Contatos:
lucas_candinho1@estudante.sesisenai.org.br
Joao_luckow@estudante.sesiseni.org.br
thiago_gehrke@estudante.sesisenai.org.br
jonathan.sardo@edu.sesisc.org.br (Orientador)

CriptoBox - Visualização da Criptografia RSA Utilizando Arduino

Nomes dos autores: João Rodrigo Heinzelmann Luckow, Lucas Candinho e Thiago Medeiros Gehrke

Áreas de conhecimento: Ciências Exatas e da Terra
Ciências da Computação

INTRODUÇÃO

A criptografia é a arte de cifrar/codificar uma mensagem como mecanismo de segurança (VICENTE et al; 2016). Uma arte milenar, utilizada desde o hieróglifo dos egípcios por meio de cifras, substituições monoalfabéticas, mensagens escritas em tiras de couro enroladas em bastões, dentre outros métodos, este recurso tornou-se fundamental nos dias atuais (DE; SILVA, 2019).

Com o advento das mídias digitais é perceptível que a utilização da criptografia faz-se indispensável, seja no âmbito da segurança ou da privacidade, uma vez que sem ela nada do que usufruímos digitalmente poderia laborar, como os serviços bancários na palma da mão, comércio online, privacidade nas milhares de mensagens trocadas diariamente (VICENTE et al; 2016). Não obstante, apesar de a criptografia estar presente em todo o meio digital atualmente, ela é pouco estudada e difundida, dificultando o entendimento acerca deste tema.

DESENVOLVIMENTO

Um dos exemplos de criptografia é a RSA, a qual, segundo Castro (2019) é uma criptografia conhecida por ter seu código de codificação público, o que chamamos de chave pública. Teoricamente, a ideia do RSA é muito simples: dados dois parâmetros p e q primos distintos e grandes, utilizamos $n = p \cdot q$ para codificar, e para decodificar precisamos conhecer p e q (conforme ilustrado nas figuras e 1 e 2).

Apesar de apresentar-se em situações contendo incontáveis algarismos, ela possui um princípio de funcionamento facilmente visualizável, se utilizados números primos de um a dois algarismos, os quais sejam fáceis de fatorar. Sob esta ótica, no presente trabalho foi desenvolvido um produto interativo utilizando arduino, no qual o usuário pode inserir dois números primos (simulando as chaves privadas existentes em uma interação digital entre emissor e receptor) e, assim, obter uma criptografia RSA visualizável, em que seja possível compreender seu princípio de funcionamento.

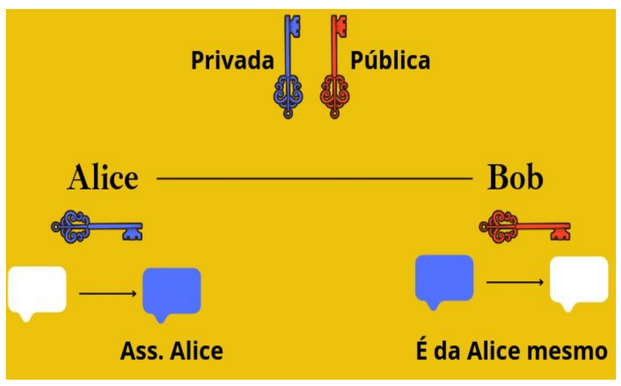

Figura 1 - Troca de Mensagem utilizando RSA
Fonte: Produção Própria

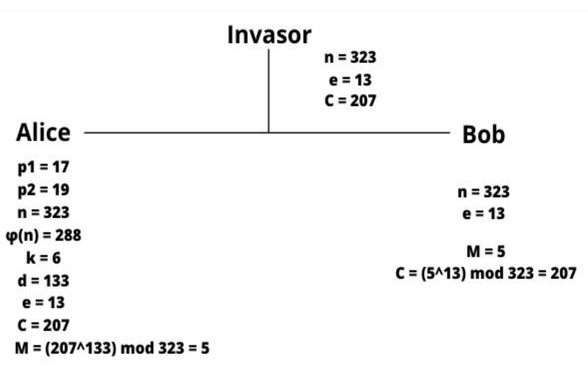

Figura 2 - Funcionamento da Criptografia RSA
Fonte: Produção Própria

RESULTADOS OBTIDOS

Após uma série de testes, simulações e construções de protótipos utilizando diversos materiais e métodos (conforme ilustrado na figura x), o produto final foi construído utilizando filamento PLA, fabricado na impressora 3D e madeira devido a quesitos de resistência do material, recursos disponíveis no ambiente e melhor disposição dos componentes no interior da caixa (arduino, protoboard e bateria 9V).

Quanto a programação, apesar terem sido encontradas algumas dificuldades relacionados à inserção das fórmulas da Criptografia RSA nas linhas de código e no quesito da randomização real dos números, o resultado final foi positivo. Desse modo, foi possível incorporar a programação ao projeto, conforme esperado.

Para agrupar os materiais fabricados no projeto, foi criado um repositório na plataforma Github (https://github.com/CriptografiaIC/CriptoBox), acesso pelo ***QR Code*** na figura 4.

Figura 4 - ***QR Code*** para o repositório
Fonte: Produção Própria

OBJETIVOS

Objetivo geral

Desenvolver um produto material, no qual seja possível visualizar a criptografia RSA.

Objetivos específicos

1. Compreender números primos;
2. Ilustrar a criptografia RSA;
3. Mostrar a matemática de maneira prática, aplicando-a;
4. Verificar conceitos matemáticos envolvidos na criptografia

METODOLOGIA

A partir da escolha do tema, foi realizado um processo de pesquisa sobre Criptografia RSA e seu funcionamento envolvendo números primos e coprimos utilizando a função phi de Euler. Com este embasamento, partimos para a simulação do processo com arduino, utilizando o tinkercad. Em seguida, desenvolvemos a programação da dinâmica, adicionando as funcionalidades presentes no hardware (leds, display, potenciômetros), e, em paralelo, iniciamos a construção de um protótipo do produto.

No decorrer deste processo, acabamos encontrando algumas dificuldades nos métodos esperados e limitações em determinados tipos de materiais. Em função disso, foram elaborados diversos tipos de prototipos físicos (conforme ilustrado na figura 3) até chegarmos ao produto final.

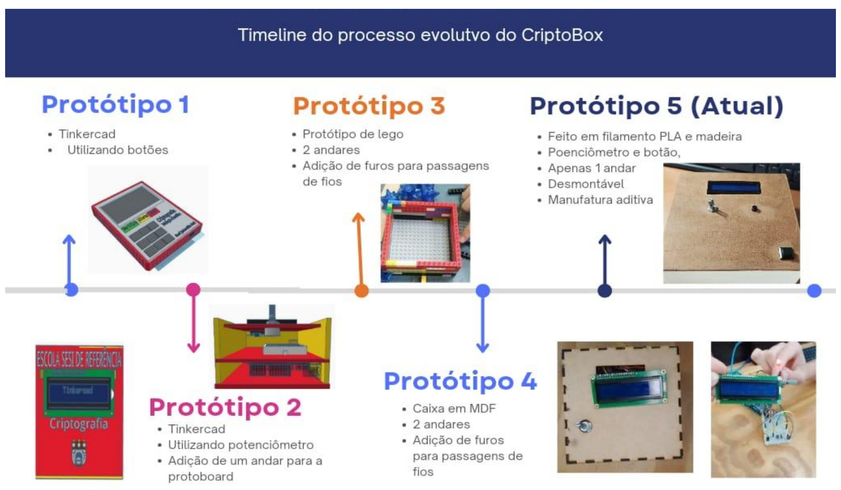

Figura 3 - Linha do tempo dos protótipos
Fonte: Produção Própria

CONCLUSÕES

Após a construção do produto final e da realização da programação incorporando a função phi de Euler e adicionando as demais funcionalidades presentes no modelo, pôde-se concluir que é possível tornar a criptografia RSA visualizável através de um produto físico similar a uma calculadora, capaz de realizar o cálculo para obter uma criptografia RSA a partir da inserção de dois números primos (chaves privadas).

Ademais, a realização do projeto, no estado atual permite extensão e adição de funcionalidades, visto que, inicialmente, o projeto está restrito a um procedimento linear e apenas realiza operações com a criptografia RSA.

REFERÊNCIAS

CASTRO, C. UNIVERSIDADE FEDERAL DE SANTA CATARINA CRIPTOGRAFIA RSA. [s.l: s.n.]. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/203902/TCC_Camila.pdf?sequence=1&isAllowed=y>. Acesso em: 19 dez. 2023.

DE, W.; SILVA, M. INSTITUTO FEDERAL GOIANO -CAMPUS CERES BACHARELADO EM SISTEMAS DE INFORMAÇÃO A EVOLUÇÃO DA CRIPTOGRAFIA E SUAS TÉCNICAS AO LONGO DA HISTÓRIA CERES -GO. [s.l: s.n.]. Disponível em: <https://repositorio.ifgoiano.edu.br/bitstream/prefix/795/1/tcc_Willian_Wallace_de_Matteus_Silva.pdf>

VICENTE, Aparecido; ARAÚJO, Bernardo de; ROCHA, Luciano Magno; ALMEIDA, Vitor Henrique Ferreira de Lima; HADDAD, Elias. A CRIPTOGRAFIA E SUA IMPORTÂNCIA NA ATUALIDADE. Revista Atena@ .Vol.1 – Número 0 – AGOSTO 2016 . Disponível em: <https://periodicosunimes.unimesvirtual.com.br/index.php/gestaoenegocios/article/view/630>.