PLANO DE PESQUISA

Feira de Ciências, Empreendedorismo e Inovação da Bahia

Título do Projeto: *Encryption's Builder Studio* - Estúdio Construtor de Encriptação
Estudantes: Thiago Santos Sousa
Professor Orientador: Silvelane Lima de Queiroz Pereira
Colégio: Centro Territorial de Educação Profissional Recôncavo II Alberto Torres
Série/Ano dos Estudantes: 2º ano
Questão ou Problema Identificado: Em um mundo em que as redes de computadores e as conexões evoluíram bastante, os ataques cibernéticos também cresceram em larga proporção. Tais atos são praticados por indivíduos que possuem conhecimentos em tecnologia da informação e utilizam seus conhecimentos para realizar a prática de ataques e roubos cibernéticos. As maiores vítimas destes tipos de ataques são pessoas que possuem poucas habilidades na utilização dos meios tecnológicos. Como guardar/trocar mensagens ou arquivos de modo seguro? Buscando contribuir para tornar o ambiente informatizado mais seguro de um modo geral, seja na troca básica de mensagens e e-mails, no armazenamento de informações e senhas, etc. o *Encryption's Builder Studio* - Estúdio Construtor de Encriptação uma aplicação desenvolvida combinar múltiplas criptografias, capaz de proteger os dados de forma segura e dinâmica.
Hipótese ou Objetivo: Desenvolver algoritmos de criptografia que podem ser utilizados entre a aplicação e o banco de dados, proporcionando uma comunicação entre o sistema de forma confiável e segura. A fim de contemplar o objetivo geral os seguintes objetivos específicos foram listados: ● Contribuir para proteção na troca de e-mails e arquivos, através dos algoritmos de criptografia aumentando a segurança ao criptografar as informações.

- Proporcionar a encriptação de forma simples através dos algoritmos de forma que todos os indivíduos possam utilizar o recurso.
- Avaliar os danos causados pela utilização dos algoritmos ao criptografar os dados.
- Analisar a eficiência do uso do aplicativo através do feedback dos usuários.
- Corrigir eventuais falhas apresentadas no aplicativo.

Descrição Detalhada dos Materiais e Métodos (Procedimentos) que serão utilizados:

A pesquisa inicialmente será pautada através de estudos bibliográficos, vídeos, reportagens, artigos científicos, pesquisas, elementos necessários para compreensão e desenvolvimento do tema criptografia, visando desenvolver uma aplicação, capaz de encriptar e desencriptar dados e arquivos.

Após a pesquisa dos artigos, um protótipo da aplicação foi desenvolvido, e em seguida disponibilizado na internet - através da plataforma desenvolvida para hospedá-lo - para realização de testes iniciais pelos usuários.

Um formulário será disponibilizado para que os usuários da aplicação avaliem o app dando o feedback necessário para correções posteriores do aplicativo. E se o aplicativo atingiu objetivo para melhorar a segurança das informações quando elas são criptografadas e guardadas.

O ambiente de criação de algoritmos de encriptação, são desenvolvidos a partir dos padrões de chaves e vetores de inicialização (IV), algoritmos que podem ser usados para proteger múltiplas informações que devem ser criptografadas (textos ou bytes), utilizando algoritmos simétricos, que através CBC (cipher block chaining) se tornam mais seguros. No processo de uma encriptação assimétrica, a informação perpassa por uma variação de duas chaves (pública e privada).

Para a pesquisa sobre criptografia: foram utilizados o computador com acesso à internet; Manuais, cursos e vídeos online sobre criptografia e matemática;

Para a construção do aplicativo, utilizou-se os softwares Microsoft Visual Studio Community 2019 (aplicação gratuita para estudos de **.NET** no Windows);Microsoft Windows PowerShell ISE (Programa disponível no Microsoft Windows); SQLite (Sistema de Gerenciamento de Bancos de Dados gratuito disponível para computador);

No desenvolvimento do site para hospedar o aplicativo: foi utilizada a plataforma Wordpress (gratuito, disponível em https://wordpress.com/) e Domínio do Infinity Free (site que disponibiliza domínios gratuitos para estudos para hospedagem de sites e bancos de dados).

Bibliografia (Três referências mais importantes)

FIARRESGA, Victor Manuel Calhabrês *et al*. **Criptografia e matemática.** 2010. Tese de Doutorado.

FOLHA, Rodrigo Barbosa CR-ASPE: uma técnica de criptografia para dados espaciais armazenados na nuvem / Rodrigo Barbosa Folha. – 2017. Disponível em: https://repositorio.ufpe.br/bitstreamhttps://bityli.com/lGkLrKV/123456789/25851/1/DISSERTA%C3%87%C3%83O%20Rodrigo%20Folha%20.pdf

HOSANG, Alexandre. Política Nacional de Segurança Cibernética: uma necessidade para o Brasil. **Escola Superior De Guerra**, Rio De Janeiro, 2011. Disponível em: https://bdtd.ucb.br:8443/jspui/bitstream/123456789/1417/1/Alcyon%20Ferreira%20de%20Souza%20Junior.pdf