BOLETIM DE PESQUISA E DESENVOLVIMENTO

43

ISSN 1677-9266
Março/2018

Protocolo para cifra de uso único via função NOT controlada

ISSN 1677-9266
Março/2018

Empresa Brasileira de Pesquisa Agropecuária
Embrapa Informática Agropecuária
Ministério da Agricultura, Pecuária e Abastecimento

BOLETIM DE PESQUISA E DESENVOLVIMENTO 43

Protocolo para cifra de uso único via função NOT controlada

Jacomo Giovanetti Minto Neto
Edgard Henrique dos Santos
Alexandre de Castro

Embrapa Informática Agropecuária
Campinas, SP
2018

Exemplares desta publicação podem ser adquiridos na:

Embrapa Informática Agropecuária
Av. Dr. André Tosello, 209 - Cidade Universitária,
Campinas - SP
Fone: (19) 3211-5700
www.embrapa.br/informatica-agropecuaria
www.embrapa.br/fale-conosco/sac

Supervisão editorial
Kleber X. Sampaio de Souza

Revisão de texto
Adriana Farah Gonzalez

Normalização bibliográfica
Maria Goretti G. Praxedes

Projeto gráfico da coleção
Carlos Eduardo Felice Barbeiro

Editoração eletrônica
Tuíra Santana Favarin, sob supervisão de Flávia Bussaglia Fiorini

Foto da capa
Vecteez (https://pt.vecteezy.com/)

1ª edição on-line - 2018

Dados Internacionais de Catalogação na Publicação (CIP)
Embrapa Informática Agropecuária

Minto Neto, Jacomo Giovanetti.
Protocolo para cifra de uso único via função NOT controlada / Jacomo Giovanetti Minto Neto, Edgard Henrique dos Santos, Alexandre de Castro.- Campinas : Embrapa Informática Agropecuária, 2018.
21 p. il.: cm. - (Boletim de pesquisa e desenvolvimento / Embrapa Informática Agropecuária, ISSN 1677-9266; 43).
1. Criptografia. 2. Segurança de dados. 3. Criptografia simétrica. 4. Porta Cnot. I. Santos, Edgar Henrique dos. II. Castro, Alexandre de. III. Embrapa Informática Informática Agropecuária. IV. Título. V. Série.

CDD 005.8

Sumário

Protocolo para cifra de uso único via função NOT controlada

Jacomo Giovanetti Minto Neto[1]
Edgard Henrique dos Santos[2]
Alexandre de Castro[3]

Resumo – Criptografia é uma técnica de proteção da informação que consiste em codificar o conteúdo de uma mensagem por meio da utilização de algoritmos matemáticos a fim de criar padrões de segurança de armazenamento de dados e de gestão de tráfego entre dispositivos automatizados. Neste trabalho, é apresentado um protocolo de criptografia simétrica baseada em cifra de uso único *One-Time Pad*, (OTP) associada ao modo de operação *Electronic Code Book* (ECB). O protocolo consiste em um algoritmo que divide a mensagem original em blocos, e cada bloco é criptografado separadamente combinando caractere por caractere da mensagem original a uma chave criptográfica aleatória que é utilizada apenas uma vez para garantir que o sistema seja imperscrutável. A chave criptográfica é obtida por meio da porta lógica *Controlled-NOT gate* (CNOT) para alcançar um texto cifrado seguro.

Termos para indexação: Criptografia, otp, criptografia simétrica, porta cnot.

[1] Tecnólogo em Análise e Desenvolvimento de Sistemas, bolsista de iniciação científica - CNPq, Embrapa Informática Agropecuária, SP.

[2] Analista de sistemas, analista na Embrapa Informática Agropecuária, Campinas, SP.

[3] Físico, Doutor em Ciências, pesquisador da Embrapa Informática Agropecuária, Campinas, SP .

Protocol for one-time pad via controlled-NOT function

Abstract – Cryptography is an information protection technique that consists of encoding the content of a message through the use of mathematical algorithms in order to create security patterns of data storage and traffic management between automated devices. In this project, it is presented a symmetric cryptographic protocol based in One-Time Pad (OTP) associated to the Eletronic Code Book (ECB) operation mode. The protocol consists of an algorithm that divides the original message in blocks, each block being separately encrypted and combining character by character of the original message to a random cryptographic key that is used only once to ensure that the system is inscrutable. The cryptographic key is obtained through CNOT gate to achieve secure encrypted text.

Index terms: Cryptography, otp, symmetric cryptography, cnot gate.

Introdução

O uso da Criptografia – um conjunto de regras matemáticas que visa codificar a informação de forma que só o emissor e o receptor consigam decifrá-la – torna-se essencial para manter a privacidade de usuários e/ou para construir formas de armazenamento seguras de dados.

Uma forma intuitiva de armazenamento físico seguro de informações é a utilização de um armário com fechadura, onde somente quem possui a chave tem acesso aos itens ali contidos. A representação virtual desse tipo de armazenamento é o que se conhece por criptografia simétrica, ou seja, um algoritmo que usa a mesma chave criptográfica para encriptação de texto puro e decriptação do texto cifrado. Se a chave é verdadeiramente aleatória, o resultado da encriptação simétrica é o que se conhece por cifra de uso único *One-Time Pad* (OTP). Esse tipo de encriptação é assintoticamente seguro e é considerado inquebrável mesmo em teoria (Castro, 2017).

A teoria relacionada à cifra de uso único é fortemente baseada na hipótese de unidirecionalidade (*one-wayness*) de caminhos computacionais (Castro, 2014). Essa conjectura matemática sustenta a existência de uma permutação (função simétrica) para a qual o cálculo em uma direção é fácil, enquanto reconstruir o estado de entrada a partir do estado de saída é computacionalmente difícil. Neste trabalho é apresentado um sistema unidirecional de criptografia, onde a chave aleatória é gerada pela porta lógica NOT controlada (*controlled NOT gate*) (CNOT). Esta porta constrói bits entrelaçados – um tipo de estrutura binária que não pode ser fatorada – de tal forma que o estado de saída inviabiliza a inversão da função criptográfica por qualquer meio determinístico (Castro, 2017).

Cifra de uso único

O OTP é um sistema de criptografia de chave de uso único considerado completamente seguro. Nesse sistema, cada byte de uma mensagem (no formato plaintext) é criptografado com um byte de uma chave aleatoriamente gerada e cada byte só pode ser usado uma única vez, ou seja, para cada mensagem (plaintext) nova é imprescindível o uso de uma nova chave, e esta deve ser no mínimo do mesmo tamanho de seu plaintext ou maior. Respeitadas essas premissas, a cifra é considerada segura e não pode ser quebrada mesmo em teoria.

Considere o exemplo abaixo:

$$y_0 = (x_o + k_0) mod 2$$

$$y_1 = (x_1 + k_1) mod 2$$

.

.

.

onde y é o um bit da cifra, x é um bit do plaintext e k um bit da chave. Se o atacante tem conhecimento sobre o valor de y_0 (0 ou 1), por exemplo, ele não pode determinar o valor de x_0. Isso é, se k_0 foi gerado a partir de uma fonte verdadeiramente aleatória, então as soluções $x_0=0$ ou $x_0=1$ possuem 50% de chance de serem corretas, uma vez que 0 xor 0 = 1 xor 1 e 0 xor 1 = 1 xor 0.

Contudo, conforme Stallings (2010), a utilização do OTP é limitada a mensagens e chaves de mesmo comprimento. Além disso, há dois problemas fundamentais:

1. Há um problema prático da geração de grandes quantidades de chaves aleatórias. Qualquer sistema utilizado pode exigir milhões de caracteres aleatórios de forma regular. O fornecimento de caracteres verdadeiramente aleatórios nessa quantidade é uma tarefa significativamente complexa.

2. Ainda mais agravante é o problema da distribuição e proteção das chaves. Para cada mensagem enviada, é necessária uma chave de comprimento igual tanto para o emissor quanto para o receptor.

O fato de a chave ter de ser do mesmo tamanho do *plaintext* ou maior dificulta seu uso para a encriptação de dados ou documentos grandes. Se a informação contém um Gigabyte, então temos uma chave do mesmo comprimento, o que faz com que seja inviável o uso dessa criptografia para a maioria das aplicações.

Para minimizar o problema do comprimento da chave, utiliza-se a técnica de modo de operação. Para Stallings (2010), um modo de operação, em essência é uma técnica para aprimorar o efeito de um algoritmo de criptografia ou adaptar o algoritmo para uma aplicação, tal como aplicar uma cifra de bloco para uma sequência de blocos de dados ou um fluxo de dados. Assim, neste trabalho, um modo de operação de ciframento de blocos com blocos de comprimento fixo será utilizado com o intuito de minimizar o problema da distribuição de chaves que consiste em reduzir o tamanho da chave sem afetar a sua propriedade de aleatoriedade.

Na encriptação de dados padrão, há vários modos de operação que podem ser usados. Aqui, é abordado apenas um, devido a sua simplicidade de aplicação: *Electronic CodeBook* (ECB). O modo ECB consiste em dividir o *plaintext* em blocos, e realizar a encriptação direta e independentemente em cada bloco do plaintext, assim, a sequência resultante de saída é o texto cifrado. A função abaixo representa a encriptação utilizando o modo de operação ECB:

$$Y_j = ENCRIPT_k(M_j) \qquad \text{para } j = 1...n.$$

Para todo bloco é utilizada a mesma chave k, e a cifra sendo o resultado das várias cifras $Y_{(1...n)}$ concatenadas no final. Para mensagens longas, o ECB pode não ser seguro. Se a mensagem é altamente estruturada, será possível para um criptoanalista explorar essas regularidades (Stallings, 2010).

Esse tipo de modo de operação, para ser seguro, leva em consideração que a mensagem seja aleatória, pois se o mesmo bloco aparecer repetidas vezes (o que acontece com mensagens com estruturas bem definidas) então aparecerá um conjunto de blocos iguais, tornando vulnerável a análise de padrões a partir da cifra final. Contudo, se a mensagem não contiver padrões repetidos ou for preparada por um processo de branqueamento (randomização), o ECB é seguro. Alternativamente, pode-se usar uma chave diferente para cada bloco de uma mensagem que contenha padrões repetidos, conforme sugere o Institute of Electrical and Electronics Engineers (2008). A seguir, Figura 1 descreve o modo de aplicação do ECB neste trabalho.

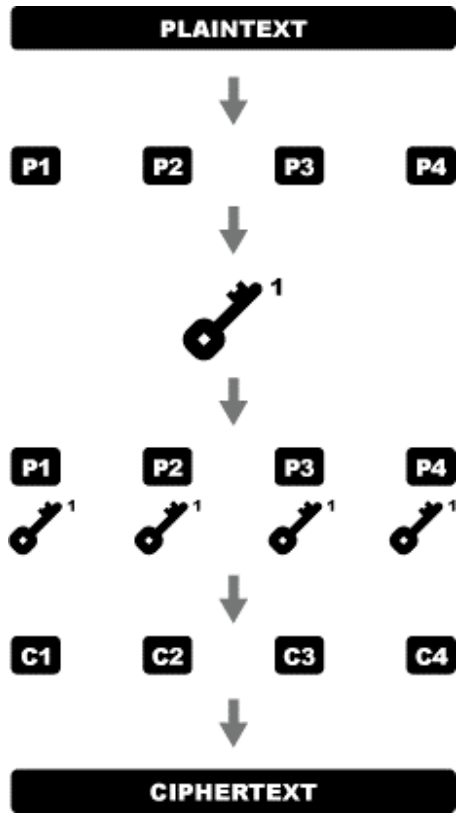


Figura 1. Transformação do plaintext para ciphertext usando ECB.

Como mostra a Figura 1, o *plaintext* é dividido em blocos $p1, p2,...pn$. Após este processo é gerada a chave a partir de um gerador demonstrado a seguir utilizando uma porta lógica quântica. Em sequência é aplicada a mesma chave com um algoritmo de encriptação para cada bloco do *plaintext*, assim surgindo os blocos cifrados $c1,c2,...cn$. No passo seguinte é realizada a concatenação dos blocos cifrados resultando no *ciphertext*, ou seja, a mensagem criptografada.

A seguir, é demonstrado o gerador de chaves por meio da operação da porta lógica quântica NOT controlada (CNOT), uma porta lógica reversível de fundamental importância para a computação quântica, pois sua operação facilita a obtenção de fortemente correlacionados (Williams, 2011).

A tabela verdade da porta NOT controlada (CNOT) é apresentada na Tabela 1.

Tabela 1. Tabela verdade da CNOT.

$controle$	$alvo$	$controle'$	$alvo'$
$\mathbf{0}\rangle$	$0\rangle$	$\|0\rangle$	$0\rangle$
$\mathbf{0}\rangle$	$1\rangle$	$\|0\rangle$	$1\rangle$
$\mathbf{1}\rangle$	$0\rangle$	$1\rangle$	$1\rangle$
$\mathbf{1}\rangle$	$1\rangle$	$1\rangle$	$0\rangle$

A porta lógica CNOT consiste em 2 qubits. O qubit é a informação mais simples em um sistema quântico, tendo dois estados de base computacional possíveis: $|0\rangle$ e $|1\rangle$. A CNOT altera o segundo qubit (qubit alvo), se e somente se, o primeiro qubit (qubit de controle) for igual a $|1\rangle$, e não faz nada se o qubit de controle for igual a $|0\rangle$. A primeira coluna da tabela representa os estados antes da operação e a segunda, após a operação.

De forma geral, a porta lógica CNOT pode ser escrita sobre dois qubits, operacionalmente, $|a\rangle$ e $|x\rangle \epsilon GF_2$, em que o primeiro é o qubit de controle, o último é o qubit alvo, e GF_2 é o campo de Galois de dois elementos, $GF_2=\{0,1\}$, assim, $CNOT|a,x\rangle = |a,a \oplus x\rangle$, onde $a \oplus x = (a+x) mod 2$.

Note que para $a = x$, $CNOT|a,x\rangle = |a,x^2 \oplus x\rangle$, e, para $a \neq x$, $CNOT|a,x\rangle = |a,x^2 \oplus x \oplus 1\rangle$, onde $x^2 \oplus x \oplus 1 = NOT(x^2 \oplus x)$, com $x = \{0,1\}$, e considerando que $x \wedge x = x$ e que a operação lógica AND corresponde a operação de multiplicação, nós temos $x^2 = x$. (Castro, 2014, Castro; Minto Neto, 2015).

A partir dessa construção para porta NOT Controlada, pode-se gerar um texto cifrado seguro uma vez que a saída da CNOT são quatro estados entrelaçados conhecidos como estados de Bell. São eles:

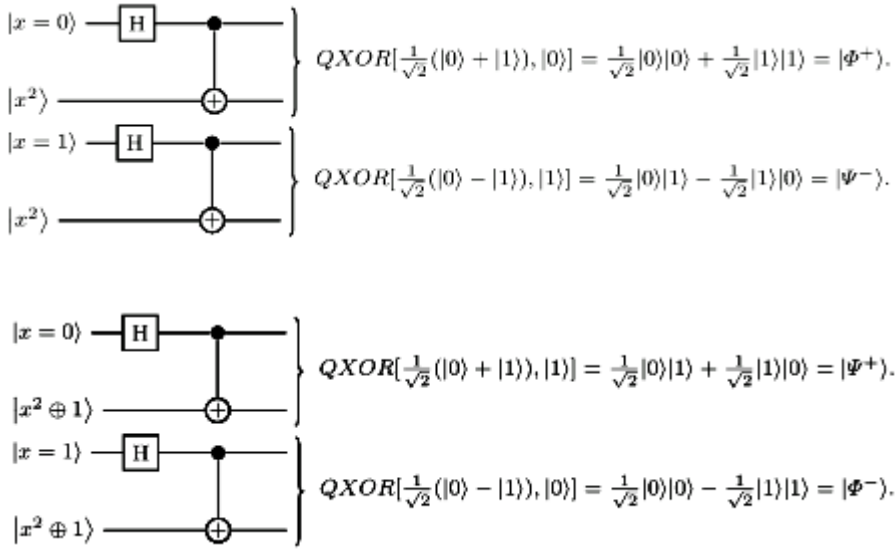
$$|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|01\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|10\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|11\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Considere que um qubit é dado pela seguinte expressão (Kunz, 1979):

$$|x\rangle_{x=\{0,1\}} \underset{\rightarrow}{H} \frac{1}{\sqrt{2}}[(-1)^x|x\rangle + |1-x\rangle]$$

(Equação 1)

A seguir, a representação do circuito quântico gerando os estados de Bell. (Castro, 2017):



Esse circuito simples aplica a porta de Hadamard dado pela $Equação1$ para a primeira linha e aplica uma porta lógica XOR ao bit alvo, produzindo estados maximamente entrelaçados ou emaranhados

$|\phi^{\pm}\rangle = (|0\rangle \pm |1\rangle)QXOR|0\rangle = QXOR(|0\rangle \pm |1\rangle, |0\rangle) = QXOR(|0\rangle, |0\rangle) \pm QXOR(|1\rangle, |0\rangle)$ e $|\psi^{\pm}\rangle = (|0\rangle \pm |1\rangle)QXOR|1\rangle = QXOR(|0\rangle \pm |1\rangle, |1\rangle) = QXOR(|0\rangle, |1\rangle) \pm QXOR(|1\rangle, |1\rangle)$, em que a constante de normalização é omitida. A operação quântica do OR exclusivo (QXOR) corresponde a porta CNOT.

Após os estados de Bell gerados, vemos que não é possível desentrelaçar. Veja este estado de Bell, por exemplo:

$$|0\rangle|0\rangle \pm |1\rangle|1\rangle$$

Note que não há como colocar em evidência qualquer dos estados $|0\rangle$ ou $|1\rangle$. Agora, em contrapartida, mesmo se pegarmos um estado de Bell que permite colocar em evidência qualquer dos estados para tentar fatorar, percebe que não é possível fatorar, pois não retorna a sua equação original, ou informação original. Veja este estado de Bell que nos permite colocar em evidência os estados para tentar fatorar.

$$|0\rangle|1\rangle \pm |1\rangle|0\rangle \text{ (Equação2)}$$

Nesse caso, não é possível fatorar, pois o produto dos estados $|0\rangle$ e $|1\rangle$ não é comutativo, ou seja, $|0\rangle|1\rangle \neq |1\rangle|0\rangle$, pois os $|.\rangle$ são matrizes. Veja que o resultado não retorna igual a $Equação2$:

$$|0\rangle(|1\rangle \pm |1\rangle) = |0\rangle|1\rangle \pm |0\rangle|1\rangle$$

$$|1\rangle(|0\rangle \pm |0\rangle) = |1\rangle|0\rangle \pm |1\rangle|0\rangle$$

A seguir, é apresentado o pseudocódigo (algoritmo) de encriptação e decriptação da criptografia simétrica baseada na porta lógica quântica CNOT e associada ao modo de operação ECB, onde x representa um cipher bit e a um key bit.

Encriptar(X):

X recebe o Plaintext;

$Blocks$ recebe o retorno do ECB aplicado ao X;

$oneBlock$ recebe um bloco aleatório de $Blocks$;

$Chave$ recebe o retorno de $oneBlock|a \oplus x) \oplus |x)$;

$REPITA$ (para i = 0; enquanto i < tamanho de $Blocks$; $i = i + 1$):

$Cifra_i$ recebe $Blocks_i \oplus Chave$;

$FIMREPITA$

$Ciphertext$ recebe $Cifra$ transformada em String;

$Retorna(Ciphertext, Chave)$

FIM Encriptar.

Decriptar(X, K):

X recebe o Ciphertext;

K recebe a Chave;

$Blocks$ recebe o retorno do ECB aplicado ao X;

$REPITA$ (para i = 0; enquanto i < tamanho de $Blocks$; $i = i + 1$):

$Text_i$ recebe $Blocks_i \oplus K$;

$FIMREPITA$

$Plaintext$ recebe $Text$ transformado em String;

$Retorna(Plaintext)$

FIM Decriptar.

Cenário

Como demonstração de uma aplicação prática da criptografia simétrica apresentada neste trabalho é utilizado o protótipo que foi desenvolvido (Castro et al. 2015) na Empresa Brasileira de Pesquisa Agropecuária (Embrapa). As imagens a seguir aplicam a encriptação e decriptação de uma informação como forma de demonstração.

O protótipo foi implementado no ambiente de programação NetBeans IDE, onde o código é apenas a tradução do pseudocódigo encontrado neste trabalho para a linguagem de programação Java.

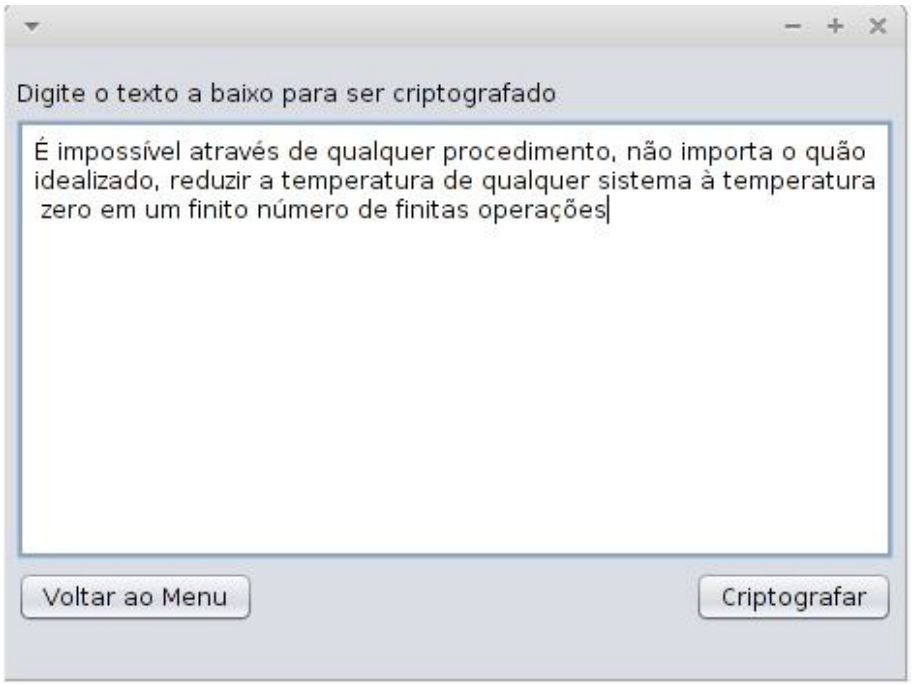


Figura 2. Exemplo de encriptação de um texto.

Fonte: Castro et al. (2015).

Na Figura 2 é inserida a informação na qual se deseja criptografar (ou ocultar) e então é acionado o botão “Criptografar” a fim de executar o algoritmo. Logo, na Figura 3 é demonstrado o texto criptografado e sua chave gerada.

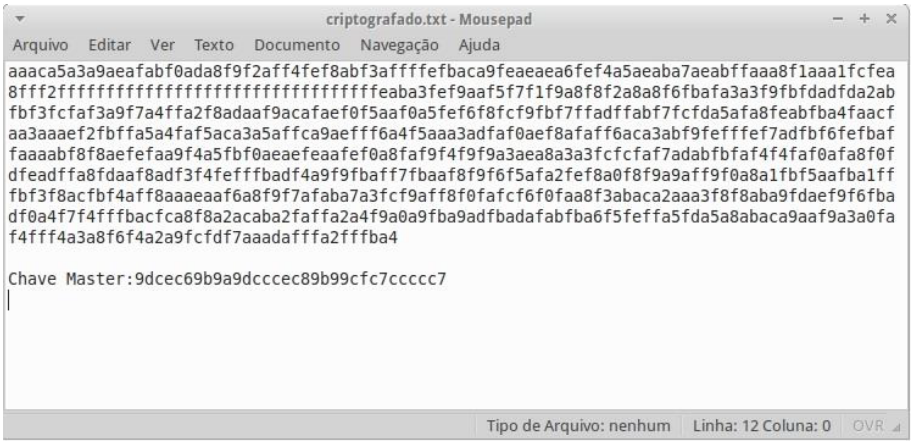


Figura 3. Texto cifrado e sua chave gerada.

Fonte: Castro et al. (2015).

Agora nas Figura 4 e 5, é demonstrada a operação inversa, a recuperação da informação, também podendo ser chamada de descriptografia. Na Figura 4, é copiada cifra (texto criptografado) e a senha do arquivo para o sistema em seus determinados campos. Logo, na Figura 5 é apresentado o texto descriptografado (ou seja, retornou ao plaintext).

Figura 4. Decriptação do texto cifrado.

Fonte: Castro et al. (2015).

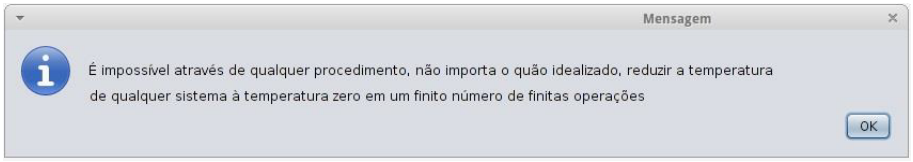


Figura 5. Resultado da Decriptação.

Fonte: Castro et al. (2015).

Considerações finais

O algoritmo proposto neste trabalho teve como implementação o modo de operação ECB por ser o mais simples dos modos de operação conhecidos, o qual pressupõe para ser seguro que a mensagem de entrada não tenha estruturas bem definidas. Se utilizadas mensagens preparadas por branqueamentos e chaves criptográficas geradas pela operação NOT controlada, o resultado é uma cifra assintoticamente segura, dado que a chave é gerada aleatoriamente. O uso da porta lógica quântica CNOT viabiliza a não dependência de fenômenos naturais externos ao próprio computador para geração de chaves aleatórias, sendo, então, uma tecnologia de baixo custo. Além disso, por ter sido desenvolvido nacionalmente, evita-se a dependência de tecnologia estrangeira na área da segurança da informação.

Em trabalhos futuros, serão implementados e analisados outros modos de operação como, por exemplo, *Cipher-block chaining* (CBC); *Cipher feedback* (CFB); *Output feedback* (OFB); e o *Counter* (CTR) (Dworkin, 2001) em conjuntos com a porta CNOT no intuito de realizar testes de criptoanálise, em que é possível verificar a eficiência de cada modo de operação, juntamente com o algoritmo de criptografia aqui apresentado. Em outros modos que não o ECB, a preparação por branqueamento da mensagem pode ser dispensável, tornando o sistema como um todo autossuficiente.

Referências

CASTRO, A. de. One-way-ness in the input-saving (Turing) machine. **Physica A**: Statistical Mechanics and its Applications, v. 415, n. 1, p. 473-478, Dec. 2014. DOI: 10.1016/j.physa.2014.08.021.

CASTRO, A. de. Quantum one-way permutation over the finite field of two elements. **Quantum Information Processing**, v. 16, p. 149, 2017. DOI:10.1007/s11128-017-1599-6.

CASTRO, A. de; MINTO NETO, J. G. **Sistema de criptografia simétrica via porta lógica quântica**. Campinas: Embrapa Informática Agropecuária, 2015. 3 p. (Embrapa Informática Agropecuária. Comunicado técnico, 119).

CASTRO, A. de; SANTOS, E. H. dos; MINTO NETO, J. G. **Ouroborus block cipher mode. Versão 1.0**. Campinas: Embrapa Informática Agropecuária, 2015. 1 CD-ROM.

DWORKIN, M. **Recommendation for block cipher modes of operation:** methods and techniques. Washington: National Institute Of Standards And Technology, 2001. 66 p. Disponível em: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf>. Acesso em: 1º jun. 2017.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE standard for cryptographic protection of data on block-oriented storage devices**. New York, 2008. 32 p. (IEEE Std 1619™-2007). Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4493450>. Acesso em: 22 fev. 2018.

KUNZ, H. O. “On the Equivalence Between One-Dimensional Discrete Walsh-Hadamard and Multidimensional Discrete Fourier Transforms”. **IEEE Transactions on Computers**, v. 28, n. p. 267-268, Mar. 1979. DOI:10.1109/TC.1979.1675334.

STALLINGS, W. **Cryptography and network security**: principles and practice. 5th ed. Boston: Pearson Prentice Hall, 2010. 744 p.

WILLIAMS, C. P. **Explorations in quantum computing**. 2nd ed. London; New York: Springer, 2011. 717 p. (Texts in computer science).

MINISTÉRIO DA
AGRICULTURA, PECUÁRIA
E ABASTECIMENTO

BRASIL
GOVERNO FEDERAL

CGPE 14412