DOI: http://dx.doi.org/10.29069/forscience.2014v2n2.e120



# PROJETO E DESENVOLVIMENTO DE UM HARDWARE RECONFIGURÁVEL DE CRIPTOGRAFIA PARA A TRANSMISSÃO SEGURA DE DADOS

**Otávio de Souza Martins Gomes**[1]
**Rodolfo Labiapari Mansur Guimarães**[2]

## RESUMO

Neste trabalho serão mostradas algumas conclusões prévias e escolhas realizadas para o desenvolvimento de uma interface de criptografia simétrica, utilizando *hardware* reconfigurável para a transmissão segura de dados. Os dispositivos reconfiguráveis permitem o desenvolvimento deste *hardware* de maneira segura e com uma grande flexibilidade, além da possibilidade de realizar algumas alterações com um mínimo de custo e tempo adicionais. Até o momento foram desenvolvidos os modelos para a implementação. O próximo passo será iniciar o desenvolvimento do *hardware*, que utilizará linguagens de descrição de *hardware* e *Field Programmable Gate Arrays* (FPGAs).

**Palavras-chave:** Segurança. FPGA. PSoC. 3DES. VHDL.

# DESIGN AND DEVELOPMENT OF AN CRYPTOGRAPHY RECONFIGURABLE HARDWARE FOR SECURE DATA TRASMISSION

## ABSTRACT

This paper presents some conclusions and choices about the development of a symmetric cryptography reconfigurable hardware interface to allow a safe data communication. Reconfigurable hardwares allow the development of this kind of device with safety and flexibility, and offer the possibility to change some features with low cost and in a fast way. So far, the hardware models and functionalities were developed. The next step is to start the hardware implementation, which will use hardware description languages and FPGAs.

**Keywords**: Security. FPGA. PSoC. 3DES. VHDL.

[1] Doutorando em Engenharia Elétrica pela Universidade Federal de Itajubá (Unifei), mestrado em Engenharia Elétrica pela Unifei e docente efetivo do Instituto Federal de Minas Gerais – Campus Formiga. E-mail: otavio.gomes@ifmg.edu.br.
[2] Graduando em Ciência da Computação pelo IFMG- Campus Formiga. E-mail: rodolfolabiapari@gmail.com.

# 1 INTRODUÇÃO

A troca de informações entre as pessoas sempre foi um dos itens básicos da sobrevivência de toda a humanidade. Em determinadas épocas, tais informações eram levadas por um mensageiro ou eram gravadas, geralmente em papéis, e continham um grande problema em si. Em caso de roubo ou de espionagem, elas poderiam ser interceptadas e lidas por pessoas que não tinham a devida autorização dos membros relacionados diretamente com a mensagem, e isso poderia acarretar sérios problemas, tanto pelo roubo quanto pela alteração dos dados, com o propósito de induzir o destinatário, por exemplo, para uma armadilha. Em uma guerra, o simples roubo de uma informação sigilosa poderia determinar o grande vencedor, que poderia utilizar as informações contidas na mensagem a seu favor, colocando um país e, consequentemente, a vida de muitas pessoas em risco (STALLINGS, 2008).

A criptografia é usada como uma técnica de alteração de dados, seguindo um código ou algoritmo preestabelecidos pelo remetente e pelo destinatário, para que as informações que serão enviadas sejam ininteligíveis, a não ser para as pessoas que possuem a chave correta do código. A chave torna todo o embaralhamento da mensagem um processo simétrico, de forma a permitir realizar os processos de modo inverso, utilizando os parâmetros corretos para retornar a mensagem inicial.

Na década de 70 ainda não existia um algoritmo suficientemente forte. Então, o *National Institute of Standards and Technology* (NIST), do governo norte-americano, escolheu o *Data Encryption Standard* (DES), da IBM, como o principal algoritmo da época (OLIVEIRA, 2002). Em 1978, foi adotado pelo *National Bureou of Standard*, e, em 1981, foi empregado como padrão pelo grupo ANSI (CÔRREA; CARMO, 2009; NIST, [200-?]). Hoje, há diversos órgãos que normalizam e controlam os padrões de segurança de dados (STALLINGS, 2008).

O algoritmo 3DES foi desenvolvido para ser implementado tanto em *software* quanto em *hardware,* assim como seu predecessor, o algoritmo DES (TERADA, 2008).

A lógica programável proporciona ao desenvolvedor a possibilidade de se adequar aos vários níveis de projetos, para prototipagem ou circuitos finais, além da fácil alteração do projeto a qualquer momento. Álgebra Boole, mapa de Karnaugh e Linguagens de Descrição de Hardware também são incluídas neste ramo de desenvolvimento. O FPGA, no qual será a plataforma de desenvolvimento final, é uma classe de circuitos integrados com propósito geral de *hardware* reconfigurável.

A Computação Reconfigurável é uma solução intermediária na resolução de problemas complexos, possibilitando combinar a velocidade do *hardware* com a flexibilidade do *software,* buscando melhor desempenho e baixo custo, com vistas à manutenção em projetos onde isso não é facilitado, como em desenvolvimento de circuitos (PEDRONI 2010).

## 1.1 CRIPTOGRAFIA SIMÉTRICA E A QUEBRA DO DES

Para a criptografia simétrica, os métodos utilizados devem ser conhecidos tanto pelos remetentes quanto por seus destinatários, e também deve existir uma chave em comum entre eles. Para tornar a mensagem ilegível de volta à original, é necessário que o destinatário faça o inverso do método feito pelo remetente com esta mesma chave. Assim, o método realiza os cálculos/procedimentos que estão ligados diretamente ao tamanho, tipo e conteúdo da chave, resultando na saída correta ao fim de sua execução.

Os algoritmos simétricos utilizam uma chave *k*, que criptografa um texto legível *x* através de operações lógico-aritméticas, resultando num outro texto ilegível tal que $f_k(x) = y$. O texto ilegível pode ser enviado por uma rede insegura para seu destino, onde *y* só é descriptografado pela função inversa $f_K^{-1}(y) = x$ se e somente se for utilizada a mesma chave *k*.

A ciência que tenta descobrir o texto claro a partir do texto cifrado sem a chave chama-se criptoanálise. Hoje, com o uso de computadores, os algoritmos estão ficando mais complexos (KAHN, 2002).

Porém, a criptoanálise não está inoperante. Lars Knudsen (KNUDSEN, 1998) classificou vários tipos de ataque em blocos cifrados. Atualmente, existem muitos resultados positivos oriundos do estudo da criptoanálise, assim como a grande descoberta de que o algoritmo DES pode ser quebrado em poucos dias utilizando Dispositivo Lógico Programável (PLD).

Portanto, ao publicar uma mensagem já transcrita, qualquer um poderá ter essa mensagem ilegível em mãos, mesmo com o algoritmo, mas *somente os que tiverem sua verdadeira chave* conseguirão revelar o conteúdo da mensagem (CARTILHA, 2012).

## 2 DESENVOLVIMENTO

Este projeto de pesquisa tem como objetivos projetar e construir, utilizando as plataformas PSoC e FPGA, *hardwares* reconfiguráveis que realizem a função de criptografar

dados. Até o presente momento, foi realizada a revisão bibliográfica sobre o assunto, bem como o estudo dos algoritmos de criptografia DES e 3DES, sendo o desenvolvimento deste último na linguagem de alto nível *C*, para a compreensão de suas estruturas.

O algoritmo DES possui vários pequenos blocos de funções que se baseiam em substituições, permutações e operações lógicas. Suas características de *confusão* e *difusão* dificultam ainda mais o roubo da informação, sendo necessários 18 processos para que um texto puro selecionado transforme-se totalmente em um texto cifrado.

Eli Biham, na década de 90, melhorou a criptoanálise diferencial do DES, criando o 3DES, que executava 3 codificações DES sucessivamente, utilizando, no mínimo, 2 chaves diferentes, criando uma nova "chave" de, no mínimo, 128 *bits* (NIST, 2014; E.F.F., 1998). Assim, em termos matemáticos, a fórmula matemática para a criptografia do 3DES seria $C = DES_{k3}\{DES_{k2}\{DES_{k1}(TextoPuro)\}\}$ onde *C* é o resultado final, *TextoPuro* é o texto puro, $DES_k$ é o algoritmo de criptografia e $ki$ seria a chave $i$ utilizada.

## 3 CONCLUSÃO

A implementação dos algoritmos de criptografia em *software*, desenvolvidos em Linguagem C, foi realizada com sucesso e representa a primeira parte deste projeto, que está em andamento.

Conforme Matsui (1994); Moreno, Pereira e Chiaramonte (2005), a criptografia em *hardware* é mais segura que a desenvolvida em *software,* devido à dificuldade de se quebrar a chave e/ou descobrir como foi realizada a implementação. O próximo passo será a implementação desses algoritmos em *hardware*. Com a finalização dos protótipos em FPGA, serão avaliados o desempenho e a corretude dos algoritmos em *hardware*, por meio de testes em ferramentas de medição.

## AGRADECIMENTOS

Os autores agradecem ao Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais – IFMG o apoio financeiro por meio do projeto de pesquisa aprovado no Edital: 156/2013.

## REFERÊNCIAS

CORRÊA, A. S. F. M.; CARMO, L. F. R. da C. **Algoritmos Simétricos para *Software* Embarcado**. Rio de Janeiro: UFRJ, 2009. Disponível em: <http://equipe.nce.ufrj.br/rust/Mestrado%202009/SionSimetricAlg2009_SR.pdf>. Acesso em: 11 nov. 2013.

CARTILHA DE SEGURANÇA PARA INTERNET. **Criptografia**, 2012. Disponível em: <http://cartilha.cert.br/criptografia/>. Acesso em: 13 dez. 2013.

E. F. F. **Cracking DES**: secrets of how federal encryption research, agencies Wiretap Politics subvert & Chip Design. [S.l.]: O'Reilly Media, 1998.

KAHN, D. **Remarks of David Kahn**: commemorating the 50th Anniversary of the National Security Agency. [S.l.]: FAS: Intelligence Resource Program, 2002.

KNUDSEN, L. **Contemporary Block Ciphers**: lectures on data security, 1998. p. 105-126.

MATSUI, M. Linear Cryptanalysis Method for DES Cipher: in advances in Criptology, Eurocrypt 93, Lectures Notes in Computer Science. **Springer Berlin Heidelberg**, 1994. v. 765, p. 386-397, 1994.

MORENO, E. D.; PEREIRA, F. D.; CHIARAMONTE, R. B. **Criptografia em Software e Hardware**. 1. ed. Rio de Janeiro: Novatec, 2005.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) INFORMATION TECHNOLOGY LABORATORY, [200-?] Disponível em: <http://csrc.nist.gov/ groups/ST/toolkit/examples.html>. Acesso em: 21 jan. 2014.

OLIVEIRA, M. L. R. **Uma análise da segurança e da eficiência do algoritmo de criptografia posicional**. 2012. 43 f. (Bacharelado em Ciência da Computação) – Universidade Federal de Lavras (UFLA), Lavras, 2002. Disponível em: <http://www.bcc.ufla.br/wp-content/uploads/2013/2001/Uma_analise_da_seguranca_e_da_eficiencia_do_algoritmo_de_criptografia_posicional.pdf>. Acesso em: 23 fev. 2014.

PEDRONI, V. A. **Eletrônica Digital Moderna e VHDL:** princípios digitais, eletrônica digital, projeto digital, microeletrônica e VHDL. São Paulo: Elsevier, 2010.

STALLINGS, W. **Criptografia e segurança de redes**: princípios e práticas. 4. ed. Rio de Janeiro: Pearson, 2008.

TERADA, R. **Segurança de dados**: criptografia em redes de computador. 2. ed. São Paulo; Edgar Bluchler, 2008.

**Recebido em**: 16/11/2014

**Aprovado em**: 28/11/2014

**Publicado em**: 26/01/2015