Criptografia com números irracionais

Fábio Borges
borges@lncc.br

Renato Portugal
portugal@lncc.br

Jauvane C. de Oliveira
jauvane@lncc.br

Resumo

Definição. Seja $\mathbb{M}$ o conjunto de todas as mensagens possíveis e $\mathbb{C}$ o conjunto de todos criptogramas. Dizemos que um criptossistema garante um Segredo Perfeito quando as probabilidades P satisfazem à condição

$$P_C(M) = P(M), \tag{1}$$

para todo $M \in \mathbb{M}$ e todo $C \in \mathbb{C}$.

Shannon [2] mostrou que existe pelo menos um criptossistema, *one-time-pad*, que garante um segredo perfeito. Comparado à criptografia assimétrica, temos a diferença entre segurança computacional e segurança matemática. Hoje, o *one-time-pad* é conhecido como o único sistema matematicamente seguro [1], no entanto, tem o inconveniente que o tamanho da chave deve ser maior ou igual o da mensagem.

Na tentativa de criar criptossistemas seguros, surgiram os algoritmos classificados como *key stream*. Tais algoritmos tentam gerar, a partir da chave, uma seqüência aleatória do tamanho da mensagem. Como a chave é menor que a mensagem, temos que a igualdade (1) não é satisfeita. Nesse método, uma nova chave pode ser estabelecida a cada troca de mensagem.

Os dígitos fracionários de um número irracional são uma seqüência infinita que não tem período. Evidente que quanto maior a seqüência maior o processamento necessário para calculá-la, no entanto, poderíamos ter uma chave menor que a mensagem. Nosso objetivo é transferir o custo do tamanho da chave para um custo computacional.

Teorema 1 *Dados um produto de primos distintos $p_1 \cdots p_n$ e $r > 1$, inteiro, temos que $\sqrt[r]{p_1 \cdots p_n}$ é um número irracional.*

Prova. Suponha, por contradição, que esta raiz é um número racional na sua forma irredutível, isto é, $mdc(a, b) = 1$,

$$\sqrt[r]{p_1 \cdots p_n} = \frac{a}{b},$$

logo

$$p_1 \cdots p_n b^r = a^r,$$

assim $p_1 | a^r$ e conseqüentemente $p_1 | a$. Seja $a = a' p_1$, então

$$p_1 \cdots p_n b^r = (a' p_1)^r.$$

Portanto

$$p_2 \cdots p_n b^r = a'^r p_1^{r-1}.$$

O que é uma contradição, pois p_1 não dividir fator algum a esquerda da igualdade, uma vez que $mdc(a, b) = 1$. ■

Agora temos um gerador de infinitos números irracionais. Antecipadamente apresentamos o algoritmo em 1.

Algoritmo 1 Número Irracionais

Recebe uma mensagem M
Recebe uma chave $r, c, d, p_1, \ldots, p_n$
$I = \frac{c}{d}\sqrt[r]{p_1 \cdots p_n}$
k recebe $|M|$ casas decimais da mantissa de I
para $i := 1$ até $|M|$ **faça**
    $C[i] = k[i] \oplus M[i]$
retorne C

O algoritmo 1 se resume no *one-time-pad*, pois com os números racionais podemos formar qualquer seqüência que queiramos, uma vez que podemos aproximar qualquer número por um número racional. Neste caso, temos o inconveniente que a chave pode ficar maior que a mensagem.

Teorema 2 *Se*

$$\sqrt[r]{p_{m+1}} - \sqrt[r]{p_m} < 1,$$

com p_m e p_{m+1} primos consecutivos, então todo número pode ser aproximado através da raiz de um produto de primos.

Prova. Seja k o número que desejamos aproximar, então

$$k^r = p_1 \ldots p_n(f_1 \ldots f_s),$$

onde f_i são fatores primos com potências maiores que um. Se p_m o maior primo menor que $f_1 \ldots f_s$

$$p_m < f_1 \ldots f_s < p_{m+1}.$$

Assim, usando a hipótese, temos que

$$\sqrt[r]{f_1 \ldots f_s} - \sqrt[r]{p_m} < 1.$$

■

Para se provar que o algoritmo 1 é um segredo perfeito é necessário provar a hipótese do teorema 2, no entanto, tal hipótese não deve ser simples de se provar, pois é uma generalização da conjectura de Andrica [3],

$$\sqrt{p_{m+1}} - \sqrt{p_m} < 1. \tag{2}$$

Outra questão que ficou pendente foi como passar números primos grandes sem aumentar muito o tamanho da chave. As entradas do algoritmo 1 podem receber expressões matemáticas e localizar o menor primo maior que o resultado da expressão. Por exemplo, podemos passar $próximo\_primo(5^{604})$, tal número tem 423 dígitos decimais.

Neste caso, o espaço de busca das chaves é maior que a mensagem, além de termos todas as combinações de criptograma, assim se a conjectura (2) for satisfeita temos (1) um segredo perfeito.

Referências

[1] Bruen, A and Forcinito, M. A., Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century, Wiley-Interscience, (2004)

[2] Shannon, C. E., Communication theory of secrecy systems , *Bell System Tech. J.*, vol. 28, pp. 656–715 (1949)

[3] Smarandache, F., Conjectures which generalize Andrica's conjecture, *Octogon Math. Mag.*, vol. 7, pp. 173–176 (1999)