Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 10, n. 1, 2023.

Trabalho apresentado no XLII CNMAC, Universidade Federal de Mato Grosso do Sul - Bonito - MS, 2023

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Análise da Confusão, Difusão e da Utilização do Modo de Operação CTR no Algoritmo Criptográfico AES

Mariana Teixeira[1], Ana Luísa Fernandes[2], Ivan Aldaya[3], Cintya Wink de Oliveira Benedito[4], Marcelo Luís Francisco Abbade[5]
Faculdade de Engenharia - Unesp, São João da Boa Vista, SP

Resumo. O objetivo deste trabalho é analisar a existência das propriedades de confusão e difusão no algoritmo de encriptação de cifra de bloco e chave simétrica AES (*Advanced Encryption Standard*) utilizando algoritmos implementados no Matlab®. As análises estatísticas quantitativas apresentadas foram feitas para dois comprimentos de chave diferentes: 128 e 256 bits, de modo a entender se uma chave maior possibilita melhora nas propriedades de confusão e difusão. Além disso, também foi implementado o modo de operação CTR (*Counter Mode*) para criptografar mensagens com mais de um bloco de 128 bits. Características deste modo de operação foram analisadas e análises estatísticas foram utilizadas para mostrar que a encriptação de mensagens semelhantes não geraram o mesmo texto cifrado. Especificamente, buscou-se mostrar a existência da aleatorização por meio de análises quantitativas.

Palavras-chave. Criptografia, AES, Confusão, Difusão, Modos de Operação.

1 Introdução

A segurança dos dados enviados e recebidos é tópico atual e amplamente discutido, já que a cada dia são mais utilizados meios tecnológicos para transmissão de dados confidenciais. O processo de segurança é baseado nos princípios da criptografia, que tem como propósito promover a confidencialidade, garantindo que somente remetente e destinatário da mensagem possam entendê-la. Os algoritmos criptográficos podem ser divididos em cifras assimétricas, que também são conhecidas como algoritmos de chave pública, e cifras simétricas, também conhecidas como algoritmos de chave privada. No primeiro caso, os usuários possuem uma chave pública para fazer o processo de encriptação e utilizam uma chave privada para desencriptar. O usuário que deseja transmitir a mensagem aplica nela o algoritmo de encriptação utilizando a chave pública do receptor, que utiliza sua chave privada para desencriptar e então obter a mensagem [3]. As cifras assimétricas têm como representante mais utilizado o algoritmo estabelecido por Rivest-Shamir-Adleman: RSA [4], que pode ser utilizado para que os usuários troquem entre si uma chave privada para ser utilizada nas cifras simétricas. As cifras simétricas utilizam uma mesma chave para o processo de encriptação e desencriptação. De forma simplificada, o usuário que deseja transmitir alguma informação aplica o algoritmo de encriptação simétrico à sua mensagem, utilizando uma chave k. Com esse procedimento, é possível obter um texto cifrado que é enviado até o receptor. Por sua vez, o receptor aplica o algoritmo simétrico para desencriptação utilizando a mesma chave do usuário transmissor, recuperando assim a mensagem. Nos casos em que as mensagens tenham um tamanho específico

[1]mt.cardoso@unesp.br
[2]luisa.souza@unesp.br
[3]ivan.aldaya@unesp.br
[4]cintya.benedito@unesp.br
[5]marcelo.abbade@unesp.br

quando são utilizadas cifras simétricas, o algoritmo utilizado é chamado cifra de bloco. A cifra de bloco mais utilizada atualmente foi desenvolvida por dois criptógrafos belgas: Joan Daemen e Vincent Rijmen. O AES (*Advanced Encryption Standard*) é uma cifra de bloco que utiliza mensagens de tamanho 128 bits e chaves variando entre 128, 192 e 256 bits [1]. O AES é utilizado em protocolos muito conhecidos, tais como o HTTPS (protocolo de transmissão de dados), o FTPS (uma extensão do protocolo FTP, que é um protocolo de transferência de arquivos) e também o SFTP (protocolo de transferência de arquivos), além do uso em serviços de VPN conhecidos. Uma outra aplicação do AES pode ser notada em um protocolo de comunicação amplamente utilizado na área de Internet das Coisas: o protocolo Zigbee.

Para algoritmos que utilizam cifras de bloco serem considerados seguros, eles devem oferecer as propriedades de confusão e difusão estabelecidas por [5]. A difusão é uma propriedade que exige que o algoritmo gere textos diferentes se uma mesma chave é utilizada para encriptar mensagens similares. Com isso, cada bit da mensagem de entrada deve afetar muitos bits da mensagem cifrada. Por exemplo, se duas mensagens possuem somente um bit diferente entre si e a mesma chave é usada para fazer a encriptação, então a difusão estabelece que os textos cifrados devem ser diferentes entre si em cerca de 50% dos bits. Já a confusão é a propriedade que exige relação "suficientemente complexa" entre a chave e o texto cifrado, de modo que a chave não possa ser deduzida por propriedades estatísticas. Por exemplo, ao enviar uma mesma mensagem duas vezes com chaves que diferem entre si somente por um bit, a confusão exige que os textos cifrados devem diferir entre si de aproximadamente 50% dos bits. Assim, é possível analisar a confusão e difusão por meio do conceito de efeito avalanche, ou seja, a modificação de um único bit (na mensagem ou na chave) acaba gerando modificação de diversos bits do texto cifrado. Existem também alguns casos em que deseja-se encriptar mensagens com tamanho diferente do bloco de 128 bits que deve entrar no AES, utilizando a mesma chave criptográfica. Nestes casos, a fim de garantir a confidencialidade ou a integridade da mensagem criptografada, faz-se necessário utilizar modos de operação [3]. Modos de operação são algoritmos que realizam a encriptação de dados maiores e em alguns casos promove autenticação, garantindo que a mensagem realmente veio do usuário transmissor. Uma característica importante dos modos de operação é que devem fornecer aleatorização, ou seja, se a mesma mensagem for criptografada duas vezes utilizando a mesma chave, o modo de operação deve garantir que os dois textos criptografados difiram entre si em cerca de 50% dos bits. Alguns exemplos de modos de operação são definidos em [2]. Neste trabalho iremos analisar o CTR (*Counter mode*), um modo de operação que permite a encriptação de maneira paralela, ou seja, vários blocos podem ser encriptados ao mesmo tempo, gerando melhora em sua performance computacional. O fato de os blocos serem independentes entre si também é uma vantagem do CTR, já que os erros não se propagam e se torna possível a análise de bits alterados em cada bloco. Além disso, o CTR é utilizado no GCM (*Galois Counter mode*), um modo de operação que garante a autenticação, e não somente encriptação das mensagens. Neste contexto, o objetivo central deste trabalho é apresentar análises estatísticas quantitativas para comprovar a existência de confusão e difusão no algoritmo AES, bem como na utilização do modo de operação CTR. Além desta contribuição, que apesar de simplificada não é de conhecimento dos autores a sua apresentação neste formato, os autores também realizaram toda a implementação computacional dos algoritmos utilizados. Análises estatísticas mais robustas baseadas em técnicas de inferência estatística poderiam ser utilizadas mas não foram o foco deste trabalho.

Este trabalho está estruturado da seguinte forma. Na Seção 2 apresentamos o AES, descrevendo brevemente as operações utilizadas neste algoritmo. Já na Seção 3 os conceitos de confusão e difusão foram apresentados assim como o modo de operação CTR de interesse deste trabalho. E por fim, na Seção 4 análises que comprovam que o AES possui as propriedades de confusão e difusão serão apresentadas, além de analisar a influência do tamanho da chave em tais propriedades. Além disso, apresentamos as análises realizadas sobre o uso do modo de operação CTR.

DOI: 10.5540/03.2023.010.01.0020

2 Algoritmo AES

O AES é um algoritmo de criptografia de cifra simétrica e de cifra de bloco que criptografa mensagens de 128 bits utilizando chaves variando entre 128 (AES-128), 192 (AES-192) e 256 (AES-256) bits. Para criptografar, o algoritmo executa 10 rodadas para uma chave de 128 bits, 12 rodadas para uma chave de 192 bits e 14 rodadas para uma chave de 256 bits, sendo que em cada rodada utiliza uma chave diferente e, em cada round, são realizados 4 estágios chamados: *AddRoundKey*, *SubBytes*, *ShiftRows* e *MixColumns*. Todas as operações realizadas para o AES estão contidas no Corpo de Galois $GF(2^8)$.

A Figura 1 representa um diagrama de blocos do funcionamento AES-128. Para este trabalho foi realizado o estudo de todas as etapas e operações do AES, assim como a implementação computacional de todas elas, porém não iremos apresentar com detalhes e sugerimos a referência [3]. Resumidamente, para a primeira rodada os 128 bits (16 bytes) de entrada, organizados em uma matriz 4×4, passam pela operação da função lógica XOR (*exclusive-or*) com uma chave inicial k_0 que também está organizada em uma matriz 4×4, este estágio é chamado *AddRoundKey*. Para as rodadas com as chaves $k_1, \ldots, k_9$, o resultado da primeira operação passará pelos estágios: *SubBytes*, *ShiftRows*, *MixColumns* e *AddRoundKey*. Na rodada final, com a chave k_{10}, a operação de *MixColumns* não é realizada. Especificamente no estágio *SubBytes*, uma tabela de substituição conhecida como S-box (*Substitution box*) é utilizada [3]. Nesse estágio, cada byte de entrada é substituído pelos bytes contidos na tabela. Essa substituição é responsável por introduzir confusão aos dados, assegurando que a mudança em cada um dos bits de entrada se propague rapidamente. O estágio *ShiftRows* consiste em deslocar o primeiro byte da segunda linha para a última posição, os dois primeiros bytes da terceira linha para as duas últimas posições e os três primeiros bytes da quarta linha para as três últimas posições, deslocando assim os demais bytes. Essa transformação é responsável por adicionar difusão, ou seja, cada bit de entrada deve afetar um número considerável de bits da mensagem criptografada. Adicionalmente, o estágio *MixColumns* consiste da aplicação de uma transformação linear na matriz vinda do estágio anterior. Nela, cada byte na entrada influencia quatro bytes na saída, o que torna esse estágio o maior responsável por adicionar difusão ao AES.

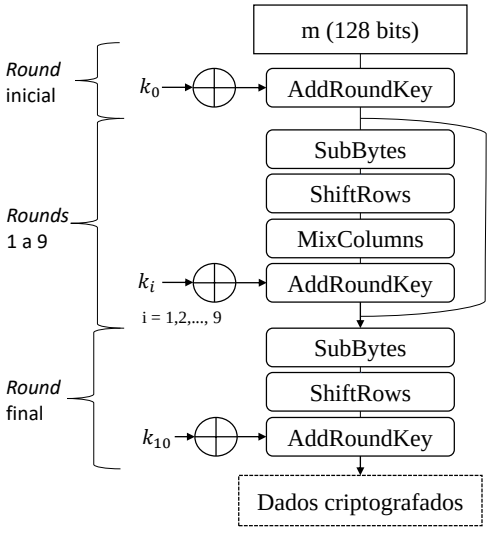


Figura 1: AES e seus estágios. Fonte: próprio autor.

Além de seu uso no *SubBytes*, a S-box também é aplicada no processo de expansão de chaves. Esse processo é responsável por gerar as chaves derivadas da chave inicial, que são utilizadas em cada rodada do AES. Para o AES-128, a expansão de chaves gera um total de 11 subchaves a serem utilizadas em 10 rodadas e para o AES-256 são geradas 15 subchaves a serem utilizadas em 14 rodadas.

O processo de decriptação é similar à encriptação, porém é realizado em ordem inversa. As subchaves utilizadas são as mesmas, no entanto a primeira subchave utilizada para a decriptação é a da décima etapa. Além disso, sabemos que na décima etapa do processo de encriptação não há o estágio *MixColumns*. Assim, para a primeira etapa da decriptação não será realizada a operação inversa do *MixColumns*. Como a decriptação é um processo inverso, a ordem dos estágios a ser realizada também será inversa: *AddRoundKey*, *MixColumns*, *ShiftRows* e *Subbytes*.

3 Confusão, Difusão e Modo de Operação CTR

Nesta seção iremos apresentar as análises realizadas para mostrar que os algoritmos implementados AES-128 e AES-256 apresentam as propriedades de confusão e difusão.

A confusão é uma operação de encriptação onde a relação entre a chave e o texto cifrado é complexa. Ela é dada quando a alteração de um bit da chave gera uma grande alteração dos bits do texto cifrado. Quando essa alteração de bits afeta cerca de metade dos bits do texto cifrado, temos o chamado efeito avalanche. Para comprovar a eficácia da confusão no AES e a existência do efeito avalanche, foi feito um código em Matlab® para ser adicionado ao algoritmo de encriptação do AES já implementado. Por meio dele, introduziu-se um texto de entrada de 128 bits, o qual foi utilizado como base para todas as operações. Em seguida, foi sorteada uma chave aleatória e aplicou-se o algoritmo de encriptação. O texto cifrado encontrado foi armazenado em uma matriz para posterior utilização. Um bit da chave foi alterado por vez e aplicou-se novamente no AES para a mesma mensagem. A comparação entre o texto cifrado inicial e os textos cifrados modificados por cada alteração na chave foram colocada em uma matriz. Nessa matriz, foi realizada uma comparação por meio de um XOR, ou seja, se ocorre variação do bit após a mudança na chave, essa variação é indicada por 1.

Para exemplificar, consideremos a seguinte matriz:

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & \text{NaN} \\ 0 & 1 & 1 & 1 & 3 \\ 1 & 0 & 1 & 1 & 3 \\ 1 & 1 & 0 & 1 & 3 \\ 1 & 1 & 1 & 0 & 3 \\ 3 & 3 & 3 & 3 & \text{NaN} \end{pmatrix}. \tag{1}$$

A primeira linha indica uma chave original aleatória com quatro bits. A segunda linha indica os bits do texto cifrado que são alterados quando o primeiro bit da chave é alterado. O número três na última coluna indica a soma de todos os bits do texto cifrado que são alterados com a mudança do primeiro bit da chave. Já a terceira linha indica os bits do texto cifrado alterados quando o segundo bit da chave é alterado. A última coluna dessa linha indica a soma de todos os bits do texto cifrado que foram alterados pela mudança do segundo bit da chave. As demais linhas (quatro e cinco) seguem o mesmo princípio. Por fim, para a linha seis, a primeira coluna mostra quantas vezes o primeiro bit do texto cifrado foi alterado, a segunda coluna mostra quantas vezes o segundo bit do texto cifrado foi alterado e assim por diante. Como é perceptível, a quantidade de bits do texto cifrado que foram alterados resulta em uma coluna quando é utilizada uma chave. Para um número n de chaves, o resultado seria de n colunas. As colunas são importantes para a análise dos dados, visto que mostram como a mudança de um único bit da chave influencia no

texto cifrado. Para complementar o código, também foi adicionada uma coluna com a média de bits alterados. A partir dela, foi possível criar um histograma e calcular a média geral dos bits.

A difusão é uma operação de encriptação onde a relação entre o texto de entrada e o texto cifrado é complexa. No AES, ela se dá quando a alteração de um único bit do texto de entrada gera alteração de cerca de metade dos bits do texto cifrado. Para comprovar a eficácia da difusão no AES, também foi feito um código em Matlab® para ser adicionado ao algoritmo de encriptação do AES já implementado, similar ao utilizado anteriormente para confusão. Neste caso, foram alterados todos os 128 bits de um texto de entrada aleatório.

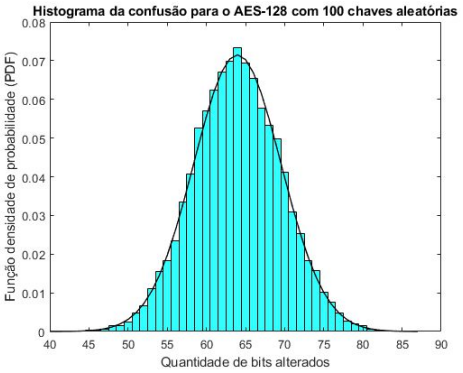
O AES, como já citado anteriormente, é uma cifra de bloco com tamanho fixo de 128 bits (16 bytes). No entanto, quando arquivos maiores que 128 bits precisam ser encriptados, é necessário quebrar os bits desse arquivo em blocos de 128 bits para que ele possa ser criptografado utilizando o AES e, para isso, os chamados modos de operação podem ser utilizados. O modo de operação CTR (*Counter Mode*) transforma cifras de bloco em cifras de fluxo, utilizando um vetor de inicialização IV (*Initiation Vector*) concatenado com um contador. Por exemplo, para o caso do AES cuja entrada deve ser 128 bits, poderíamos definir um IV aleatório com 64 bits e um contador também de 64 bits, ou até mesmo um IV com 96 bits e um contador com os 32 bits restantes. O contador deve ser escolhido de maneira a produzir uma sequência que não vai se repetir por um bom tempo. É importante ressaltar que o novo vetor formado pelo IV e o contador não necessitam ser secretos, visto que serão encriptados por uma chave que será secreta. Para implementar o CTR, definiu-se um IV que foi concatenado com o contador inicial. Esse vetor concatenado deve ser encriptado pelo AES utilizando a chave k. O vetor encriptado agora deve ser utilizado para fazer XOR com o texto de entrada, que deve ter o mesmo tamanho do vetor. O resultado desse XOR nos dará o primeiro texto cifrado.

4 Resultados

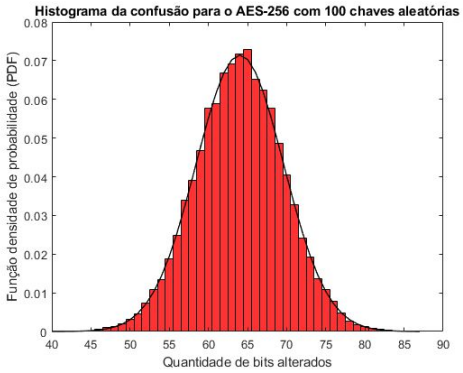
Nesta seção iremos apresentar as análises estatísticas obtidas através da implementação dos algoritmos descritos anteriormente. Para a obtenção de resultados satisfatórios, foram utilizadas 100 chaves para a confusão e 100 textos de entrada para a difusão. Para o AES-128, como cada chave ou texto de entrada possuem 128 bits, foram realizadas 12800 alterações de bit para a obtenção das médias e histogramas. Já para o AES-256, a confusão resultou em 25600 alterações de bits, já que cada chave utilizada possui 256 bits. E, para a difusão, a quantidade de bits alterados foi a mesma que para o AES-128. Importante notar que todos os histogramas obtidos foram normalizados de forma que o eixo y representasse a função densidade de probabilidade e não a frequência em que a quantidade de bits alterados ocorria.

Para a análise da confusão no AES-128, a Figura 2(a) indicou uma distribuição gaussiana com média μ de bits alterados, com a alteração de um único bit da chave, de 63.9585 bits e desvio padrão σ de 5.5793 bits. A média próxima de 64 bits era esperada e comprova a existência da confusão, ou seja, garante que com a alteração de um bit da chave, cerca de metade dos bits do texto cifrado são alterados, considerando que o texto cifrado tem 128 bits de saída. Já para a confusão no AES-256 os resultados apresentados na Figura 2(b) foram semelhantes, com a distribuição gaussiana com média μ de bits alterados de 64.0162 e desvio padrão σ de 5.5859. E, consequentemente com os dados no intervalo de 47.26 até 80.77 bits. Observa-se também que nem mesmo o intervalo dos dados se altera, o que mostra que o fato de a chave ser maior não faz com que mais bits sejam alterados no texto cifrado ao alterar um único bit da chave. Assim, a confusão é verificada da mesma forma para o AES-128 e para o AES-256.

DOI: 10.5540/03.2023.010.01.0020



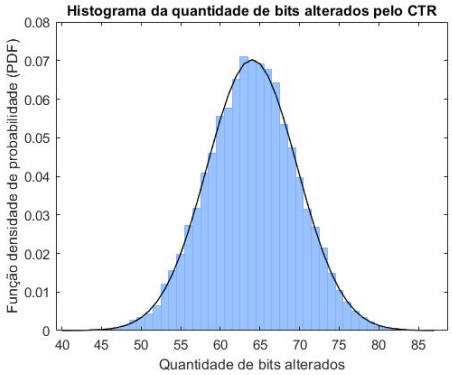
(a) Confusão AES-128



(b) Confusão AES-256

(c) Difusão AES-128

(d) Difusão AES-256



(e) Modo de Operação CTR

Figura 2: Análises Estatísticas. Fonte: próprio autor.

Para a difusão no AES-128, a Figura 2(c) indicou uma distribuição gaussiana, com dados no intervalo de 46.98 até 81.06 bits, a média de bits alterados com a alteração de um único bit do texto de entrada foi de 64.0240 bits e o desvio padrão foi de 5.6801 bits. De forma similar, para a difusão no AES-256, a Figura 2(d) mostra que também temos uma distribuição gaussiana, com dados no intervalo de 47.03 até 80.97 bits, a média de bits alterados foi de 64.0053 e o desvio

DOI: 10.5540/03.2023.010.01.0020

padrão foi de 5.6569. Em ambos os casos, a média encontrada comprova a presença da difusão, mostrando que a alteração de um único bit do texto de entrada gera alteração de metade dos bits do texto cifrado. Novamente, foi possível comprovar que a chave maior não gerou melhor resultado na análise. Assim, com difusão e confusão garantidas, é possível concluir que ocorre o efeito avalanche, já que a modificação de um único bit resulta em textos cifrados diferentes em mais de 50% dos bits.

Para comprovar a aleatorização de textos criptografados pelo CTR, foi implementado um algoritmo para teste e análises quantitativas: inicialmente um texto de entrada arbitrário foi aplicado, utilizando parâmetros fixos. Depois, todos os parâmetros foram mantidos, inclusive o texto de entrada, e um loop foi criado de modo a comparar o primeiro texto cifrado com o próximo, sendo que a cada iteração foi utilizado o contador incrementado. De maneira semelhante ao que foi feito para a confusão e difusão, calculou-se a média e fez-se o histograma para entender quantos bits são alterados utilizando um mesmo texto de entrada e incrementando o contador. Foram utilizados 20000 valores diferentes de contador, cada um deles sendo relacionado ao texto cifrado inicial. Ao aplicar o algoritmo para compreender a aleatorização do CTR, foi obtido o histograma da Figura 2(e). A média de bits alterados com a alteração do contador a cada rodada foi de 64.0091 bits e o desvio padrão foi de 5.6799 bits. Para a análise quantitativa do CTR, foi possível obter a distribuição gaussiana com dados no intervalo de 46.96 até 81.04 bits. Assim, conclui-se que ao utilizar um mesmo texto de entrada e mesma chave no CTR, são obtidos textos cifrados dissimilares em cerca de metade dos bits se é alterado somente um bit por vez do contador. Com isso, mostra-se a aleatorização dos textos criptografados por esse modo de operação. A escolha de análise do CTR foi também devido a sua utilização no GCM, garantindo a autenticação das mensagens, além da encriptação. A possibilidade da autenticação é interessante para o caso da criptografia na camada física e poderá ser foco de trabalhos futuros, nos quais podem ser utilizados os cabeçalhos das mensagens para fazer autenticação e também garantir que os instantes corretos de amostragem do sinal são identificados.

Agradecimentos

Agradecemos a Fapesp - Processo 2019/02720-7 e 2023/07667-2, ao Programa PIBIC/CNPq e a FINEP - Projeto 0527/18 pelo apoio financeiro para a realização deste trabalho.

Referências

[1] J. Daemen e V. Rijmen. **The design of Rijndael: AES - The Advanced Encryption Standard**. 2a. ed. New York: Springer-Verlag, 2002. ISBN: 978-3642076466.

[2] M. Dworkin. **Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication**. 2016. DOI: 10.6028/NIST.SP.800-38B.

[3] C. Paar e J. Pelzl. **Understanding Cryptography: A Textbook for Students and Practitioners**. 1a. ed. Londres: Springer, 2010. ISBN: 978-3-642-04100-6.

[4] R. L. Rivest, A. Shamir e L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems". Em: **Communications of the ACM** 21.2 (1978), pp. 120–126. DOI: 10.1145/359340.359342.

[5] C. E. Shannon. "Communication theory of secrecy systems". Em: **The Bell system technical journal** 28.4 (1949), pp. 656–715. DOI: 10.1002/j.1538-7305.1948.tb01338.x.

