Atividade 7 - parte 2

Identificação de Problema de Pesquisa, Objetivo, Hipótese e Justificativa da Hipótese

Jorge Luiz Medeiros Pires
790942
Bacharelado em Ciência da Computação

Giullio Emmanuel da Cruz di Gerolamo
790965
Bacharelado em Ciência da Computação

Artigo: Algoritmo de criptografia RSA: análise entre a segurança e velocidade

Identificação

Primeiramente, foi escolhido o seguinte artigo:

ANDRADE, R. S.; SILVA, F. dos S. **Algoritmo de criptografia RSA: análise entre a segurança e velocidade.** Revista Eventos Pedagógicos, [S. l.], v. 3, n. 3, p. 438–457, 2012. DOI: 10.30681/reps.v3i3.9329. Disponível em: https://periodicos.unemat.br/index.php/reps/article/view/9329. Acesso em: 31 jul. 2023.

A partir dele, foi selecionado trechos onde é possível identificar os elementos abaixo de forma clara.

Problema de Pesquisa

- *Enunciado*

  Com o aumento do poder de processamento dos computadores, existe uma disputa entre velocidade e segurança dos algoritmos de criptografia, o que implica na busca por métodos mais eficientes e seguros de criptografar mensagens.

- *Trecho e Justificativa*

  > "Os algoritmos atuais utilizam como parâmetro uma chave
  > de modo que temos uma criptografia e descriptografia diferente para cada chave diferente. Quanto maior o tamanho da chave mais difícil ela será encontrada e, portanto mais segura será a mensagem criptografada. Com o aumento do seu poder de processamento, os computadores passaram a descobriras chaves mais facilmente, exigindo assim, o aumento gradativo das mesmas. Mas de acordo com Fuzitaki (2004) esse aumento implica na diminuição do tempo decifragem e decifragem, resultando em uma disputa entre velocidade e segurança do algoritmo."

  ANDRADE, R. S.; SILVA, F. dos S. **Algoritmo de criptografia RSA: análise entre a segurança e velocidade.** Revista Eventos Pedagógicos, [S. l.], v. 3, n. 3, p. 438–457, 2012. 2 p.

  O parágrafo aborda exatamente a questão do aumento do poder de processamento dos computadores gera uma disputa entre velocidade e segurança dos algoritmos de criptografia. Esse avanço tecnológico torna possível quebrar chaves de criptografia mais facilmente. O trecho selecionado explica que os algoritmos atuais utilizam chaves como parâmetro para garantir a segurança das mensagens criptografadas. Quanto maior o tamanho da chave, mais difícil será encontrá-la e, portanto, mais segura será a mensagem

criptografada. No entanto, o avanço do poder de processamento dos computadores permite que eles descubram chaves mais facilmente, o que resulta na diminuição do tempo de decifragem e decifragem, intensificando a disputa entre velocidade e segurança dos algoritmos.

- ***A importância do problema de pesquisa***

  A importância desse problema de pesquisa está relacionada à proteção de informações sensíveis, privacidade, segurança de transações online, confiabilidade de sistemas de comunicação e o desenvolvimento de tecnologias mais seguras. Além disso, influencia a legislação e regulamentação relacionadas à privacidade e segurança cibernética. Encontrar um equilíbrio entre velocidade e segurança na criptografia é essencial para garantir a segurança das comunicações em um mundo digital em constante evolução.

Objetivo de Pesquisa

- *Objetivo*

  Demonstrar que a escolha do tamanho da chave impactará diretamente o esforço computacional necessário para fatorá-lo.

- *Trecho e Justificativa*

  > "Dessa forma, a escolha do tamanho da chave deverá levar em conta o grau de importância e o tamanho da informação que se queira proteger. Se a informação for de alta relevância, como um arquivo que contém as senhas bancárias dos correntistas, precisa-se de uma criptografia mais forte devido à importância das informações. Mas se for de baixa relevância, como arquivo pessoal, pode-se melhor criptografá-la com chaves menores, por que será mais rápido(o que será mais rápido).Embora o módulo de 1024 bits seja menos seguro que o de 4096 bits é necessário ainda um grande esforço computacional para fatorá-lo."

  ANDRADE, R. S.; SILVA, F. dos S. **Algoritmo de criptografia RSA: análise entre a segurança e velocidade.** Revista Eventos Pedagógicos, [S. l.], v. 3, n. 3, p. 438–457, 2012. 451 p.

  O artigo deixa claro que o objetivo principal é observar o tempo de processamento em função do tamanho das chaves, confrontando segurança e desempenho. Dessa forma, no artigo, é provado que ao utilizar chaves maiores, o esforço computacional necessário para fatora-las será diretamente proporcional.

Hipótese de Pesquisa

- *Hipótese*

  A escolha do tamanho da chave impacta diretamente o esforço computacional necessário para fatorar.

- *Trecho e Justificativa*

  > “O objetivo deste trabalho é abordar a relação existente entre a busca pela segurança de dados e a velocidade de codificação e decodificação do algoritmo de criptografia RSA, que utiliza um par de números inteiros como “chave”. Considerando o tamanho da chave como requisito de segurança, devido à dificuldade computacional de fatorar números inteiros extensos, simulamos estes processos, com o algoritmo implementado na linguagem de programação C, utilizando chaves aleatórias de 1024, 2048 e 4096 bits. Desta forma, observamos o tempo de processamento em função do tamanho das chaves, confrontando segurança e desempenho.”

  ANDRADE, R. S.; SILVA, F. dos S. **Algoritmo de criptografia RSA: análise entre a segurança e velocidade.** Revista Eventos Pedagógicos, [S. l.], v. 3, n. 3, p. 438–457, 2012. 1 p.

  Logo no resumo, já é possível identificar a hipótese. No seguinte trecho, “Devido à dificuldade computacional de fatorar números inteiros extensos”, é possível identificar a dificuldade de decodificação do algoritmo RSA para chaves “grandes”.