RECOMENDAÇÃO PARA O USO DO TESTE DE FREQUÊNCIA MONOBIT DO NIST EM SISTEMAS CRIPTOGRÁFICOS

Carlos Eduardo Pantoja

Nilson Mori Lazarin

Paulo Afonso Lopes da Silva

RESUMO: Visto que o NIST Test Suite é amplamente utilizado na criptologia para verificar a eficácia de geradores de números pseudoaleatórios, o objetivo deste artigo é direcionar a utilização de um de seus testes, o de Frequência Monobit, propondo um novo valor para a sequência de bits de entrada. Para isto, foram realizados experimentos com dez algoritmos criptográficos reconhecidamente não aleatórios, demonstrando, inclusive, a ineficácia desse teste estatístico com n=100.

Palavras-chave: NIST Test Suite, Criptologia, Teste de Frequência Monobit

ABSTRACT: The NIST Test Suite is widely used in cryptography to verify the efficacy of GNPAs. The objective of this paper is to direct the use of the Frequency Monobit Test proposing a new value for the initial bit sequence. Hence experiments were realized with ten cryptographic algorithms truly non-random, exposing the inefficacy of the test.

Keywords: NIST Test Suite, Cryptology, Frequency (Monobit) Test

1. INTRODUÇÃO

O *NIST Test Suite* (RUKHIN et al., 2010) é um pacote estatístico composto por quinze testes desenvolvidos pelo *National Institute of Standards and Technology* (NIST) para certificar a aleatoriedade de sequências binárias. Estas são comumente geradas por um GNPA (Gerador de Números Pseudoaleatórios) implementado em hardware ou software e utilizado em sistemas criptográficos para expansão de chaves, visando aumentar o nível de confusão[1] e difusão[2] de um algoritmo criptográfico.

Testes de aleatoriedade também são utilizados para mensurar a saída de algoritmos criptográficos, pois um dos requisitos esperados é que sua saída seja tão aleatória quanto a saída de um GNPA. Um GNPA adequado para uso em aplicações criptográficas precisa, no entanto, atender requisitos mais exigentes do que em outras aplicações, já que a saída deste deve ser imprevisível, mesmo que a semente[3] seja fraca. Esses testes são úteis, inclusive, para determinar se um dado GNPA é adequado ou não para aplicação em criptografia, porém nenhum conjunto de testes estatísticos pode absolutamente certificá-lo como apro-priado.

É importante acrescentar que o NIST *Test Suite* foi utilizado como um dos parâme-tros de avaliação dos candidatos ao concurso AES (*Advanced Encryption Standard*), no qual um algoritmo criptográfico foi eleito como padrão internacional para proteção de sistemas e dados (transações bancárias pela internet, por exemplo) (SOTO, 1999 e SOTO; BASSHAM, 2000). Entretanto, algumas inconsistências no NIST Test Suite foram apresentadas por Kim et al. (2004) e por Hamano e Kaneko (2007). Em 2009 o NIST alertou sobre um problema com a rotina de Transformada Rápida de Fourier, orientando que fossem desprezados os resultados deste teste até que uma atualização fosse divulgada.

Contudo, a necessidade de correções no *NIST Test Suite* colocou em discussão a usabilidade de cada um dos testes disponíveis. Particularmente no Teste de Frequência Monobit, observou-se a recomendação do NIST de que o comprimento mínimo de uma se-quência de bits de entrada (n) a ser testado na avaliação devesse obedecer à condição n >= 100, mas que em outros testes a sequência inicial deveria ser aleatória, assim, caso a en-trada seja considerada não aleatória, não haverá a necessidade de se prosseguir com os demais testes (RUKHIN et al., 2010, p. 25).

O objetivo deste trabalho é avaliar o desempenho do Teste de Frequência Monobit sobre amostras de sistemas criptográficos defasados, demonstrando, as limitações no uso do teste para avaliação de sistemas criptográficos computacionais. Para tanto, o texto organiza-se do seguinte modo: na segunda seção, são apresentados alguns métodos criptográficos históricos; na terceira, é abordado o teste de hipótese; na quarta, é descrito o teste de frequência Monobit; na quinta, são apresentados os experimentos realizados com uma aná-lise dos resultados; e a conclusão é apresentada na sexta seção.

2. CRIPTOGRAFIA

Criptografia é o conjunto de técnicas que proveem proteção na troca de mensagens entre remetente e destinatário de forma que um terceiro (não autorizado) não consiga obter o conteúdo da mensagem. Entretanto, os sistemas criptográficos apresentados nesta seção são inseguros contra um ataque computacional e alguns até com uma análise manual podem ser quebrados (FALEIROS, 2011). Por esse motivo, espera-se que um texto criptografado por qualquer cifra apresentada nesta seção deva ser reprovado em um teste de aleatoriedade.

Cifras de transposição

O método de transposição consiste em permutar a posição dos caracteres de uma mensagem em claro, transformando essa entrada em um anagrama e a chave de cifração utilizada define a ordem em que os caracteres serão permutados (BEZERRA et al., 2010 e TANENBAUM, 2003).

O Bastão de Licurgo (Scytale) é um método criptográfico que data de 475 a.C. com-posto de um bastão e uma fita; nesse método o remetente enrola a fita no bastão e escreve a mensagem. Em seguida, a fita é desenrolada e enviada até o destinatário que somente recuperará a mensagem original caso enrole a fita em um bastão com o mesmo diâmetro daquele utilizado pelo remetente (DIAS, 2006).

Rail Fence é uma cifra criptográfica utilizada na Guerra de Secessão norte-americana (1861-1865) cujo método baseia-se na transposição geométrica de caracteres (TKOTZ, 2005). O remetente escreve a mensagem em zigue-zague, utilizando varias linhas e formando, assim, o texto cifrado que é enviado ao destinatário.

Já a Grade Giratória de Fleissner, proposta em 1881, consiste em método criptográ-fico que utiliza uma folha de papel e um cartão

[1] O conceito de confusão está relacionado à tentativa de um algoritmo "tornar a relação entre o texto em claro, o criptograma e a chave tão complexa tão complexa quanto possível" (LAMBERT, 2004).

[2] Mudanças dos bits de forma que os padrões existentes sejam espalhados. (LAMBERT, 2004).

[3] Valor de inicialização para funções geradoras de números aleatórios.

quadrado, dividido em números pares de células. O cartão é disposto sobre o papel e contém células vazadas onde a mensagem em claro é escrita. Ao se preencher todas as células vazias, o cartão é sempre e sequencial-mente girado em 90º, até que se complete, em quatro giradas, 360º. Dessa forma, o destina-tário obterá a mensagem original se possuir um cartão idêntico ao usado pelo remetente (TKOTZ, 2005).

Cifras de substituição monoalfabéticas

As Cifras de Substituição Monoalfabética são baseadas na troca de cada caractere da mensagem original por outro caractere qualquer, com base em uma tabela previamente estabelecida (BEZERRA et al., 2010).

O ATBASH, em específico, é uma cifra de origem hebraica datada de 600 a.C, que consiste na substituição simples de cada caractere deste alfabeto pelo seu reverso (DIAS, 2006). Dessa forma, a letra A (aleph, primeira do alfabeto) era substituída pela letra T (taw, última do alfabeto), a letra B (beta, segunda do alfabeto), substituída pela letra S (shin, pe-núltima do alfabeto), assim por diante (BEZERRA et al., 2010).

A Cifra de Políbio (203 a.C - 120 a.C), por outro lado, é baseada na troca de cada le-tra da mensagem original por um par de números que representam linha e coluna em uma tabela de substituição (TKOTZ, 2005).

Por fim, é preciso destacar a Cifra de César, elaborada pelo general Júlio César, por volta de 50 a.C. (TKOTZ, 2005). Nessa cifra, o remetente substitui cada caractere da men-sagem original pelo caractere que se encontra três posições a frente no alfabeto (BEZERRA et al., 2010).

Cifras de substituição polialfabéticas

O primeiro sistema criptográfico polialfabético foi proposto por Leon Battista Alberti (1404-1472). Uma cifra polialfabética é aquela que combina várias cifras monoalfabéticas, ou seja, um único caractere na mensagem original poderá ser representado por caracteres distintos na mensagem cifrada (BEZERRA et al., 2010).

O Disco de Alberti é datado de 1466 e seu sistema criptográfico consiste em um disco com dois anéis concêntricos, um externo fixo e um interno móvel. Remetente e destinatário combinam o deslocamento do disco interno de forma que o processo de cifração se dá pela substituição de cada letra da mensagem original (no disco externo) pelo caractere equi-valente no disco interno.

A Cifra de Della Porta é datada de 1563 e é considerada como a primeira cifra de chave dupla (TKOTZ, 2005). Nesse método, são utilizados onze alfabetos de cifração distin-tos e a cada letra da mensagem original criptografada o alfabeto é substituído (BEZERRA et al., 2010).

A cifra de Vigenère é datada de 1586, sua forma de funcionamento é baseada na uti--lização de diversos alfabetos de substituição e cada caractere é substituído pelo alfabeto escolhido pela chave de cifração (DIAS, 2006).

Cifras eletromecânicas

Os sistemas criptográficos eletromecânicos surgiram no séc. XX com o intuito de facilitar o envio de mensagens secretas (DIAS, 2006). O dispositivo de maior destaque é a Máquina Enigma, amplamente utilizada na Segunda Guerra Mundial, baseada na substituição polialfabética através de rotores.

3. TESTE DE HIPÓTESE

O objetivo dos Testes de Hipóteses é verificar se uma determinada afirmação a respeito de determinada população é verdadeira (SILVA, 1999). Um teste de hipótese pode ser comparado a um julgamento, onde se assume inicialmente que o réu é inocente e o promotor deve provar a culpa do réu (MUNDIM, 2010). Conforme Silva (1999) todo teste de hipótese é formado de duas hipóteses:

H_0 , denominada hipótese de nulidade, é a afirmação a respeito do que está sendo testado e é considerada verdadeira. Entretanto, tenta-se provar que H0 é falsa com base em uma evidência, ou seja, diz-se que a diferença é estatisticamente significante.

H_1, hipótese alternativa, representa o que se deseja provar ou estabelecer, sendo formulada para contradizer a hipótese nula.

4. TESTE DE FREQUÊNCIA MONOBIT

Dada uma sequência binária qualquer o Teste de Frequência Monobit, verifica se a ocorrência de 0's pode ser considerada igual à ocorrência de 1's, ou seja, se a proporção de 0's e 1's é ½; caso seja, a sequência é considerada aleatória (RUKHIN et al., 2010).

Embora a ordem de aplicação dos quinze testes disponíveis na Suíte seja arbitrária, o

NIST aconselha que o ensaio de frequência seja executado primeiro, uma vez que esse fornece a evidência mais fundamental para a existência de não aleatoriedade em uma se-quência binária. Caso uma sequência não seja considerada aleatória neste teste, a probabilidade de também não o ser nos outros testes é alta.

O teste de frequência Monobit é dado pelo seguinte teste de hipóteses:

(H_0): a proporção de 0's e 1's é igual, ou seja, p=1/2.

(H_1): p ≠1/2.

Enquanto no teste de hipóteses clássico a probabilidade de erro é definida antes do teste, no conceito moderno denomina-se valor p, que é a probabilidade de retirar a amostra em mãos se a hipótese de nulidade é verdadeira. A regra de decisão é a seguinte: rejeitar a hipótese de nulidade se o valor p é "pequeno" (usualmente, até 5%). O valor p, ou p-valor, é uma estatística utilizada para sintetizar o resultado de um teste de hipóteses. Formalmente, o valor p é definido como a probabilidade de se obter uma estatística de teste igual ou mais extrema quanto àquela observada em uma amostra, assumindo verdadeira a hipótese de nulidade.

Conhecidos estes conceitos, pode-se interpretar os resultados do primeiro teste do NIST ao se verificar se uma sequência de bits pode ser considerada aleatória. Conforme RUKHIN et al. (2010), o teste é realizado através dos seguintes passos:

1. Calcula-se , $S_n = \sum_{i=1}^{n} X_i$, onde $X_i = \{-1, +1\}$ onde X_i= {-1,+1} caso X_i seja 0 ou 1, respectivamente.
2. Calcula-se S_{obs}, onde: $s_{obs} = \frac{|S|}{\sqrt{}}$
3. Calcular o valor P= $\left(1 - \frac{1}{\sqrt{2\pi}} exp\left(-\frac{1}{2} {S_{obs}}^2\right)\right) x2$
4. Comparar o valor p com um valor de referência arbitrado.

O valor de referência no quarto passo é chamado de nível de significância (α). Esse valor representa a probabilidade de se rejeitar a hipótese de nulidade sendo ela verdadeira, ou seja, a probabilidade de concluir que a hipótese de nulidade é falsa quando a hipótese é, de fato, verdadeira (SILVA, 1999).

Para o NIST, os valores usuais de α são: 0.05, 0.01, ou 0.001. Dessa maneira, o nível de significância é a probabilidade de concluir que uma sequência binária é não aleatória, quando, na realidade, é aleatória; se o valor p é maior que α, então a sequência pode ser considerada aleatória.

Experimentos

Para testar a hipótese inicial, foram utilizados diversos sistemas criptográficos pré-computacionais reconhecidamente não aleatórios, apresentados na seção 2, os quais, submetidos ao Teste de Frequência Monobit deveriam ter a hipótese de nulidade rejeitada.

Destaca-se que a primeira fase é composta de dez experimentos que analisa textos cifrados por algoritmos criptográficos pré-computacionais de diversos tamanhos (136≤i≤408) que deveriam ser reprovados, porém não foram.

A segunda fase, por outro lado, é composta de quatro experimentos, que analisam textos cifrados por cifras de quatro categorias distintas, com n=1040. Essa fase demonstra que sequencias maiores que 1024, produzidas por cifras pré-computacionais são reprovadas no teste de frequência Monobit, como esperado.

Primeira Fase

No primeiro experimento, foi cifrada a mensagem "Isso também passará" [Chico Xavier] através da cifra Bastão de Licurgo (TKOTZ, 2011a), o diâmetro escolhido do bastão foi 4cm. A tabela 1 apresenta a mensagem criptografada submetida ao teste Monobit.

Bastão de Licurgo						
Mensagem criptografada:		Itesasamssmpaobar				
n	S_n	S_{obs}		P-value		
136	4	0.34299717028501764		1.255293651169706		
Bastão de Licurgo						
α	0,001	0,01	0,02	0,03	0,04	0,05
Aleatório	SIM	SIM	SIM	SIM	SIM	SIM

Tabela 1: Mensagem cifrada com Bastão de Licurgo submetida ao Teste Monobit

No segundo experimento, foi cifrada a mensagem "Isso também passará" [Chico Xavier] através da cifra de Della Porta (TKOTZ, 2011b), utilizando a chave criptografia. A tabela 2 apresenta a mensagem criptografada submetida ao teste de frequência Monobit.

Cifra de Della Porta						
Mensagem criptografada:	uajictwtrxgngawlr					
n	S_n	S_{0bs}			P-value	
136	12	1.028991510855053			0.29119244439286396	
Resultado do teste Monobit						
α	0,001	0,01	0,02	0,03	0,04	0,05
Aleatório	SIM	SIM	SIM	SIM	SIM	SIM

Tabela 2: Mensagem cifrada com a Cifra de Della Porta submetida ao Teste Monobit

O código de Políbio						
Mensagem criptografada:	113311431533414215					
n	S_n	S_{0bs}			P-value	
144	-22	1.8333333333333333			0.019080656429608878	
Resultado do teste Monobit						
α	0,001	0,01	0,02	0,03	0,04	0,05
Aleatório	SIM	NÃO	NÃO	NÃO	NÃO	NÃO

Tabela 3: Mensagem cifrada com a Cifra de Políbio submetida ao Teste Monobit

No terceiro experimento, foi cifrada a mensagem "Ama sempre" [Chico Xavier] através da cifra de Políbio (TKOTZ, 2011c). A tabela 3 apresenta a mensagem criptografada submetida ao teste de frequência Monobit.

No quarto experimento, foi cifrada a mensagem "Respeita os adversários" [Chico Xavier] através da Máquina Enigma (RIJMENANTS, 2004), utilizando a chave hdx. A tabela 4 apresenta a mensagem criptografada submetida ao teste de frequência Monobit.

Máquina Enigma						
Mensagem criptografada:	hmnxaoisrkvafqhcbwtge					
n	S_n	S_{0bs}			P-value	
168	10	0.7715167498104595			0.5504285047831592	
Resultado do teste Monobit						
α	0,001	0,01	0,02	0,03	0,04	0,05
Aleatório	SIM	SIM	SIM	SIM	SIM	SIM

Tabela 4: Mensagem cifrada com a Máquina Enigma submetida ao Teste Monobit

Cifra de Vigenère						
Mensagem criptografada:	pfztvzgdeiisufuqkoywaftub					
n	S_n	S_{0bs}			P-value	
200	20	1.414213562373095			0.09103473990095257	
Resultado do teste Monobit						
α	0,001	0,01	0,02	0,03	0,04	0,05
Aleatório	SIM	SIM	SIM	SIM	SIM	SIM

Tabela 5: Mensagem cifrada com a Cifra de Vigenère submetida ao Teste Monobit

No quinto experimento, foi cifrada a mensagem "Não reclame das sombras, faça luz" [Chico Xavier] através da cifra de Vigenère (TKOTZ, 2011d), utilizando a chave criptografia. A tabela 5 apresenta a mensagem criptografada submetida ao teste de frequência Monobit.

No sexto experimento, foi cifrada a mensagem "A desilusão é a visita da verdade" [Chico Xavier] através da cifra Rail Fence (TKOTZ, 2011e). A tabela 6 apresenta a mensagem criptografada submetida ao teste de frequência Monobit.

Rail Fence						
Mensagem criptografada:	dslsoaiiaaeddaeiuaevstdvrae					
n	S_n	S_{0bs}			P-value	
216	-4	0.2721655269759087			1.4006510507458318	
Resultado do teste Monobit						
α	0,001	0,01	0,02	0,03	0,04	0,05
Aleatório	SIM	SIM	SIM	SIM	SIM	SIM

Tabela 6: Mensagem cifrada com Rail Fence submetida ao Teste Monobit

No sétimo experimento, foi cifrada a mensagem “Mais fácil sofrer, difícil é perdoar” [Chico Xavier] através do disco de Alberti (TKOTZ, 2011f), utilizando deslocamento inicial igual a 2. A tabela 7 apresenta a mensagem criptografada submetida ao teste de frequência Monobit.

Disco de Alberti						
Mensagem criptografada:	ybnefbdnxetfkpkgnfndnxpopkgtbk					
n	S_n	S_{0bs}		P-value		
240	12	0.7745966692414834		0.5466044813760489		
Resultado do teste Monobit						
α	0,001	0,01	0,02	0,03	0,04	0,05
Aleatório	SIM	SIM	SIM	SIM	SIM	SIM

Tabela 7: Mensagem cifrada com Disco de Alberti submetida ao Teste Monobit

No oitavo experimento, foi cifrada a mensagem “Sonhos não morrem, apenas adormecem na alma” [Chico Xavier] através da cifra de Fleissner (TKOTZ, 2011g). A tabela 8 apresenta a mensagem criptografada submetida ao teste de frequência Monobit.

Grade giratória de Fleissner						
Mensagem criptografada:	csnoenammnhoasoraarsldnemomaaarpmoee					
n	S_n	S_{0bs}		P-value		
288	24	1.4142135623730951		0.09103473990095257		
Resultado do teste Monobit						
α	0,001	0,01	0,02	0,03	0,04	0,05
Aleatório	SIM	SIM	SIM	SIM	SIM	SIM

Tabela 8: Mensagem cifrada com a Grade de Fleissner submetida ao Teste Monobit

No nono experimento, foi cifrada a mensagem “A felicidade não entra em portas trancadas” [Chico Xavier] através da cifra ATBASH (TKOTZ, 2011h). A tabela 9 apresenta a mensagem criptografada submetida ao teste de frequência Monobit.

ATBASH						
Mensagem criptografada:	ZUVORXRWZWVMZLVMGIZVNKLIGZHGIZMXZWZH					
n	S_n	S_{0bs}		P-value		
288	-18	1.0606601717798214		0.26720627633602323		
Resultado do teste Monobit						
α	0,001	0,01	0,02	0,03	0,04	0,05
Aleatório	SIM	SIM	SIM	SIM	SIM	SIM

Tabela 9: Mensagem cifrada com ATBASH submetida ao Teste Monobit

No décimo experimento, foi cifrada a mensagem: “Não há problema que não possa ser solucionado pela paciência” [Chico Xavier] através da cifra de César (TKOTZ, 2011i). A tabela 10 apresenta a mensagem criptografada submetida ao teste de frequência Monobit.

Cifra de César						
Mensagem criptografada:	qdrkdsureohpdtxhqdrsrvvdvhuvroxflrqdgrshodsdflhqfld					
n	S_n	S_{0bs}		P-value		
408	6	0.2970442628930023		1.3488830527863944		
Resultado do teste Monobit						
α	0,001	0,01	0,02	0,03	0,04	0,05
Aleatório	SIM	SIM	SIM	SIM	SIM	SIM

Tabela 10: Mensagem cifrada com Cifra de César submetida ao Teste Monobit

Segunda Fase

Na segunda fase, foi utilizada uma única mensagem para os quatro experimentos. A mensagem em claro submetida aos algoritmos é: "Auxilia aos outros, tanto quanto puderes. Cada pessoa que hoje te encontra talvez seja amanhã a chave de que necessitas para a solução de numerosos problemas" [Chico Xavier].

O primeiro experimento cifrou a mensagem em claro com uma cifra de transposição. A cifra utilizada foi Rail Fence (TKOTZ, 2011e), utilizou-se como parâmetros de cifragem nível=2 e deslocamento=5. A tabela 11 apresenta a mensagem criptografada submetida ao teste de frequência Monobit.

CIFRA DE TRANSPOSIÇÃO (Rail Fence)						
Mensagem criptografada:	UIIASURSATQATPDRSAAESAUHJTECNRTLESJAAHAHVDQEEE STSAASLCOEUEOOPOLMSAXLAOOTOTNOUNOUEECDPSOQE OEENOTAAVZEAMNACAEEUNCSIAPRAOUADNMRSSRBEA					
n	S_n	S_{Obs}		P-value		
1040	-208	6.44980619863884		0.0		
Resultado do teste Monobit						
α	0,001	0,01	0,02	0,03	0,04	0,05
Aleatório	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO

Tabela 11: Mensagem gerada com uma cifra de transposição

O segundo experimento cifrou a mensagem em claro com uma cifra de substituição monoalfabética. A cifra utilizada foi a Cifra de César (TKOTZ, 2011i). A tabela 12 apresenta a mensagem criptografada submetida ao teste de frequência Monobit.

CIFRA DE SUBSTITUIÇÃO MONOALFABÉTICA (Cifra de César)						
Mensagem criptografada:	DXALOLDDRVRXWURVWDQWRTXDQWRSXGHUHVFDGDSHV VRDTXHKRMHWHHQFRQWUDWDOYHCVHMDDPDQKDDFKDY HGHTXHQHFHVVLWDVSDUDDVROXFDRGHQXPHURVRSUREOHPDV					
n	S_n	S_{Obs}		P-value		
1040	-230	7.131997238879487		0.0		
Resultado do teste Monobit						
α	0,001	0,01	0,02	0,03	0,04	0,05
Aleatório	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO

Tabela 12: Mensagem gerada com uma cifra de substituição monoalfabética

O terceiro experimento cifrou a mensagem em claro com uma Cifra de Substituição Polialfabética. A cifra utilizada foi o Disco de Alberti (TKOTZ, 2011f), com deslocamento ini-cial=2. A tabela 13 apresenta a mensagem criptografada submetida ao teste de frequência Monobit.

CIFRA DE SUBSTITUIÇÃO POLIALFABÉTICA (Disco de Alberti)						
Mensagem criptografada:	BLHNXNBBTETLRKTERBVRTSLBVRTOLGPKPEDBGBOPE ETBSLPHTNPRPPVDTVRKBRBXLPAEPNBBYBVHBBDHBL PGPSLPVPDPEENRBEOBKBBETXLDBTGPVLYPKTETEOKTMXPYBE					
n	S_n	S_{Obs}		P-value		
1040	-284	8.806466155833801		0.0		
Resultado do teste Monobit						
α	0,001	0,01	0,02	0,03	0,04	0,05
Aleatório	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO

Tabela 13: Mensagem gerada por uma cifra de substituição polialfabética

O quarto experimento cifrou a mensagem em claro com uma cifra eletromecânica. Foi utilizada a Máquina Enigma (RIJMENANTS, 2004), com a chave hdx. A tabela 14 apresenta a mensagem criptografada submetida ao teste de frequência Monobit.

CIFRA ELETROMECÂNICA (Máquina Enigma)						
Mensagem criptografada:	KKJVKOOSRKNKBKXCCCJYYYYORDRFMTMEAPORFHBTVFNDUPVNQM SGYKAMXZMJHAIIAIJIBRCSTOOXYZYMJFUAVUVVVHBKRNCLIKVNTKHQ HVJASKCRMIRCMYEJNSPRTAOQIU					
n	S_n	S_{Obs}		P-value		
1040	-166	5.147441485452151		6.978861932793734E-13		
Resultado do teste Monobit						
α	0,001	0,01	0,02	0,03	0,04	0,05
Aleatório	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO

Tabela 14: Mensagem gerada por uma cifra eletromecânica

Análise dos Resultados

A primeira fase dos experimentos utilizou dez algoritmos criptográficos reconhecidamente não aleatórios com mensagens de tamanho variados. Esperava-se que as mensagens fossem consideradas como não aleatórias. A mensagem criptografada com o Código de Políbio foi considerada aleatória somente para α=0.001. Todas as outras nove mensagens criptografadas foram consideradas aleatórias para α=0.005, conforme tabela 15.

Experimento		Cifra	Tipo	Data	n	Resultado
Fase 1	1	Bastão de Licurgo	Transposição	Séc. V a.C.	136	Aleatório
	2	Della Porta	Polialfabética	Séc. XVI	136	Aleatório
	3	Código de Políbio	Monoalfabética	Séc. II a.C.	144	Aleatório α=0.001
	4	Máquina Enigma	Eletromecânica	Séc. XX	168	Aleatório
	5	Cifra de Vigenère	Polialfabética	Séc. XVI	200	Aleatório
	6	Rail Fence	Transposição	Séc. XIX	216	Aleatório
	7	Disco de Alberti	Polialfabética	Séc. XV	240	Aleatório
	8	Grade de Fleissner	Transposição	Séc. XIX	288	Aleatório
	9	ATBASH	Monoalfabética	Séc. VII a.C.	288	Aleatório
	10	César	Monoalfabética	Séc. I a.C.	408	Aleatório
Fase 2	1	Rail Fence	Transposição	Séc. XIX	1040	Não-Aleatório
	2	César	Monoalfabética	Séc. I a.C	1040	Não-Aleatório
	3	Disco de Alberti	Polialfabética	Séc. XV	1040	Não-Aleatório
	4	Máquina Enigma	Eletromecânica	Séc. XX	1040	Não-Aleatório

Tabela 15: Resultados dos experimentos

Observou-se, na segunda fase dos experimentos, que com uma entrada de n=1040, produzida por um algoritmo legado, o teste de Frequência Monobit é eficaz, gerando o resultado esperado. Portanto, analisando os resultados, é recomendada a utilização de uma entrada maior ou igual a 1024 bits quando utilizado um nível de significância inferior a 0,05 para o Teste de Frequência Monobit.

CONCLUSÃO

Foi apresentado, neste artigo, um novo limite inferior para o tamanho de sequência de bits de entrada do Teste de Frequência Monobit do NIST Test Suite, quando aplicado à análise de algoritmos criptográficos. De fato, através de experimentos, com sistemas criptográficos pré-computacionais, comprovou-se que o Teste de Frequência Monobit não é adequado para um nível de significância de 0,04 a 0,001 e sequência de bits de entrada menor que 1024 bits.

O conhecimento dessa limitação implica numa maior acurácia na execução de teste de aleatoriedade sobre geradores de números pseudoaleatórios ou algoritmos criptográficos bem como na economia de tempo nas realizações dos outros quatorze testes subsequentes, que também possuem como pré-requisito o Teste de Frequência Monobit.

O desconhecimento desta limitação pode aprovar GNPA frágeis, acarretando pro-blemas no sistema criptográfico, pois a função primordial de um GNPA é auxiliar o sistema criptográfico na geração de criptogramas com uma distribuição que não estabeleça correla-ção com os dados de entrada, evitando a existência de padrões nos criptogramas e aumen-tando o tempo computacional utilizado em um ataque do tipo ciphertext-only.

Como trabalhos futuros, novos experimentos deverão ser realizados a fim de identifi-car limitações adicionais no NIST Test Suite, assim como submeter outros conjuntos de tes-tes de aleatoriedade (i.e DIEHARD) a uma análise detalhada ao uso adequado em sistemas criptográficos.

Referências bibliográficas

BEZERRA, D. DE J.; MALAGUTTI, P. L.; RODRIGUES, V. C. DA S. **Aprendendo Criptologia de Forma Divertida**. . [S.l: s.n.]. Disponível em: <http://www.mat.ufpb.br/bienalsbm/arquivos/Oficinas_Completos/O1Completo.pdf>. Acesso em: 20 jul. 2011. , 2010

DIAS, J. L. Desenvolvimento Histórico da Criptografia. **Cesubra Scientia**, v. 3, n. 3, p. 749-761, 2006.

FALEIROS, A. C. **Criptografia**. São Carlos - SP: SBMAC, 2011. v. 52

HAMANO, K.; KANEKO, T. Correction of Overlapping Template Matching Test Included in NIST Randomness Test Suite. **IEICE Trans. Fundam. Electron. Commun. Comput. Sci.**, v. E90-A, n. 9, p. 1788–1792, set 2007.

KIM, S.; UMENO, K.; HASEGAWA, A. **Corrections of the NIST Statistical Test Suite for Randomness**. . [S.l: s.n.]. , 2004

LAMBERT, J. A. **Cifrador simétrico de blocos: projeto e avaliação**. Rio de Janeiro: Insti-tuto Militar de Engenharia, 2004.

MUNDIM, M. J. **Estatística com BrOffice**. Rio de Janeiro: Ciência Moderna, 2010.

RIJMENANTS, D. **Enigma Simulator**. [S.l.]: Dirk Rijmenants 2004 - 2011, 2004.

RUKHIN, A.; SOTO, J.; NECHVATAL, J. et al. **A statistical test suite for random and pseudorandom number generators for cryptographic applications**. . [S.l.]: NIST - Special Publication 800-22. Disponível em: <http://goo.gl/rnv5v>. Acesso em: 12 ago. 2011. , abr 2010

SILVA, P. A. L. DA. **Probabilidades & Estatística**. Rio de Janeiro: Reichmann & Affonso, 1999.

SOTO, J. **Randomness Testing of the Advanced Encryption Standard Candidate Algo-rithms**. NIST IR - 6390. **Anais**... [S.l.]: National Institute of Standards and Technology. Disponível em: <http://www.nist.gov/customcf/get_pdf.cfm?pub_id=151193>. , 1999

SOTO, J.; BASSHAM, L. **Randomness Testing of the Advanced Encryption Standard Finalist Candidates**. NIST IR - 6483. **Anais**... [S.l.]: National Institute of Standards and Technology. Disponível em: <http://www.nist.gov/customcf/get_pdf.cfm?pub_id=151216>. Acesso em: 21 jul. 2011. , 2000

TANENBAUM, A. **Redes de Computadores**. 4. ed. Rio de Janeiro: Elsevier, 2003.

TKOTZ, V. **Criptografia - Segredos Embalados para Viagem**. [S.l.]: Novatec, 2005.

TKOTZ, V. **O Bastão de Licurgo**. Disponível em: <http://www.numaboa.com.br/criptografia/cifras/transposicoes/322-bastao-de-licurgo>. Acesso em: 29 set. 2011a.

TKOTZ, V. **A cifra de Della Porta**. Disponível em: <http://www.numaboa.com.br/criptografia/cifras/substituicoes/polialfabeticas/345-della-porta>. Acesso em: 29 set. 2011b.

TKOTZ, V. **O Código de Políbio**. Disponível em: <http://www.numaboa.com.br/criptografia/cifras/substituicoes/monoalfabeticas/tomograficas/179-Polibio>. Acesso em: 29 set. 2011c.

TKOTZ, V. **A cifra de Vigenère**. Disponível em: <http://www.numaboa.com.br/criptografia/cifras/substituicoes/polialfabeticas/506-vigenere>. Acesso em: 29 set. 2011d.

TKOTZ, V. **Rail Fence**. Disponível em: <http://www.numaboa.com.br/criptografia/cifras/transposicoes/417-rail-fence>. Acesso em: 29 set. 2011e.

TKOTZ, V. **O Disco de Alberti**. Disponível em: <http://www.numaboa.com.br/criptografia/cifras/substituicoes/polialfabeticas/164-alberti>. Acesso em: 29 set. 2011f.

TKOTZ, V. **A grade giratória de Fleissner**. Disponível em: <http://www.numaboa.com.br/criptografia/cifras/transposicoes/418-grade-giratoria?showall=1&limitstart=>. Acesso em: 29 set. 2011g.

TKOTZ, V. **As cifras hebraicas (Atbash)**. Disponível em: <http://www.numaboa.com.br/criptografia/cifras/substituicoes/monoalfabeticas/simples/168-atbash>. Acesso em: 29 set. 2011h.

TKOTZ, V. **O Código de César**. Disponível em: <http://www.numaboa.com.br/criptografia/124-substituicao-simples/165-codigo-de-cesar>. Acesso em: 23 abr. 2011i.

Dados dos autores

Carlos Eduardo Pantoja - email.: msc.pantoja@gmail.com. Professor na área de Informática Industrial e Administração Industrial do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca.

Nilson Mori Lazarin - Mestrado em Sistemas e Computação pelo Instituto Militar de Engenharia, Brasil(2012). Professor de Carreira do Magistério EBTT do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca.

Paulo Afonso Lopes da Silva - Doutorado em Operations Research pelo Florida Institute Of Technology, Estados Unidos(1989) Professor Adjunto do Instituto Militar de Engenharia , Brasil