto-sistema SAFER+ (Secure and Fast Encryption Routine), candidato ao padrão AES (Advanced Encryption Standard) que substituirá o DES [3]. SAFER+ é uma cifra iterativa que emprega uma permutação sobre blocos de 16 caracteres construída de modo a produzir o máximo de difusão no mínimo de rodadas [4].

Cripto-sistema	Tipo de chave	#
DES	Privada	3
Gost	Privada	8
McEliece	Pública	1
Surto	Privada	1
SAFER+	Privada	1

TAB. 1: Alguns cripto-sistemas que empregam permutações.

Cifras baseadas em códigos para controle de erros, quer sejam de chave pública [5] ou privada [6], se fundamentam na modificação da estrutura de um código linear, modificação esta que usualmente preserva apenas sua linearidade. Para se obter este efeito de perda de estrutura, uma permutação é aplicada durante o processo de cifragem [7]. A tabela 1 lista alguns cripto-sistemas que empregam permutações (# denota o número de permutações em cada cripto-sistema).

A busca por permutações fortes do ponto de vista de criptografia, isto é, permutações que permitam estabelecer níveis específicos desejáveis de segurança computacional, tem sido pouco explorada na literatura [8], [9]. Neste trabalho o tema é abordado e alguns resultados são obtidos acerca do comportamento de permutações de grau n e de sua utilização para fins criptográficos. Na próxima seção alguns fatos básicos sobre permutações são apresentados e uma nova função aritmética, denotada $P_n(i)$, é introduzida e algumas de suas propriedades são estabelecidas. A seção 3 contém o principal resultado da pesquisa relatada neste trabalho, a completa especificação da função $P_n(i)$. Na seção 4 uma análise de comportamento assimptótico é apresentada. A seção 5 apresenta alguns exemplos e as conclusões do trabalho são apresentadas na seção 6.

2. PRELIMINARES

Definição 1 - *Uma permutação de um conjunto S é uma bijeção de S em S. O grau de uma permutação é a cardinalidade do conjunto sobre o qual a mesma está definida.*

Sem perda de generalidade, no que se segue, considera-se S como sendo o conjunto de inteiros $(1, 2, 3, \cdots, n)$. Dessa forma, se p é uma permutação definida em S, a imagem do inteiro $i \in S$ é denotada por $p(i)$. Pode-se então usar a seguinte lista de pares $(i, p(i))$ para especificar p :

$$\begin{pmatrix} 1 & 2 & 3 & \cdots n \\ p(1) & p(2) & p(3) & \cdots p(n) \end{pmatrix}$$

Uma notação mais compacta é obtida através do uso de ciclos. Se $a_1, a_2, a_3, \cdots, a_k \in S$, então $(a_1\ a_2\ a_3 \cdots a_k)$ denota a permutação dos elementos de S onde

$$a_1 \rightarrow a_2, \quad a_2 \rightarrow a_3, \cdots, a_{k-1} \rightarrow a_k, \quad a_k \rightarrow a_1$$

e $i \rightarrow i$, para todos os outros valores de $i \in S$. Esta permutação é chamada um ciclo (ou k-ciclo) e implica que cada elemento de S aparece apenas uma vez em um único ciclo. Um ciclo com k elementos é dito ter comprimento k.

Definição 2 - *O conjunto das $n!$ permutações de S juntamente com a operação de composição de permutações (funções) é um grupo de permutações denominado o grupo simétrico de grau n e denotado por S_n.*

Mostra-se que, em S_n, a ordem de uma permutação, isto é, o menor inteiro r tal que $p^r = e$ (o mapeamento identidade), é dado pelo mínimo múltiplo comum dos comprimentos de seus ciclos [10]. Dessa forma, em S_3, o grupo simétrico de grau 3, os elementos tem ordem 1, 2 e 3. As $3! = 6$ permutações de S_3 são $p_1 = e$, $p_2 = (12)$, $p_3 = (13)$, $p_4 = (23)$, $p_5 = (123)$ e $p_6 = (132)$.

A família de funções aritméticas $P_n(i)$ definida a seguir, desempenha um papel relevante na escolha de permutações para fins criptográficos.

Definição 3 - *$P_n(i)$ denota o número de permutações de grau n que fixam i elementos, $0 \leq i \leq n, n \geq 1$.*

Algumas propriedades simples da função $P_n(i)$ são listadas a seguir.

Propriedade 1) $P_n(n) = 1$ (Apenas a permutação identidade fixa todos os elementos).

Propriedade 2) $P_n(n-1) = 0$ (Nenhuma permutação muda apenas um único elemento. De fato, excetuando-se a permutação identidade, qualquer permutação muda pelo menos duas posições).

Propriedade 3) $\sum_{i=0}^{n} P_n(i) = n!$

Um papel de destaque é reservado à $P_n(0)$, conforme mostra o lema 1

Lema 1 - $P_n(i) = \begin{pmatrix} n \\ i \end{pmatrix} P_{n-i}(0), \qquad 0 \leq i \leq n-1$

Prova :Existem $\begin{pmatrix} n \\ i \end{pmatrix}$ maneiras de se escolher i elementos dentre os n. Para cada uma delas, os restantes $(n-1)$ elementos mudam todos de posição, o que pode ser feito, por definição, de $P_{n-1}(0)$ maneiras.

O lema 1, apesar de simples, desempenha um papel importante no sentido de caracterizar inteiramente a função $P_n(i)$. Para atingirmos esse objetivo, é necessário determinar $P_{n-1}(0)$ ou, em geral, $P_n(0)$. Nesse ponto é importante observarmos que, do ponto de vista de criptografia, claramente os mais relevantes $P_n(i)$'s são aqueles para os menores valores de i. O lema 2 a seguir mostra que $P_n(0)$pode ser obtida como solução de uma equação de diferenças de segunda ordem com coeficientes variáveis.

Lema 2 - $P_n(0)$ *satisfaz à equação de diferenças*

$$P_n(0) = (n-1)\,[P_{n-1}(0) - P_{n-2}(0)]$$

com condições iniciais e .$P_1(0) = 0$ e $P_2(0) = 1$.

Prova : Uma verificação direta mostra que as condições iniciais são satisfeitas. Sem perda de generalidade, representamos os elementos a serem permutados pelas coordenadas $1, 2, ..., n$. Focalizando nossa atenção em dois tais elementos, digamos 1 e $j, j2, 3, ..., n$, existem duas situações a serem levadas em conta :

i) 1 e j trocam de lugares e então permanecem fixos. Desde que existem $(n-1)$ escolhas para j e $(n-2)$ elementos permanecem para serem permutados, a contribuição é portanto $(n-1)P_{n-2}(0)$.

ii) Agora 1 mapeia em j, mas não vice-versa. Então tudo se passa como se estivéssemos partindo de (i) após a transposição de 1 e j. Novamente existem $(n-1)$ pontos de partida para j, mas agora $(n-1)$ elementos restam para serem (todos) permutados. Isto contribui com $(n-1)P_{n-1}(0)$. Adicionando-se as contribuições em (i) e (ii), a relação desejada é obtida.

3. SOLUÇÃO DA EQUAÇÃO DE DIFERENÇAS

De acordo com o lema 1, para explicitarmos a função $P_n(i)$ precisamos encontrar primeiramente $P_n(0)$. Isso é feito no lema 3 a seguir.

Lema 3 - $P_n(0) = n! \sum_{j=0}^{n} \frac{(-1)^j}{j!}$

Prova : Por indução :

i) Para $n = 1$ e $n = 2$ obtemos, respectivamente, $P_1(0) = 0$ e $P_2(0) = 1$ e , que atende às condições iniciais do lema 2.

ii) Passo de indução : Do lema 2, considerando válida a proposição para n e $n-1$, podemos escrever

$$P_{n-1}(0) = n\left[n! \sum_{j=0}^{n} \frac{(-1)^j}{j!} + (n-1)! \sum_{j=0}^{n-1} \frac{(-1)^j}{j!}\right]$$

Expandindo a expressão e adicionando o termo correspondente a $j = n$ no segundo somatório, chegamos a

$$P_{n-1}(0) = n!\left[n\sum_{j=0}^{n}\frac{(-1)^j}{j!} + \sum_{j=0}^{n}\frac{(-1)^j}{j!} - \frac{(-1)^n}{n!}\right]$$

ou seja

$$P_{n-1}(0) = (n+1)!\sum_{j=0}^{n}\frac{(-1)^j}{j!} + (n+1)!\frac{(-1)^{n+1}}{(n+1)!}$$

e então

$$P_{n+1}(0) = (n+1)!\sum_{j=0}^{n+1}\frac{(-1)^j}{j!}$$

de modo que o resultado é válido para $n+1$, o que conclui o passo de indução e completa a prova.

De posse dos lemas 1, 2 e 3 determinamos $P_n(i)$ Trata-se de um resultado novo que tem implicações interessantes.

Teorema 1 - $P_n(i) = \frac{n!}{i!}\sum_{j=0}^{n-i}\frac{(-1)^j}{j!}, \quad i = 0,1,...,n.$

Prova : Dos lemas 1 e 3, obtemos

$$P_n(i) = \binom{n}{i}(n-i)!\sum_{j=0}^{n-i}\frac{(-1)^j}{j!}$$

e o resultado segue-se após a expansão do coeficiente binomial

Esse resultado indica que, para um dado valor fixo de n, os maiores valores de $P_n(i)$ correspondem a $i = 0$ ou $i = 1$. De fato, como mostra o corolário 1, $P_n(i)$ é máximo para $i = 0$ ou $i = 1$, conforme n seja, respectivamente, par ou ímpar.

Colorário 1 - $P_n(0) - P_n(1) = (-1)^n$.

Prova : Do teorema 1, podemos escrever

$$P_n(0) = n!\sum_{j=0}^{n}\frac{(-1)^j}{j!}$$

e

$$P_n(1) = n!\sum_{j=0}^{n-1}\frac{(-1)^j}{j!}$$

de modo que

$$\begin{aligned} P_n(0) - P_n(1) &= n!\left(\sum_{j=0}^{n}\frac{(-1)^j}{j!} - \sum_{j=0}^{n-1}\frac{(-1)^j}{j!}\right) = \\ &= n!\left.\left(\frac{(-1)^j}{j!}\right)\right|_{j=n} \end{aligned}$$

e o resultado segue.

A Tabela 2 mostra alguns valores de $P_n(i)$. De especial interesse para criptografia é o comportamento de $P_n(i)$ para.$i = 0$ Por razões de segurança é claramente desejável que seja usado, no processo de cifragem, uma das $P_n(0)$ permutações que não fixa nenhum elemento. Entretanto, isto pode ser feito de maneira prática e segura apenas se nós tivermos uma clara compreensão do comportamento relativo de $P_n(i)$ e $n!$.

	n=1	2	3	4	5	6	7	8	9
i=0	0	1	2	9	44	265	1854	14833	133496
1	-	0	2	8	45	264	1855	14832	133497
2	-	1	0	6	20	135	924	7420	66744
3	-	-	1	0	10	40	315	2464	22260
4	-	-	-	1	0	15	70	630	5544
5	-	-	-	-	1	0	21	112	1134
6	-	-	-	-	-	1	0	28	42
7	-	-	-	-	-	-	1	0	36
8	-	-	-	-	-	-	-	1	0
9	-	-	-	-	-	-	-	-	1

TAB. 2: Alguns valores de $P_n(i)$.

4. COMPORTAMENTO ASSIMPTÓTICO

O corolário 2 a seguir mostra um resultado interessante sobre o comportamento relativo assimptótico das funções $P_n(i)$ e $n!$.

Colorário 2 - $\lim_{n\to\infty}\left(\frac{n!}{P_n(i)}\right) = i!e.$

Prova : A expansão em série de Maclaurin da função exponencial $f(x) = e^{-x}$ é

$$e^{-x} = \sum_{j=0}^{\infty}\frac{(-1)^j x^j}{j!}$$

Do teorema 1

$$\frac{P_n(i)}{n!} = \frac{1}{i!}\sum_{j=0}^{n-i}\frac{(-1)^j}{j!}$$

de modo que para $x = l$ e considerando o limite quando $n \to \infty$, obtemos

$$\lim_{n\to\infty}\left(\frac{P_n(i)}{n!}\right) = \frac{e^{-1}}{i!}$$

e o resultado segue.

Esse corolário mostra que o número e pode ser obtido através da função $P_n(0)$ (ou $P_n(1)$). Isto porque, fazendo-se $i = 0$ (ou $i = 1$) no limite acima, resulta em

$$\lim_{n\to\infty}\left(\frac{n!}{P_n(0)}\right) = e$$

A Tabela 3 mostra alguns valores da relação $R = n!/P_n(0)$, de onde se pode perceber a rapidez do processo de convergência (na 10^aiteração, o valor obtido está correto a uma precisão de 10^{-6}).

O corolário 2 fornece algumas indicações úteis sobre a viabilidade de se usar uma das $P_n(0)$ permutações que não fixam nenhum elemento. Especificamente, ele mostra que,

1	∞	6	2,7169811
2	2,0000000	7	2,7184466
3	3,0000000	8	2,7182633
4	2,6666666	9	2,7182837
5	2,7272727	10	2,7182817

TAB. 3: Alguns valores de $R = n!/P_n(0)$.

para um dado valor fixo de n suficientemente grande (e.g., $n \geq 10$), o número de permutações que fixam i elementos, $i = 2, 3, 4, ...$, decresce, de forma monotônica, com percentuais em relação ao total de permutações de, respectivamente, 18, 39%, 6, 13%, 1, 53%, etc. Dessa forma vemos que, mesmo para valores moderados de n (Tabela 2), $P_n(0)$ e $P_n(1)$ representam, cada uma, aproximadamente $(100/R)\% = 36,7\%$ de todas as $n!$ permutações de grau n. Considerando os recursos computacionais do criptoanalista bem como aspectos práticos de implementação, esta informação pode ser usada no projeto de cripto-sistemas que fazem uso de permutações como parte de sua chave privada .

5. EXEMPLOS

Nesta seção alguns exemplos simples são apresentados visando ilustrar alguns dos resultados obtidos anteriormente.

Exemplo 1 - A difusão ótima em uma cifra iterativa é obtida quando qualquer símbolo de texto claro influencia todos os símbolos de texto cifrado em um número mínimo de rodadas. O embaralhamento armênio (Ea), responsável pela difusão ótima no cripto-sistema SAFER+ é um elemento de ordem 70 do grupo simétrico S_16. Especificamente

$$Ea = (1\ 13\ 3\ 5\ 15\ 11\ 9)\,(2\ 6\ 8\ 14\ 12)\,(4\ 16),$$

onde os elementos 7 e 10 são mantidos fixos.

Exemplo 2 - A seguir estão listadas todas as $4! = 24$ permutações de S_4, agrupadas de duas formas, a saber (1) em classes de elementos de mesma ordem $R_4(r)$, $r = 1, 2, 3, 4$ e (2) em classes $F_4(i)$ correspondentes aos valores de $P_4(i)$ para $i = 0, 1, 2, 4 (F_4(3) = 0)$:

$R_4(1)$ $= \{(1)(2)(3)(4) = e\}$.
$R_4(2)$ $= \{(12)(34), (13)(24), (14)(23), (12), (13), (14), (23), (24), (34)\}$.
$R_4(3)$ $= \{(123), (132), (124), (142), (134), (143), (234), (243)\}$.
$R_4(4)$ $= \{(1234), (1243), (1324), (1342), (1423), (1432)\}$.

$F_4(0)$ $= \{(12)(34), (13)(24), (14)(23), (1234), (1243), (1324), (1342), (1423), (1432)\}$.
$F_4(1)$ $= \{(123), (132), (124), (142), (134), (143), (234), (243)\}$.
$F_4(2)$ $= \{(12), (13), (14), (23), (24), (34)\}$.
$F_4(4)$ $= \{(1)(2)(3)(4) = e\}$.

Observa-se que as 6 permutações de maior ordem em S_4 pertencem todas à classe $F_4(0)$, isto é, são permutações que não fixam nenhum elemento.

6. CONCLUSÕES

Permutações tem sido empregadas em cripto-sistemas simétricos ou assimétricos, fazendo parte, ou não, da chave do sistema. Em qualquer caso, o objetivo principal é propiciar a difusão dos símbolos de texto claro sobre o texto cifrado, em consonância com o princípio da difusão de Shannon. Nesse contexto, este trabalho analisa aspectos relativos à escolha de permutações de grau n, visando sua utilização em criptografia. Inicialmente, uma nova família de funções aritméticas $P_n(i)$, indexada em $i, i = 0, 1, ..., n$, foi introduzida, a qual indica o número de permutações de grau n que fixam i elementos. Visando o objetivo de utilizar aquelas permutações que mais contribuam para aumentar a difusão do processo de cifragem, tomou-se necessário explicitar analiticamente $P_n(i)$ e avaliar seu comportamento para valores específicos de i. Algumas de suas propriedades foram estabelecidas e foi mostrado que $P_n(i)$ satisfaz uma equação de diferenças com coeficientes variáveis, cuja solução foi então obtida. Dessa forma, foi possível estabelecer uma avaliação quantitativa que tem implicações para o projeto de cripto-sistemas que empregam permutações em sua chave privada. O comportamento assimptótico de $P_n(i)$ foi analisado e mostrou-se que a relação entre o número total de permutações de grau n e $P_n(0)$ converge para o numero e, a base do sistema de logaritmos neperianos.

AGRADECIMENTOS

Os autores agradecem as valiosas sugestões dadas pelo Professor Hélio M. de Oliveira durante a preparação deste trabalho.

REFERÊNCIAS

[1] C. E. Shannon, "Communication Theory of Secrecy Systems", Bell System Tech. J., vol. 28, pp. 656-715, Oct., 1949.

[2] National Bureau of Standards, NBS FIPS PUB 46, "Data Encryption Standard", US Department of Commerce, January 1977.

[3] Advanced Encryption Standard (AES) - A Crypto Algorithm for the Twenty-first Century, http ://www.nist.gov/aes, http ://www.cylink.com/SAFER.

[4] J. L. Massey, "On the Optimality of SAFER+ Diffusion", Second Advanced Encryption Standard Candidate Conference, Rome, Italy, March 22-23, 1999.

[5] R. J. McEliece, "A Public-Key Cryptosystem Based on Algebraic Coding Theory", DSN Progress Report 42-44, pp. 114-116, Jet Propulsion Laboratory, Pasadena, CA, Jan./Feb. 1978.

[6] R. M. Campello de Souza, J. Campello de Souza, "Array Codes for Private-Key Encryption", Electronics Letters, vol. 30, No. 17, pp. 1394 - 1396, August 1994.

[7] R. M. Campello de Souza, J. Campello de Souza, "Códigos Produto Multiníveis Para Correção de Erros Bi-Separáveis com Aplicações em Criptografia", Revista Brasileira de Telecomunicações, vol. 10, No. 1, pp. 7 - 14, dezembro 1995.

[8] P. Mathys, "On the Specification of Permutations for Block Ciphers", Proceedings of the IEEE International Symposium on Information Theory, pg. 232, January 1990.

[9] L. Mittenthal, "A Source of Cryptographically Strong Permutations for Use in Block Ciphers", Proceedings of the IEEE International Symposium on Information Theory, pg. 233, January 1990.

[10] J. R. Durbin, "Modern Algebra", 3rd. Ed., JohnWiley, 1992.

Ricardo Menezes Campello de Souza formou-se em Engenharia Elétrica pela Universidade Federal de Pernambuco em 1974, obteve o título de Mestre em Ciências pela mesma Universidade em 1979 e o titulo de PhD pela University of Manchester, Inglaterra, em 1983, ambos em Engenharia Elétrica. Desde 1979 é Professor do Departamento de Eletrônica e Sistemas da UFPE, onde foi coordenador do Programa de Pós-graduação em Engenharia Elétrica no período 1984-1987, Chefe do Departamento no período 1987-1992 e atualmente ocupa a posição de Professor Adjunto. Seus interesses de pesquisa incluem matemática discreta, criptografia, teoria algébrica da codificação e processamento digital de sinais.

André Neumann Kauffman formou-se em Engenharia Elétrica, modalidade Eletrônica (*cum laude*), pela Universidade Federal de Pernambuco em 1997, onde cursa atualmente o programa de Mestrado em Engenharia Elétrica. Seus interesses de pesquisa incluem matemática discreta, criptografia e processamento digital de sinais.

Rossana Claudia Cursino Lima é concluinte do Curso de Graduação em Engenharia Elétrica, modalidade Eletrônica, da Universidade Federal de Pernambuco. Seus interesses de pesquisa incluem criptografia, processamento digital de sinais e comunicações móveis.