Criptografia de textos baseada na difração de ondas em fenda simples

Hitoshi S. Yanaguibashi, Carlos R. A. Peixoto
Centro Universitário do Pará (CESUPA) – Área de Ciências Exatas e Tecnologia (ACET)
Laboratório de Computação Natural (LCN) - 66.060- 230, Belém – Pará – Brasil
E-mail: {hitoshiseki, carlosrapeixoto}@gmail.com

Igor Ruiz Gomes
Centro Universitário do Pará (CESUPA) – Área de Ciências Exatas e Tecnologia (ACET)
Laboratório de Computação Natural (LCN) - 66.060- 230, Belém – Pará – Brasil
E-mail: ruiz.igor@gmail.com

RESUMO

A quantidade de dados transferidos na internet e em empresas é muito grande, e nem todos podem ser acessados por qualquer pessoa. Portanto, os esquemas de criptografia, que são usados para manter o sigilo de mensagens ou de dados armazenados [2], entram em ação. Como consequência do avanço dos esquemas criptográficos, surge um maior número de pessoas tentando ultrapassar estas barreiras. Diante desse fato, novas propostas de criptografia são criadas, e uma delas é a Criptografia baseada na difração de ondas em fendas simples.

Chama-se de difração de uma onda, o encurvamento sofrido por seus raios quando a onda encontra obstáculos à sua propagação [3], de forma mais simples, é a capacidade que a onda tem de contornar obstáculos.

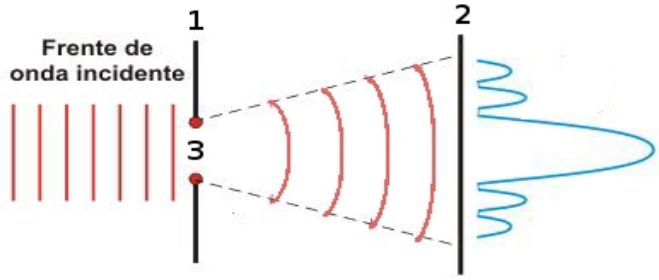

Figura 1 – Difração de onda.

A idéia da criptografia será explicada com base na Figura 1. O ponto 1 é o primeiro anteparo que possui uma fenda no ponto 3, por onde as ondas irão passar. Ao passar pela fenda, as mesmas sofrem difração e seguem para um segundo anteparo, no ponto 2, que é onde elas irão incidir. O desenho em azul representa a intensidade da onda no momento em que ela incide no anteparo 2. Logo, é importante notar que o meio do anteparo 2 é atingido com mais intensidade do que os demais. Como visto na ilustração, os picos imediatamente adjacentes ao pico máximo possuem uma intensidade relativamente baixa quando comparados com o maior[1]. A mesma utiliza a criptografia de substituição de caracteres.

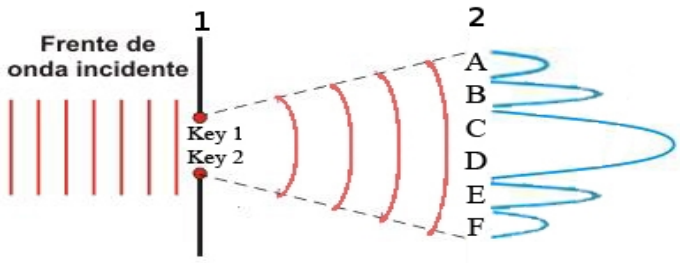

Figura 2 – Difração criptográfica.

A figura 2 ilustra a proposta da criptografia baseada na difração de ondas em fenda simples, onde, na realidade, o objetivo da mesma é alcançado com a incidência de apenas uma onda. Conforme explicado na figura 1, o ponto 1 representa o primeiro anteparo que possui uma fenda, é importante notar que agora a fenda possui duas chaves, *Key* 1 e *Key* 2. As ondas difratam e incidem em um anteparo 2, que é o texto a ser criptografado.

A frente de onda incide no anteparo 1 e parte da onda que difrata na fenda recebe duas chaves criptográficas, *Key* 1 e *Key* 2. Ao longo do caminho, a onda vai perdendo energia, logo, a onda incide com maior intensidade no meio do anteparo 2, que é a trajetória que forma 90º com o anteparo 1, e com menor intensidade nas extremidades. A quantidade de vezes que um caractere é criptografado está diretamente ligado à intensidade da onda, no momento em que incide no anteparo. Em uma situação normal, a intensidade dos picos adjacentes ao pico maior seriam bem menores que o mesmo, mas no problema proposto, a intensidade diminuirá de uma razão constante.

Para criptografar o texto, é necessário que seja determinado o número de vezes que um caractere irá receber a chave criptográfica, que também é um caractere. Para isso, é verificado se o número de caracteres do texto é ímpar ou par, caso seja ímpar, é feita uma alteração para torná-lo par. Depois, o número de caracteres do texto é dividido por 2, onde resultado é o número de iterações para recebimento da chave. A *Key* 1 será responsável por criptografar a primeira metade e a *Key* 2, a segunda metade do texto. Por exemplo, o texto "ABCDEF" tem 6 caracteres, isso significa que serão feitas 3 iterações. Portanto, os caracteres 'C' e 'D' irão receber 3 vezes as chaves *Key* 1 e *Key* 2, respectivamente, e os adjacentes serão somados menos vezes. Ao final tem-se 'A' e 'F' modificados para 'A'+Key 1 e 'F'+Key 2, 'B' e 'E' para 'B'+Key 1+Key 1 e 'E'+Key 2+Key 2 , 'C' e 'D' para 'C'+Key 1+Key 1+Key 1 e 'D'+Key 2+Key 2+Key 2.

As principais vantagens dessa criptografia, que dificultam a quebra da mensagem, é que a codificação dos caracteres depende das posições em que estão[4], e não do tipo dos mesmos, portanto, dificilmente duas letras iguais terão a mesma representação ao serem criptografadas, além de que o texto poderá ser criptografado por duas chaves, diferentes ou não.

A criptografia proposta foi desenvolvida utilizando a linguagem de programação Java. Os testes realizados, utilizando esta idéia, foram bastante positivos do ponto de vista da velocidade de codificação e decodificação de textos, da segurança proporcionada, que é relativamente boa, além da facilidade de implementação do algoritmo para atingir tal objetivo.

Como trabalhos futuros, pretende-se aumentar a complexidade da criptografia, com a proposta de se utilizar a idéia da difração de ondas em fendas duplas, onde já se consideram as interferências que podem ser geradas entre as ondas.

Palavras-chaves*: Difração, Fenda, Criptografia*

Referências

[1] H. L. FRAGNITO, A. C. COSTA, *"Difração da luz por fendas"*, Unicamp-IFGW, 2008.

[2] J. A BUCHMANN, "*Introdução à criptografia"*, Berkeley, 2001.

[3] N. V. BÔAS, R. H. DOCA, G. J. BISCUOLA, "*Tópicos de física 2: termologia, ondulatória e óptica"*, Saraiva, 2002.

[4] R. B. CHIARAMONTE, E. D. MORENO, *"Criptografia Posicional: Uma Solução para Segurança de Dados - CONCEITOS, EXEMPLOS E DESEMPENHO"*, Faculdade de Informática de Marília, 2001.