Classificador binário para 3DES utilizando técnicas de Recuperação de Informação

Leandro M Ferreira, José Antonio M Xexéo*
IInstituto Militar de Engenharia (IME) –
Praça General Tibúrcio, 80, 22290-270, Praia Vermelha,
Rio de Janeiro, RJ, Brasil
**leandroferreira@ime.eb.br*

RESUMO: *Este artigo descreve a criação de um classificador binário para criptogramas que distingue entre as classes "3DES" ou "não 3DES" usando técnicas de Recuperação de Informação. O criptograma é dividido em "palavras" de 8 bits e, através do cálculo de similaridade com documentos pré-processados, é previsto se o criptograma foi gerado pelo Triplo DES (3DES), em modo ECB, em cifras de pelo menos 100KB de tamanho. Essa classificação é possível devido à existência de pequenas diferenças de similaridades apresentadas por documentos gerados pelo 3DES quando comparados com alguns dos finalistas do concurso do AES: Rijndael (AES), Serpent, Twofish e RC6 (utilizando chaves de mesmo tamanho). Esse classificador pode ser utilizado como um primeiro passo para a criptoanálise: identificação do algoritmo que gerou uma dada cifra.*

PALAVRAS-CHAVE: *Classificação binária. Recuperação de Informação. Triplo DES.*

ABSTRACT: *This paper describes the creation of a binary classifier for cryptograms that distinguishes between the classes "3DES" or "not 3DES" using Information Recovery techniques. The cryptogram is divided into 8 bit "words" and, by calculating the similarity to preprocessed documents, it is predicted which cryptograms have been generated by Triple DES (3DES), in ECB mode, for ciphers of at least 100 KB in size. This classification is possible due to the existence of small differences in similarities shown by documents ciphered using 3DES when compared against some of the AES contest finalists: Rijndael (AES), Serpent, Twofish and RC6 (using same size keys). This classifier can be used as a first step in cryptanalysis: identification of the algorithm that generated a given cipher.*

KEYWORDS: *Binary classification. Information Retrieval. Triple DES.*

1. Introdução

A criptografia busca tornar uma mensagem legível (chamada de texto em claro) em uma mensagem ilegível (chamada criptograma ou cifra) que apenas o destinatário da mensagem possa tornar novamente legível. Para consegui-lo utiliza-se um algoritmo criptográfico e uma chave. A dificuldade de um atacante em descobrir a mensagem através do criptograma se dá pelo fato de esse não conhecer a chave, ao contrário do destinatário, que a possui.

Através da história, diversos algoritmos para obter tal resultado foram desenvolvidos, desde a mais simples cifra de substituição monoalfabética (conhecida como Cifra de César) até os modernos sistemas computacionais como o "Advanced Encryption Standard" (AES). Após o surgimento de computadores capazes de testar por força bruta um grande número de chaves em pouco tempo, a criptografia passou a utilizar-se de algoritmos que criam problemas de difícil solução computacional sem a chave correta, mas de fácil solução caso se possua a chave.

Segundo [1], a presença de redundância no texto em claro é propagada pelo processo de cifragem, de tal modo que os padrões do texto se propagam para os criptogramas. Esses padrões todavia encontram-se ocultos como resultado da confusão e difusão presentes no processo de cifragem. A presença destes padrões permite o agrupamento segundo os pares (algoritmo, chave) utilizando-se o cálculo de similaridade como proposto por [2]. A classificação de uma cifra desconhecida segundo apenas o algoritmo que a originou é um problema mais complexo, pois esse método necessitaria de um esforço computacional similar ao de testar por força bruta todas as chaves possíveis, e um dicionário contendo exemplos de cifras geradas por cada chave possível.

A técnica de Recuperação de Informação (RI) que permite o agrupamento pelo par (algoritmo, chave) é o cálculo de similaridade entre documentos cujas palavras são os blocos de cifragem (64 bits por exemplo). Utilizando a divisão da "palavra" em tamanhos menores do que o bloco de cifragem (como 32, 16 ou 8 bits), foi possível obter-se um classificador binário capaz de separar os criptogramas desconhecidos gerados em modo ECB ("Electronic CodeBook") em duas classes: "3DES" contendo as cifras geradas pelo algoritmo "Triple Data Encryption Standard" (3DES) ou "não 3DES" contendo as cifras geradas por alguns dos algoritmos finalistas do concurso para o "Advanced Encryption Standard" (AES). - Rijndael ou AES, Serpent, Twofish ou RC6. Essa classificação é feita apenas considerando-se o algoritmo, e não o par (algoritmo, chave). O algoritmo MARS, o outro finalista do concurso, não foi elencado por restrições de escopo dos experimentos realizados.

2. Motivação

A criptoanálise busca recuperar a mensagem original através de falhas no algoritmo de cifragem ou descobrindo a chave correta. Segundo os princípios descritos em [3], a segurança do sistema deve ser baseada no desconhecimento da chave e não na ignorância sobre o processo de cifragem. Dessa forma, é geralmente assumido que o atacante conhece tudo sobre o processo de cifragem, suas peculiaridades e vulnerabilidades. Todavia em uma situação real, para que o atacante seja capaz de explorar essas deficiências, se faz necessário descobrir qual algoritmo foi utilizado para realizar a cifragem. Assim, um processo de classificação de ci-

fras desconhecidas pode ser o primeiro passo no processo de criptoanálise caso essa informação não possa ser obtida por outros meios.

Este artigo propõe um classificador binário que identifica cifras geradas pelo algoritmo 3DES, que é como um primeiro passo em direção a criar um classificador ***capaz de identificar as cifras de acordo com o algoritmo de cifragem e possivelmente também pelo modo de operação.***

3. Trabalhos relacionados

Estudos anteriores como [2, 4 e 5] conseguiram agrupar criptogramas baseados nos pares (algoritmo, chave) usados para criá-los. Em uma situação real, a hipótese de apenas uma chave ser utilizada é restritiva. Com a presença de múltiplos algoritmos e múltiplas chaves o problema se torna mais complexo e relevante para uso em ambientes práticos.

Deste modo um classificador binário, que distingue entre cifras geradas pelo algoritmo 3DES ou por alguns dos finalistas do AES independente de chave utilizada, traz um passo importante para se obter um classificador de múltiplas classes entre os diversos algoritmos.

Em outro trabalho, [6] realizou uma análise do uso de técnicas de Recuperação de Informação para agrupar cifras de acordo com o algoritmo de cifragem. [7] e mais recentemente [8] buscaram identificar os algoritmos e métodos de cifragem que geraram determinada cifra utilizando-se de "Support Vector Machines" (SVM) e conseguiram resultados com acurácia superiores a 80% quando as chaves utilizadas nas bases de treino e teste eram as mesmas.

4. Descrição do problema

Diferentes textos (que contêm redundância), quando cifrados por um mesmo algoritmo e chave usando o modo ECB, fazem padrões emergirem nos criptogramas resultantes. Através da semelhança entre estes criptogramas (ou seja a repetição de padrões entre eles) pode-se então agrupá-los segundo os algoritmos que os geraram. O objetivo do algoritmo de agrupamento de criptogramas é: dado um conjunto de criptogramas como entrada, separar tais criptogramas em diferentes grupos, onde cada grupo conterá os elementos cifrados por determinado algoritmo. O esquema do problema de agrupamento está apresentado na Figura 1. Por exemplo, caso o conjunto de entrada seja composto dos seguintes elementos:

{C1(T1, AES, k1), C2(T2, AES, k1), C3(T2,3DES, k2), C4(T3, 3DES, k3), C5(T1, RSA, k3), C6(T2, RSA, k4), C7(T1, Serpent, k1),C8(T3, Serpent, k5) }

Onde C1(T1, AES, k1) representa uma cifra C1 gerada usando-se AES e chave k1 sobre o texto T1. Os 4 grupos que devem ser encontrados estão dispostos na Tabela 1

Tab 1: Exemplo de agrupamento de cifras.

Grupo 1	Grupo 2	Grupo 3	Grupo 4
C1(T1, AES, k1)	C3(T2, 3DES, k2)	C5(T1, RSA, k3)	C7(T1, Serpent, k1)
C2(T2, AES, k1)	C4(T3, 3DES, k3)	C6(T2, RSA, k4)	C8(T3, Serpent, k5)

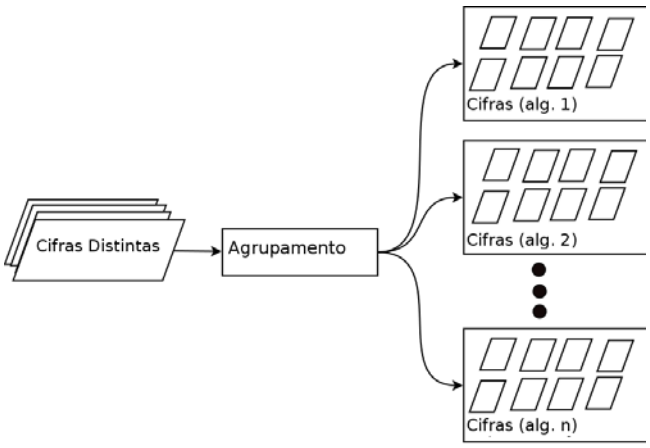


Fig.1 **–** Caracterização do problema de agrupamento.

A segunda parte do problema é realizar a classificação. Neste problema a entrada é um criptograma cujo método de cifragem é desconhecido. Através de uma base de treino composta por um conjunto de textos cifrados por diferentes algoritmos, o criptograma é classificado dentro de alguma das classes. Um classificador binário apenas distingue a cifra entre duas possíveis classes, já um classificador múltiplo faz a classificação dos criptogramas entre vários algoritmos distintos.

No caso específico do classificador binário apresentado neste trabalho existem duas classificações possíveis: Classe «3DES» ou "não 3DES". A eficácia do classificador será avaliada utilizando-se as medidas de precisão, abrangência e acurácia.

5. Descrição da base de dados de treinamento

A base de dados utilizada foi criada a partir da base Reuters-21578, Distribuição 1.0 (disponível em: http://www.daviddlewis.com/resources/testcollections/reuters21578) composta de 22 arquivos de documentos contendo textos de notícias em inglês. Cada um dos documentos tem tamanho próximo a 1,4 MB, gerando uma base de textos em claro de 30MB. Esta escolha se baseou na facilidade de obtenção, tamanho e quantidade de uso em pesquisa científica. O tamanho dos arquivos gera bastante repetição, permitindo a classificação. Entretanto testes foram realizados com cifras de tamanhos menores, geradas a partir do truncamento dos textos originais em tamanhos menores. A análise do impacto da redução do tamanho das cifras apresentadas ao algoritmo é realizada na seção 7.

Foram então gerados conjuntos de 5 chaves distintas, um conjunto para cada algoritmo de cifragem elencado nos experimentos (AES, Serpent, Twofish, RC6 e 3DES). Assim foram nomeadas as chaves AES1 ate AES5, Serpent1 ate Serpent5 e assim por diante. Todas essas chaves foram geradas aleatoria e independentemente, além de possuírem tamanho de 128 bits.

Posteriormente, cada algoritmo citado anteriormente foi executado sobre cada arquivo de texto em claro, em modo ECB, uma vez com cada chave distinta pertencente ao próprio algoritmo gerando 660 arquivos cifrados. Além disso, para fins de testes com mesmas chaves, as 5 chaves do AES (AES1 ate AES5) foram elencadas como chaves globais (que também seriam empregadas nos outros algoritmos para uso quando se quisesse testar com diferentes algoritmos e mesma chave). E os demais algoritmos de cifragem foram exe-

cutados com essas chaves sobre todos os arquivos gerando mais 440 arquivos cifrados. Este esquema está apresentado na Figura 2.

Ao final do processo a base de dados consiste de 990 arquivos de aproximadamente 1,4MB cada. Destes arquivos 110 foram cifrados pelo algoritmo AES, 220 pelo algoritmo Serpent (110 com chaves Serpent1 a Serpent5 e 110 com chaves AES1 a AES5), 220 pelo algoritmo Twofish (110 com chaves Twofish1 a Twofish5 e 110 com chaves AES1 a AES5), 220 pelo algoritmo RC6 (110 com chaves RC6_1 a RC6_5 e 110 com chaves AES1 a AES5) e 220 com o algoritmo 3DES (110 com chaves 3DES1 a 3DES5 e 110 com chaves AES1 a AES5).

6. Descrição da solução proposta

6.1 Técnicas de Recuperação de Informação

A linguagem natural em qualquer idioma apresenta redundância. Essa característica, explicada por [9] faz com que padrões emerjam nos textos escritos. As cifras de bloco atuais separam um texto em claro em blocos de tamanho iguais para cifragem e possuem alguns modos de operação. O modo de operação ECB preserva esses padrões, pois cada bloco cifrado depende apenas do bloco de entrada e da chave. Ou seja, blocos em claro iguais, cifrados com a mesma chave, geram blocos cifrados iguais.

Para realizar o processo de separação, o algoritmo utiliza um modelo vetorial para textos calculando em sequência a matriz de similaridade entre os textos cifrados. Trabalhando com cifras em bloco, o dicionário de palavras possíveis na verdade são sequências binárias do tamanho do bloco. Isso faz com que existam 2^m possíveis palavras, onde m é o número de bits de um bloco. Assim, se a matriz de similaridade apresentar um número não nulo entre dois criptogramas quaisquer já é grande a chance de terem sido cifrados por um mesmo par (algoritmo, chave). A Tabela 2 mostra um exemplo de matriz de similaridade e a Figura 3 mostra o esquema do cálculo da matriz de similaridade.

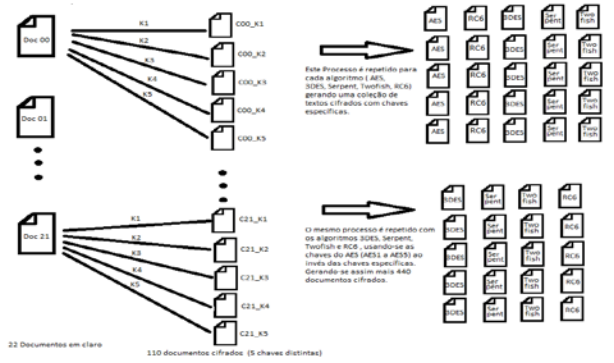
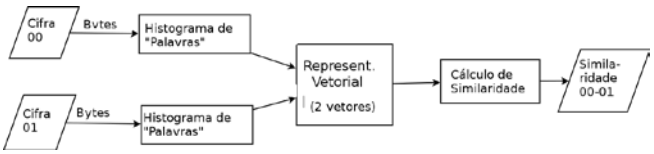


Fig.2 – Criação da base de dados.

Tabela 2: Exemplo de matriz de similaridade.

	Doc 1	Doc 2	Doc 3	Doc 4
Doc 1	**1**	**0,183**	**0**	**0,350**
Doc 2	**0,183**	**1**	**0**	**0,400**
Doc 3	**0**	**0**	**1**	**0**
Doc 4	**0,350**	**0,400**	**0**	**1**



1.

Fig.3 – Cálculo da Matriz de Similaridade.

Tab 3: Valor médio de similaridade por tamanho de palavra considerado.

Tam. palavra	Mesmos (algoritmo, chave)	(algoritmo, chave) distintos	3DES X não 3DES
64 bits	0,88	0	0
32 bits	0,91	3,5x10-6	1,25x10-6
16 bits	0,95	0,43	0,28
8 bits	0,9997	0,9975	0,9950

6.2 Considerando a divisão do bloco de cifragem como palavra

Ao considerar-se as palavras com tamanhos divisores do bloco de 64 bits (32, 16 e 8 bits), notou-se que as cifras geradas por conjuntos distintos de (algoritmo, chave) apresentavam similaridades diferentes de zero embora ainda muito inferiores à similaridade entre pares gerados pelo mesmo par (algoritmo, chave). Além disso, foi possível perceber que a similaridade entre documentos cifrados por um dos finalistas do concurso AES testados e documentos cifrados por 3DES apresentava valores relativamente menores, o que possibilitou a criação do classificador apresentado neste trabalho.

A Tabela 3 demonstra as similaridades médias encontradas entre cifras que foram criadas pelo mesmo par (algoritmo, chave), entre cifras que foram geradas por pares (algoritmo, chave) distintos mas com ambos os algoritmos pertencentes ao grupo de cifras não geradas por 3DES e, por fim, entre uma cifra gerada por 3DES e outra gerada por um algoritmo diferente do 3DES.

A partir da percepção de comportamento distinto das cifras geradas pelo 3DES, quando comparadas com cifras da base geradas pelos finalistas do AES testados, criou-se o classificador binário entre as classes "3DES" e "não 3DES". O motivo dessa aparente diferença de comportamento para cifras geradas pelos algoritmos 3DES ainda está sob estudo e as hipóteses levantadas são: menor tamanho efetivo da chave (112 bits para 3DES) em relação aos 128 bits dos demais algoritmos, possível menor proximidade de sequência aleatória nas cifras geradas pelo esquema de cifragem utilizado pelo 3DES ou diferenças entre as funções intrínsecas de cada algoritmo.

6.3 Classificador binário proposto

O classificador consiste em duas etapas. Na fase de treino são calculados os histogramas de todos os documentos considerando-se um tamanho de palavra escolhido. O modelo recebe estes histogramas para que na fase de teste seja possível calcularem-se as similaridades entre os documentos da base e a cifra a ser classificada.

Na fase de teste, o classificador recebe uma cifra sem a classe identificada, calcula a similaridade com os documentos da base e aplica sobre estes dados o algoritmo de classificação. No caso da presença de classe verdadeira disponível, é então verificada a correta classificação ou não desta cifra de

teste. O esquema do classificador está representado na Figura 4.

Na tentativa de se obter um classificador mais preciso e capaz de classificar textos cifrados de tamanhos menores, optou-se pela criação de um modelo de classificação próprio levando-se em conta a diferença de similaridade entre o texto a ser classificado com relação a documentos cifrados por algoritmos diferentes do 3DES e com relação a documentos cifrados pelo 3DES.

O processo incia-se com a separação do texto cifrado em blocos de 8 bits, e a contagem de cada ocorrência destas 256 "palavras" possíveis, gerando um histograma. Para poder classificar documentos de tamanhos distintos, este histograma é normalizado multiplicando-se pela relação de tamanhos entre o documento da base de dados e o documento a ser classificado. O histograma normalizado é então comparado com o histograma similar pré-calculado para cada documento da base de testes.

Procede-se então o cálculo de similaridade (distância cosseno) entre os dois documentos. Munido da similaridade do documento a ser classificado com cada um dos documentos da base, calcula-se a média de similaridade entre a cifra e os documentos não 3DES da base de treino e entre a cifra e os documentos gerados pelo 3DES da base de treino. O resultado dessas médias é comparado com os limiares de classificação. Após sucessivas iterações, chegou-se à conclusão que os limiares que separavam as duas classificações (3DES ou não 3DES) diminuíam com o tamanho do texto a ser classificado. Esse efeito é mostrado na Figura 5, e em escala logarítmica na Figura 6, para mais fácil visualização.

Para solucionar tal problema, o limiar de classificação é ajustado por uma interpolação entre os valores de limiar medidos mais próximos (superior e inferior ao tamanho de arquivo em questão), conforme mostrado na Equação 1(L representa limiar de classificação e T é tamanho do arquivo).

$$L_{aj} = \frac{(L_{alto} \times |T - T_{baixo}|) + (L_{baixo} \times |T - T_{alto}|)}{|T_{alto} - T_{baixo}|} \qquad (1)$$

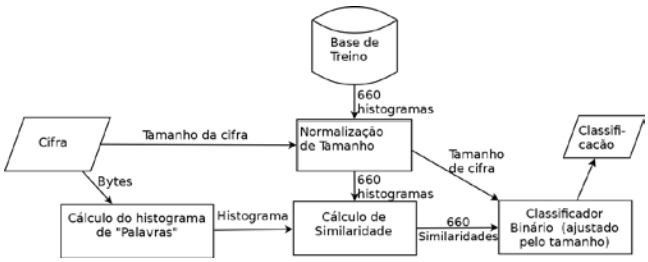


Fig.4 – Esquema do classificador binário.

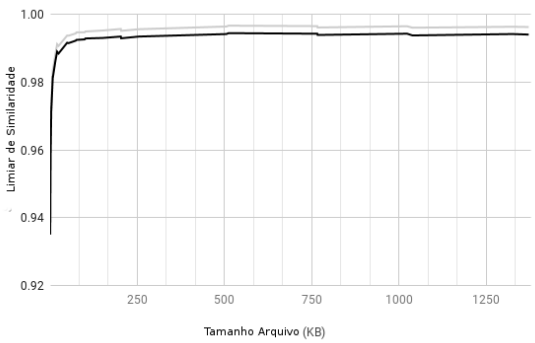


Fig.5 – Gráfico de ajuste do Limiar de classificação. A linha clara mostra comparação contra não 3DES, e a linha escura comparação com o 3DES.

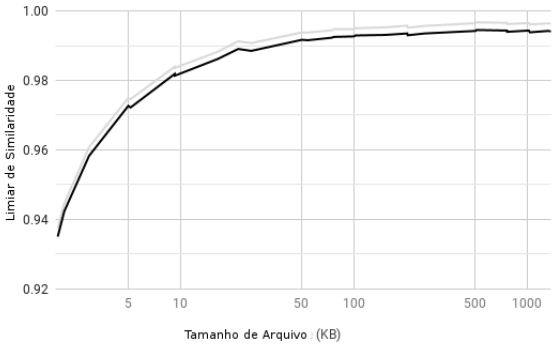


Fig.6 – Gráfico de ajuste do Limiar de classificação (Em escala log). A linha clara mostra comparação contra não 3DES, e a linha escura comparação com o 3DES.

7. Teste do classificador

O teste do classificador foi conduzido da seguinte maneira: Um dos 22 textos da base de treino foi escolhido e truncado para o tamanho desejado. Em seguida, o texto em claro resultante foi cifrado usando 4 algoritmos (AES, Serpent, Twofish e RC6) cada um com uma chave distinta, gerada pseudo aleatoriamente durante a execução do teste. De maneira similar foi feita a cifragem usando o 3DES, mas com duas chaves distintas. Estas 6 cifras eram então submetidas ao classificador. Esse processo foi repetido até que o número desejado de classificações fosse alcançado para cada tamanho de arquivo. (Foi escolhido o valor de 36 tentativas). O tamanho foi reduzido e o processo repetido. Os tamanhos escolhidos foram de 1.4MB, 1 MB, 500KB, 200KB, 100KB, 50KB, 25KB, 10KB (aproximadamente 1000 palavras de texto).

7.1 Resultados dos testes

Obteve-se acurácia de 100% com os tamanhos: 1.4MB, 1 MB, 500KB e 200KB. O resultado para 200KB foi de acurácia de 100%, com precisões e abrangências iguais a 1, conforme demonstra a Tabela 4. Todavia, conforme o tamanho de texto reduziu-se abaixo de 200KB, a acurácia reduziu-se como demonstram as Tabelas 5 a 8.

Tab 4: Resultado do classificador com textos de 200KB de tamanho.

Matriz de confusão	Real Não 3DES	Real 3DES	Precisão
Predito Não 3DES	24	0	1
Predito 3DES	0	12	1
Abrangência	1	1	
Acurácia	100%		

Tab 5: Resultado do classificador com textos de 100KB de tamanho.

Matriz de confusão	Real Não 3DES	Real 3DES	Precisão
Predito Não 3DES	24	1	0,96
Predito 3DES	0	11	1
Abrangência	1	0,9167	
Acurácia	97,22%		
Matriz de confusão	Real Não 3DES	Real 3DES	Precisão
Predito Não 3DES	24	1	0,96
Predito 3DES	0	11	1
Abrangência	1	0,9167	

Acurácia	97,22%		

Tab 6: Resultado do classificador próprio com textos de 50KB de tamanho.

Matriz de confusão	Real Não 3DES	Real 3DES	Precisão
Predito Não 3DES	22	1	0,9565
Predito 3DES	2	11	0,8461
Abrangência	0,9167	0,9167	
Acurácia	91,67%		

Tab 7: Resultado do classificador próprio com textos de 25KB de tamanho.

Matriz de confusão	Real Não 3DES	Real 3DES	Precisão
Predito Não 3DES	22	5	0,8148
Predito 3DES	2	7	0,7777
Abrangência	0,9167	0,5833	
Acurácia	80,56%		

Tab 8: Resultado do classificador próprio com textos de 10KB de tamanho.

Matriz de confusão	Real Não 3DES	Real 3DES	Precisão
Predito Não 3DES	14	0	1
Predito 3DES	10	12	0,5454
Abrangência	0,5833	1	
Acurácia	72,22%		

8. Conclusão

Mediante uso de técnicas de Recuperação de Informação sobre os criptogramas, foi possível, através da escolha de tamanhos de palavras divisoras do bloco de 64 bits (8 bits no caso específico em estudo), gerar um classificador binário para identificar os criptogramas gerados pelo algoritmo 3DES usando o modo de operação ECB.

Os testes comprovaram a viabilidade do classificador com o uso de uma base de treino de 550 cifras geradas a partir de 22 documentos de texto, usando-se 5 algoritmos distintos e 5 chaves específicas por algoritmo. Foi possível obter classificação 100% correta para documentos incluindo uma base de testes com cifras geradas por chaves pseudoaleatórias de no mínimo 200KB. A acurácia reduziu para 97,22% quando tratando cifras desconhecidas de tamanho 100KB. A acurácia para cifras de tamanhos menores foi menor embora ainda acima do valor de escolha aleatória. A redução da acurácia coincide com o brusco decréscimo no valor de limiar, mostrado anteriormente nas Figuras 5 e 6.

8.1 Trabalhos futuros

Considerando os resultados obtidos neste trabalho, evidencia-se a possibilidade de buscar, em trabalhos futuros, classificadores binários para outros algoritmos ou um possível classificador de múltiplos algoritmos. Além disso, pode-se verificar a possibilidade de classificar corretamente textos oriundos de outras linguagens ou até mesmo documentos cifrados a partir de documentos não textuais (como imagens, áudio ou vídeo).

As hipóteses que justifiquem a diferença de comportamento das cifras geradas pelo algoritmo 3DES em relação aos "não 3DES" podem ser testadas a fim de descobrir o motivo de tal diferença. Ainda como trabalho futuro, elenca-se a melhoria do classificador 3DES visando a classificar com maior acurácia os textos cifrados de tamanhos menores do que 100 KB.

Referências Bibliográfica

[1] C.E. Shannon, Communication Theory of Secrecy Systems, Bell Labs Technical Journal, vol. 28, 1948, pg 656.

[2] C. Oliveira, J.A.M. Xexéo, C.A.B. Carvalho, Clustering and categorization applied to cryptanalysis, Cryptologia, vol 30, 2006, pg. 26.

[3] A. Kerckhoffs, La Cryptographie Militaire, Journal des Sciences Militaires, vol IX, 1883, pgs 5-83,161-191.

[4] W.A.R. Souza, L.A.V. de Carvalho, J.A.M. Xexéo, Identification of n block ciphers, IEEE Latin America Transactions, vol. 9, 2011, pg. 184

[5] R.H. Torres, G.A. Oliveira, Identification of keys and cryptographic algorithms using genetic algorithm and graph theory, IEEE Latin America Transactions, vol 9, 2011, pg 178.

[6] S.Nagireddy, A pattern Recognition Approach to Block Cipher Identification, Dissertaçãio de mestrado, Indian Institute of Technology Madras, Madras, India, 2008.

[7] A.D. Dileep, C.C. Sekhar, Identification of block ciphers using support vector machines, Proc. International Joint conference on Neural Networks, 2006 Vancouver, BC, Canada, pg. 2696.

[8] C. Tan, Y Li, S. Yao, A novel identification Approach to Encryption Mode of Block cipher, Advances in Intelligent Systems Research, vol. 136, 2016, pg 586.

[9] Shannon, C.E. A Mathematical Theory of Communication, The Bell System Technical Journal, vol. 27, 1948, pgs 379-423,623-656.