Resumo Expandido

Título da Pesquisa (Português): Projeto e Desenvolvimento de um Hardware Reconfigurável de Criptografia para a Transmissão Segura de Dados.		
Título da Pesquisa (Inglês): Design and Development of a Reconfigurable Hardware Encryption for Secure Data Transmission.		
Palavras-chave: Criptografia, 3DES, DES, FPGA, Hardware Reconfigurável.		
Keywords: Encryption, 3DES, DES, FPGA, reconfigurable hardware.		
Campus: Formiga.	**Tipo de Bolsa**: Iniciação Tecnológica.	**Financiador**: CNPq.
Bolsista(s): Rodolfo Labiapari Mansur Guimarães.		
Professor Orientador: Otávio de Souza Martins Gomes.		
Área de Conhecimento: 1.03.00.00-7 Ciência da Computação, 3.04.00.00-7 Engenharia Elétrica.		**Edital**: 156/2013.

Resumo:

Esta pesquisa tem como objetivo a implementação de um algoritmo de criptografia simétrico num sistema de *hardware* reconfigurável. Proporcionará a codificação de mensagens de forma rápida e segura a fim que o texto final ilegível possa ser transmitido por um ambiente inseguro aplicando a restrição que somente os que tenham previamente a chave utilizada para a codificação, possam desvendar o conteúdo desta. Utilizar Dispositivos Lógico Programáveis (PLDs) tem-se a liberdade de desenvolver um projeto grande como este realizado com destreza, segurança, fácil prototipagem e manutenção além de baixo custo.

Abstract:

This research aims to implement a symmetric encryption algorithm in reconfigurable hardware system. Provide the encoding of messages quickly and securely to the end garbled text can be transmitted by an unsafe environment by applying the restriction that only those who have previously the key used for encryption, can unravel the contents of this. Using Programmable Logic Devices (PLDs) has the freedom to develop a large project like this done deftly, safety, easy prototyping and maintenance as well as low cost.

INTRODUÇÃO:

A troca de informações entre as pessoas sempre foi um dos itens da sobrevivência de toda a humanidade. Tais informações eram levadas por um enviado ou gravadas geralmente em papeis 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 que deviam estar relacionados diretamente com essa mensagem, sendo que isso poderia acarretar sérios problemas apenas pelo roubo ou até mesmo da alteração desses dados com o propósito de confundir o destinatário, por exemplo, para uma armadilha. Em uma guerra, o simples roubo de uma informação sigilosa poderia determinar o grande vencedor pois poderia utilizar as informações que continham na mensagem a seu favor colocando um país e, consequentemente, a vida de muitas pessoas em risco (STALLINGS, 2008).

Com base nesse enorme problema, foram criados simples métodos que transpunham esses textos planos/claros (mensagens legíveis e de fácil entendimento) em mensagens que não poderiam ser de maneira alguma interpretadas por humanos sem tais métodos, com o intuito de dificultar em um tempo mínimo e se possível impedir totalmente o seu entendimento.

Para a criptografia simétrica, os métodos utilizados devem ser conhecidos tanto pelos remetentes e quanto por seus destinatários. Também deve existir uma chave em comum entre eles pois para tornar novamente a mensagem ilegível idêntica a original, é necessário que o destinatário faça exatamente o inverso do método feito pelo remetente utilizando esta mesma chave. De uma maneira simplista, deve-se utilizar o mesmo algoritmo de modo 'inverso' em conjunto com a chave correta no qual foi utilizada na realização da criptografia da mensagem para que o método realize os cálculos/procedimentos corretos os quais estão diretamente ligados ao tamanho, tipo da chave e o conteúdo da chave.

Também chamados de algoritmos de chave secreta, os algoritmos utilizam uma chave *K* que criptografa um texto legível *x* resultando num outro texto ilegível y tal que $f_K(x) = y$. O texto *y* pode ser transmitido por uma rede insegura para seu destino onde *y* é decifrando pelo algoritmo inverso $f^{-1}_K(y) = x$ se e somente se o destinatário utilizar a mesma chave *K* tal como mostra a Figura 1.

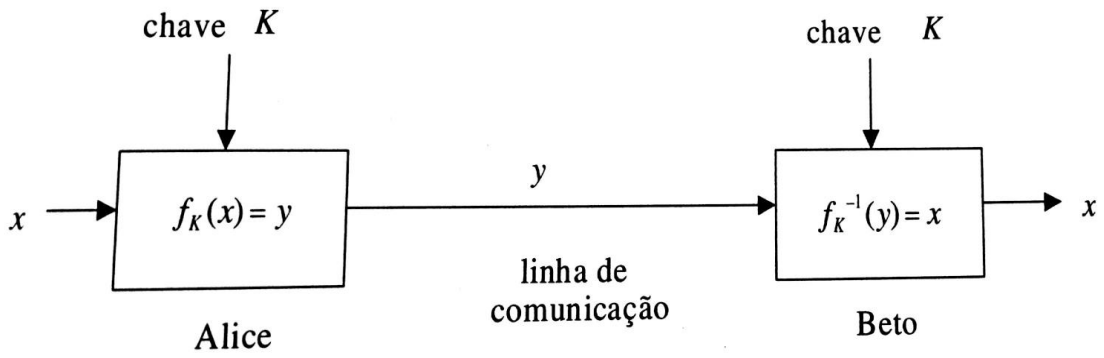

Figura 1: Criptografia Simétrica.

Supondo que Alice (remetente) deseja mandar uma mensagem para Beto (destinatário) sem que Carlos (interceptador não autorizado a ler o conteúdo da mensagem) interprete o conteúdo desta, as chaves

se tornam o quesito fundamental desta situação. Utilizar chaves que não são autenticadas por Alice e Beto, impedirá que Carlos, mesmo tendo o algoritmo em mãos, de conseguir de forma alguma resgatar a mensagem original de maneira facilitada. Carlos teria que testar todas as combinações de chaves possíveis para a quebra da informação sendo que isso poderia levar uma eternidade.

Para determinados tipos de situações é indispensável que a tradução da mensagem seja realizada num tempo máximo *t.* Caso contrário, todo o trabalho pode ser descartado pelo fato da informação não ser relevante mais. Imaginando que uma mensagem descreve que as tropas de determinado país vão atacar dois dias depois do envio da carta. Se os inimigos traduzirem a carta 5 dias depois do envio dela, o valor da tradução não teria importância alguma.

A ciência que tenta descobrir o texto claro a partir do texto cifrado sem a chave ou descobrir a lógica utilizada para sua encriptação chama-se criptoanálise. Hoje, com s utilizados para beneficiar e agilizar os processos de criptografia, tornam o processo de criptoanálise mais complexo pois a cada dia os algoritmo estão ficando mais complexos. Sobre o assunto da dificuldade de encontrar as respostas dos métodos de criptografia dos dias atuais, David Kahn comentou (KAHN, 1974):

> Muitos são os criptossistemas oferecidos pelas centenas dos vendedores comerciais hoje que não podem ser quebrados por qualquer método conhecido da criptoanálise. Certamente que, em tais sistemas, mesmo um ataque de texto escolhido, em que um texto selecionado é combinado contra sua mensagem cifrada, não pode entregar a chave que destrava outras mensagens. Por isso, então, a criptoanálise está inoperante. Mas esse não é o fim da história. A criptoanálise pode estar inoperante, mas há mais do que um único caminho para tirar a pele de um gato.

Lars Knudsen (KNUDSEN, 1999) classificou vários tipos de ataque em blocos cifrados sendo esses a Ruptura total, o algoritmo Distinguindo, Dedução da Informação, Dedução Global e Dedução do Exemplo. Atualmente, existem muitos resultados positivos oriundos do estudo da criptoanálise tal como a grande descoberta que o algoritmo DES que será apresentado neste documento, pode ser quebrado em poucos dias (GILMORE, 1998).

Portanto, ao publicar uma mensagem já transcrita, qualquer pessoa poderá ter essa mensagem ilegível em mãos mesmo com o algoritmo na qual foi criptografada, mas somente as pessoas com o algoritmo e sua verdadeira chave que conseguirão revelar seu conteúdo de maneira legível (CARTILHA, 2012).

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 81 foi adotado como padrão em segurança pelo grupo ANSI utilizando o nome DEA (DA COSTA CARMO, CORRÊA, 2009) (NITS). Hoje, há diversos órgãos que normatizam e controlam os padrões de segurança de dados (STALLINGS, 2008).

METODOLOGIA:

Materiais e Métodos

FPGA

Os dispositivos lógico programáveis (PLDs, *Programmable Logic Devices*) tornaram-se incrivelmente populares devido sua obsolescência em permitir a substituição do desenvolvimento de circuitos ASIC de uma forma nova facilitada mantendo as mesmas características originais do projeto, sua facilidade na prototipagem com complexidade reduzida, velocidade na execução de seus circuitos simulando uma velocidade de um circuito ASIC, menor custo de energia e com menor custo de fabricação. Eles possuem recursos em *hardware* que permitem sua reconfiguração no próprio circuito integrado que foi implementado para execução de novas funções de circuitos lógicos, correções de erro entre muitas outros (COSTA, MESQUITA, PINHEIRO, 2011). Podem ser projetados para ocuparem menos espaço dentro do módulo ou possuírem velocidades mais elevadas.

A lógica programável proporciona ao desenvolvedor a possibilidade de se adequar aos vários níveis de projetos sendo estes para prototipagem ou até o desenvolvimento de circuitos finais, além da fácil alteração do projeto a qualquer momento. Álgebra Boole, mapa de Karnaugh, e Linguagens de Descrição de *Hardware* (HDL) também são incluídas neste ramo de desenvolvimento.

Atualmente, existe basicamente 3 tipos de PLDs: os Dispositivos Lógicos Programáveis Simples (SPLD, *Simple Programmable Logic Devices*), Dispositivos Lógico Programáveis Complexos (CPLD, *Complex Programmable Logic Devices*), Matrizes Lógicas Programáveis no Campo (FPGA, *Field Programmable Gate Array*) sendo que estes podem ser encontrados pelas empresas Achronix, Actel, Altera, Atmel, Cypress, Lattice, Quicklogic e Xilinx sendo suas ferramentas de projeto Achronix CAD Environment, Libero IDE, Quartus II, Integrated Development System, Warp, ispLEVER, QuickWorks, ISE (COSTA, MESQUITA, PINHEIRO, 2011). Nesta pesquisa utilizará um FPGA da Altera usando o *software* Quartus II.

O FPGA é um circuito lógico-programável, isto é, uma classe de circuitos integrados com propósito geral. É um dispositivo semicondutor que é utilizado para o processamento de informações digitais. A Computação Reconfigurável é uma solução intermediária na resolução de problemas complexos, possibilitando combinar a velocidade do *hardware* com a flexibilidade do *software* com a meta da procura do melhor desempenho possível (PEDRONI, 2010).

Algoritmo DES e 3DES

Como este projeto de pesquisa tem como objetivo projetar e implementar, utilizando a plataforma FPGA, um *hardware* reconfigurável de criptografia simétrica para a transmissão segura de dados, escolheu-se o algoritmo de criptografia 3DES para ser estudado e desenvolvido. O 3DES baseia-se totalmente no algoritmo DES onde possui vários pequenos blocos de funções que permite o desenvolvimento modular possibilitando sua adaptação em ambientes específicos e melhoria. Utilizando cifra de bloco, independentemente do tamanho do texto puro (mensagem), o algoritmo DES usará blocos de 64 *bits*. Sua característica de confusão

e difusão dificulta ainda mais o roubo da informação sendo necessários 18 processos para que um texto puro selecionado se transforme totalmente em um texto cifrado (SHANNON, 1949) (TERADA, 2000).

- **Difusão:** em cifra de bloco binária, pode ser feita repetindo várias vezes o processo de permutação;
- **Confusão:** torna as ligações da chave com a mensagem cifrada tão complexas a ponto de atrasar mais ainda o processo de criptoanálise do algoritmo.

Matthew Robshaw (ROBSHAW, 1995), menciona que as técnicas difusão e confusão são tão bem-sucessivas que elas se tornaram a base do projeto moderno de cifra de blocos.

A principal característica do algoritmo de criptografia DES é a função Feistel. Ela é composta por duas entradas e duas saídas de dados. Para realizar suas operações, a função Feistel necessita que seja passada a ela o texto de tamanho 64 *bits* e também a chave de criptografia. No início, o texto é dividido em duas partes e essas são divididas para que cada uma opere diferentemente da outra metade enquanto a função se repete várias vezes para que no fim, elas se reúnem novamente formando um bloco de texto cifrado com o mesmo tamanho. Assim, é possível fazer o processo inverso retornando ao texto claro passando por parâmetro o bloco criptografado realizando os passos de modo inverso.

Todas as iterações (rodadas) têm a mesma estrutura. O que difere entre elas é que a cada iteração, as operações são realizadas apenas em uma das duas metades do texto onde elas são trocadas de lugar ao longo da execução. Ao todo, são realizada 16 operações invertendo as posições de cada metade da mensagem. Ou seja, para que o algoritmo possa continuar a ser simétrico e permitir o passo reverso (decifra), as metades são trocadas de lugar tornando a metade que não foi trabalhada anteriormente a próxima a ser operada. E com isso, a cada iteração, a função principal utiliza uma sub-chave *Ki* derivada da chave original *K*. De modo geral, todas as sub-chaves *Ki* são diferentes entre si e também entre a chave principal *K* .

Eli Biham na década de 90, melhorou a criptanálise diferencial do DES criando o 3DES. Assim, executando 3 codificação DES sucessivamente utilizando no mínimo 2 chaves diferentes, cria-se uma nova “chave” (NIST) (GILMORE, 1998).

RESULTADOS E DISCUSSÕES:

De início, desenvolveu-se o algoritmo criptográfico 3DES em linguagem alto nível.

Era necessário desenvolver o algoritmo sem utilizar bibliotecas matemáticas prontas que realizassem as operações de forma facilitada. Além disso, seria uma opção também desenvolver em um dispositivo PSoC[1] onde este utiliza a linguagem de programação *C.* Sendo assim, foi decidido que o algoritmo seria feito em linguagem *C* para que possa aprender sobre seu funcionamento em detalhes e assim desenvolver cada módulo/procedimento separado pra que esta possa ser reproduzida ao realizar o desenvolvimento em linguagem de descrição de *hardware.* O desenvolvimento também poderia ser realizado em Programação Orientada a Objetos, Funcional entre outras, mas foi desenvolvido em linguagem Imperativa pelo fato da linguagem descritiva de *hardware* também ser imperativa e sequencial. Facilitaria mais ainda a implementação utilizando uma de alto nível imperativa como a linguagem *C* como foi feita.

Percebeu-se que para codificar o algoritmo em alto nível precisaria de vários sub-processos especiais tais como rotações, permutações e operações em vetores de *bit*, e operações de processamento de chave e texto puro. Tudo com implementação própria para conhecimento profundo do algoritmo e seu modo de execução.

Também foi desenvolvidos relatórios parciais sobre a implementação do código em alto nível e também tutoriais sobre equipamentos que serão utilizados ao longo do projeto de pesquisa. Os equipamentos foram o *Logic16* da Seleae e também o microprocessador PSoC 3 – 8051 do CY8KIT-001.

Atualmente está em fase de implementação o algoritmo DES de criptografia em linguagem de descrição de hardware. Está sendo implementado o procedimento que realiza a cifragem do código pelo algoritmo DES sendo que o DES possui duas funções principais (operação com o texto e com a chave). Já o procedimento de operação com as chaves já foi implementado pelo desenvolvedor. A implementação inicial é baseada no DES o 3DES, que é o objetivo final da pesquisa, é simplesmente a execução do DES três vezes consecutivas com no mínimo duas chaves diferentes e este será o último passo a ser realizado no desenvolvimento do algoritmo em linguagem de descrição de *hardware.*

Todos os módulos desenvolvidos são testados utilizando *softwares* de simulação de linguagens de descrição de *hardware.* Como são vários módulos, começou-se o desenvolvimento de cada um deste separado e assim verificando sua corretividade. Todos os testes realizados com o método de processamento das chaves até agora desenvolvido foram descritos seus resultados com sucesso. Além da corretude, tais módulos devem ter a sincronia de desenvolvimento não sendo cada um executado no momento certo sem que capture ou gere sinais inválidos dos outros blocos anteriores/subsequentes.

[1] É composto de um núcleo, analógico configurável e blocos digitais, e encaminhamento programável e interconexão.

CONCLUSÕES:

Até o momento foi realizada pesquisas bibliográficas do assunto, estudo superficial sobre vários algoritmos de criptografia em especial ao algoritmo 3DES onde foi feito seu desenvolvimento. Também foi realizado um curso introdutório sobre a linguagem VHDL além de estudos sobre ferramentas que serão utilizadas no projeto. O algoritmo foi desenvolvido na linguagem de alto nível *C* e está atualmente em desenvolvimento em linguagem de descrição de *hardware.* Também estão sendo realizadas apresentações internas no instituto sobre as atividades de pesquisa e também o desenvolvimento de relatório dos equipamentos que serão utilizados ao longo da pesquisa.

Com o crescimento dos investimentos nacionais na área de microeletrônica e na fabricação de circuitos integrados, é importante a realização de projetos de pesquisa na área de prototipagem de dispositivos reconfiguráveis, tendo em vista que eles participam ativamente do ciclo de projeto de um ASIC, na fase de validação da ideia proposta.

Sabendo que 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, sem contar da sua grande flexibilidade de desenvolvimento (GRABBE, 1992) (MORENO, 2005) e somando com o algoritmo que está em funcionamento na linguagem *C*, com a finalização do projeto, desenvolvimento, simulação, prototipagem e validação do *hardware*, pode-se comparar o desempenho das mesmas, ou seja, *hardware* e *software* e tirar as devidas conclusões como custo, facilidade de desenvolvimento, velocidade de processamento de texto entre outros. Também será possível utilizá-lo em projetos mais complexos, como a transmissão de dados da rede elétrica (*SmartGrid*) ou em sistemas SCADA.

REFERÊNCIA BIBLIOGRÁFICA:

COSTA, Cesar da; MESQUITA, Leonardo; PINHEIRO, Eduardo. Elementos de Lógica Programável com VHDL e DSP. **Érica, 1º ed, São Paulo**, 2011.

CRIPTOGRAFIA. Publicado dia 06/03/2012. Acessado dia 13/12/13. Disponível em: <http://cartilha.cert.br/criptografia/>.

DA COSTA CARMO, Luiz Fernando Rust; CORRÊA, André Sion Fernandes Muniz. Algoritmos Simétricos para Software Embarcado. 2009.

GILMORE, John. Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design. 1998.

GRABBE, J. Orlin. The DES algorithm illustrated. **Laissez Faire City Times**, v. 2, n. 28, p. 12-15, 1992.

KAHN, David. **The codebreakers**. Weidenfeld and Nicolson, 1974.

KNUDSEN, Lars R. Contemporary block ciphers. In: **Lectures on Data Security**. Springer Berlin Heidelberg, 1999. p. 105-126.

MORENO, Edward David; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. Criptografia em Software e hardware. **São Paulo: Novatec**, 2005.

NIST. **National Institute of Standards and Technology** - Information Technology Laboratory. Acessado 21/01/2014. Disponível em: <http://csrc.nist.gov/groups/ST/toolkit/examples.html>.

OLIVEIRA, Mário Luiz Rodrigues. Uma análise da segurança e da eficiência do algorítmo de criptografia posicional. **Monografia de graduação, Universidade Federal de Lavras**, 2002.

PEDRONI, Volnei A. **Circuit Design with VHDL**. Cambridge, MA: MIT Press, 2010.

ROBSHAW, M. J. B. The Block Ciphers–RSA Laboratories Technical Report TR-601. **RSA Laboratories**, 1995.

SHANNON, Claude E. Communication theory of secrecy systems*. **Bell system technical journal**, v. 28, n. 4, p. 656-715, 1949.

STALLINGS, William. **Cryptography and Networks Security: Principles and Practices**. Ed. Prentice Hall, Second Edition, 2008.

TERADA, Routo. **Segurança de dados: criptografia em redes de computador**. Edgard Blucher, 2000.

Participação em Congressos, publicações e/ou pedidos de proteção intelectual:

GUIMARÃES, Rodolfo Labiapari Mansur; GOMES Otávio Souza Martins. **Projeto e desenvolvimento de um hardware reconfigurável de criptografia para a transmissão segura de dados.** Revista Científica ForScience V. 2, n. 2, 2014.