Técnica de Criptografia Baseada na Evolução de Autômatos Celulares Unidimensionais

Polycarpo S. Neto, Wellington D. de Almeida e Francisco J. A. de Aquino

***Resumo*— Este artigo tem por objetivo o estudo de um método criptográfico baseado em autômatos celulares unidimensionais juntamente com um código corretor de erros, visando o desenvolvimento de uma técnica alternativa de criptografia de mensagens de texto. A principal diferença na aplicação desta técnica sobre um conjunto de informações é a não existência de padrões pré-definidos ou conhecidos.**

Palavras-chave: **Criptografia, Autômatos celulares, Código de blocos.**

I. INTRODUÇÃO

A comunicação entre dispositivos nos tempos contemporâneos torna-se cada vez mais indispensável. Junto com a necessidade de comunicação, existe a necessidade de prover novas técnicas de segurança da informação [1]. Em substituição aos métodos tradicionais, a criptografia baseada no caos, a partir do uso dos autômatos celulares (AC) é uma das formas emergentes de criptografia e mostra-se bastante eficaz, pois baseia-se na não existência de padrões pré-definidos que facilitam o trabalho de quem tenta descobrir a mensagem [2].

Um autômato celular (AC) unidimensional têm o comportamento de um vetor de *N* células, cada uma com valor binário e evoluem a partir de uma regra. Os estados das células são alterados conforme as regras de transição, que dependem da vizinhança, que são as células em torno da célula que será. Podemos representar a composição de um AC como $\gamma = (L, k, \delta, f)$, onde o *L* é conhecido como *lattice* do autômato e representa sua forma geométrica, *k* é o conjunto de estados assumíveis por cada célula, δ é a vizinhança de uma determinada célula (fator influenciado pelo raio r definido para o autômato) e o f a função de transição de estado [1-4].

Neste trabalho, buscamos implementar um código no software *Scilab* para criptografia de textos de tamanhos variáveis utilizando regras dos autômatos celulares caóticos.

II. FUNDAMENTAÇÃO

A. Criptografia de chave privada

Dizemos que um método criptográfico é de chave privada, quando é usada apenas uma única chave tanto para criptografar, quanto decriptar a mensagem. Desse modo, os envolvidos na comunicação precisam possuir a mesma chave e esta deve ser secreta (ver Fig. 1). Para que este mecanismo possa funcionar com segurança, é necessária a existência de um canal seguro para a transmissão da chave, e esta deve ser trocada a cada nova comunicação, caso contrário está sujeita a ser quebrada por criptoanálise[3].

Fig.1. Criptografia de chave privada.
Fonte: Os autores.

B. Autômatos Celulares Caóticos

Os AC's são modelos computacionais cuja evolução é processada a partir de suas condições iniciais usando uma função que determina o estado da próxima geração [4]. Do ponto de vista criptográfico, deseja-se obter um AC que é capaz de prescrever uma evolução caótica [2-5]. Para um AC de raio r=1, temos a evolução dada pela Eq.1 para produção de sequências aleatórias:

$$x_i^{t+1} = x_{i-1}^t \oplus x_i^t V x_{i+1}^t \quad (1)$$

O comportamento instável de um autômato num sistema determinístico influenciado por um número razoável de fatores, é o que definimos como caos determinístico. Graças a dependências das iterações anteriores e das condições iniciais, acaba existindo uma amplificação dos erros existentes, assim o autômato adota um comportamento pseudoaleatório. Essa dependência garante que para pequenas modificações na entrada, teremos grandes modificações na saída.

C. Código de bloco

Para obter um código de bloco (*n*,*k*), o codificador de canal aceita a informação em blocos sucessivos de *k bits*, para cada bloco, ele adiciona *n-k bits* redundantes que se relacionam algebricamente como os k bits de mensagem, produzindo um bloco codificado de *n bits*, sendo que *n>k*. O bloco de *n bits* denomina-se palavra código e *n*, tamanho de bloco do código.

O codificador produz bits à taxa $R_0 = (n/k)\,Rs$, onde *Rs* é a taxa de bits da fonte de informação. A relação $r = k/n$ é a taxa de código, onde o intervalo de valores varia de 0 à 1. A taxa R_0 denomina-se taxa de dados do canal. Vemos assim que a taxa de código é uma grandeza adimensional, enquanto a taxa de dados do canal pode ser medida em *bits/s*[3].

Polycarpo S. Neto, Wellington D. de Almeida e Francisco J. A. de Aquino são afiliados ao Instituto Federal de Educação Ciência e Tecnologia do Ceará (IFCE), Fortaleza, CE, Brasil. Emails: policarponeto.pn@gmail.com, wellingtondantas39@gmail.com , fcoalves_aq@ifce.edu.br.

III. METODOLOGIA

A metodologia desta técnica é dividida em três partes, uma de pré-processamento, uma de evolução das regras dos autômatos e outra de pós-processamento. A técnica desenvolvida neste artigo funciona atualmente para caracteres de codificação ASCII estendida.

O pré-processamento consiste em preparar o texto para retirada de erro por possíveis regras não completamente invertíveis. Essa parte do método é ainda composta da inserção de informações extras intercaladas entre os bits da mensagem original.

Depois que ocorre o pré-processamento da mensagem, é feita uma adição de bits de paridade para que se possa fazer correções futuras. Para isso, foi utilizado um código de bloco linear, onde para cada 4 bits de informação do texto limpo, existem 4 bits de informação redundante, sendo então que num vetor de 8 bits (1 byte), tem-se uma taxa de código de 1/2.

Nesse ponto, a mensagem deve ser entendida como um conjunto de bits formadores do autômato, estando sujeita a regras de evolução por n ciclos, com $n \geq 0$. No processo de recuperação, o autômato evolui novamente n vezes de acordo com as regras complementares, que para este processo, são comutativas (ver Tabela I). Por fim, a mensagem obtida da solução do criptograma, passa pelo código corretor de erros.

TABELA I. RELAÇÃO DE PARES DE REGRA.

REGRAS DE EVOLUÇÃO	REGRAS COMPLEMENTARES	NÚMERO DE CICLOS
15	85	1
51	51	5
170	240	2
204	204	4
43	113	1

Fonte: Os autores.

IV. RESULTADOS

Utilizando como texto a ser criptografado, a informação "*Encontro Anual do Iecom em Comunicações, Redes e Criptografia*.", obtemos de resultado o seguinte criptograma visto na Fig.2:

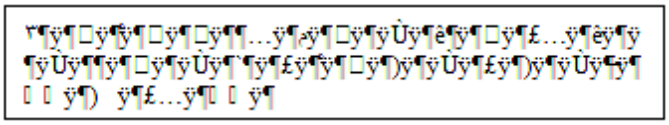

Fig.2. Criptograma.
Fonte: Os autores.

Depois de obter o criptograma, pela passagem das regras complementares de evolução reversa dos autômatos, obtemos como mensagem recuperada a mensagem "*Encontro Anual do Iecom em Comunicações, Redes e Criptografia*".

Sabendo que, ao criptografar o texto, os caracteres obtidos não têm padrão reconhecível, que mostre qualquer similaridade com o texto original, e que, pela adoção do código corrector de erro de taxa 1/2, o número de caracteres no criptograma é o dobro de caracteres do texto claro, fica difícil ao interceptador conseguir obter a mensagem original. Com a finalidade de comprovar os resultados, é mostrado na Fig.3 (Histograma Original) e na Fig.4 (Histograma cript.) a distribuição das freqüências dos valores dos objetos que compõem a mensagem original e a mensagem criptografa (criptograma). Observando as duas figuras vemos que, os gráficos são totalmente diferentes, fato decorrente da caóticidade dos autômatos que desordena a mensagem original por.

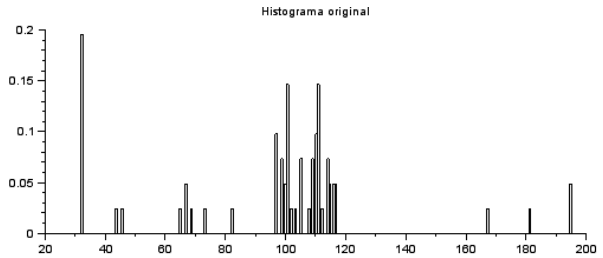

Fig.3. Histograma do texto original.
Fonte: Os autores.

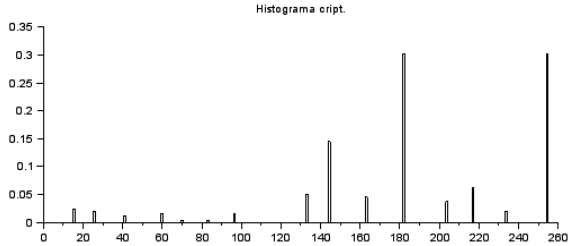

Fig.4. Histograma do texto criptografado.
Fonte: Os autores.

V. CONCLUSÃO

Neste artigo foi realizado o estudo sobre uma nova técnica de criptografia baseada nos AC's. A técnica obtida mostra-se eficaz, com pequenos problemas corrigidos a partir de um código corretor de erro em relação ao uso do par de regras 43 ↔113, que gerou erros para ciclos n>1. Pelos testes feitos com cada regra, conclui-se que existe a comutatividade entre estas, sendo que cada regra, é totalmente reversível por sua complementar. Como principal conclusão, fica que, é um método seguro, onde não existem padrões conhecidos e qualquer mudança nas condições iniciais provoca grandes diferenças na saída criptografada.

REFERÊNCIAS

[1] M.L.A. Castro e R.O.Castro. "Autômatos celulares: implementações de von Neumann, Conway e Wolfram." *Revista de Ciências Exatas e Tecnologia* 3.3, 2008, pp. 89-106.

[2] A.C.Rojas, e A.R. Matas. "Autómatas celulares y aplicaciones." UNIÓN, Revista Iberoamericana de Educación Matemática 46, 2016, pp. 33-48.

[3] S. Haykin. Sistemas de comunicação analógicos e digitais. Bookman 4 ed., 2004.

[4] T.C. dos Santos, Cellular automata and cryptography, Dissertação de Mestrado, Universidade do Porto, Porto, Faculdade de Ciências da Universidade do Porto em Ciência de Computadores, 2014.

[5] E.C.Silva, J.A.J.P.Soares, e D.A.Lima. "Autômatos celulares unidimensionais caóticos com borda fixa aplicados à modelagem de um sistema criptográfico para imagens digitais." *Revista de Informática Teórica e Aplicada*, 23.1, 2016, pp. 250-276.