UNIVERSIDADE CATÓLICA DE SANTOS
CIÊNCIAS DA COMPUTAÇÃO

JOÃO PEDRO THOMAZ KAIRALLA DOS SANTOS
LUCAS FERREIRA DE BRITO
MIGUEL MUSSALAM SILVA
THIAGO DANILOW DE ARAUJO

CRIPTOGRAFIA RSA: FUNCIONAMENTO E LÓGICA

SANTOS – SÃO PAULO
2023

Sumário

1. PROBLEMA DE PESQUISA

À medida que a tecnologia continua a avançar, nossos dados pessoais estão cada vez mais armazenados nos servidores de grandes empresas. Com essa revolução digital, a importância da criptografia nunca foi tão evidente. Garantir que nossas informações permaneçam acessíveis apenas para as pessoas certas é uma prioridade crítica.

Nesse cenário desafiador, a criptografia RSA tem sido uma ferramenta confiável, evoluindo ao longo dos anos. No entanto, a diferença entre uma criptografia segura e uma insegura é uma batalha constante, semelhante a um jogo de gato e rato. Isso significa que a criptografia deve estar sempre em constante evolução para se manter eficaz.

Com um uso tão frequente da tecnologia RSA por diversas empresas, acabamos nos perguntamos se essa tecnologia é realmente segura, se o papel dela é realmente cumprido devidamente. Por essa problemática procuraremos responder o nível criptográfico do tipo RSA, suas limitações, eficácia e nível de segurança e como ele se compara com outras, se é ou não segura.

2. CONTEXTUALIZAÇÃO DE PESQUISA

Em 2020, a empresa de segurança Venafi realizou uma análise abrangente de 1 milhão de sites ao longo de 18 meses. O resultado desse estudo revelou que aproximadamente 51% dos sites examinados empregavam a tecnologia de criptografia RSA.

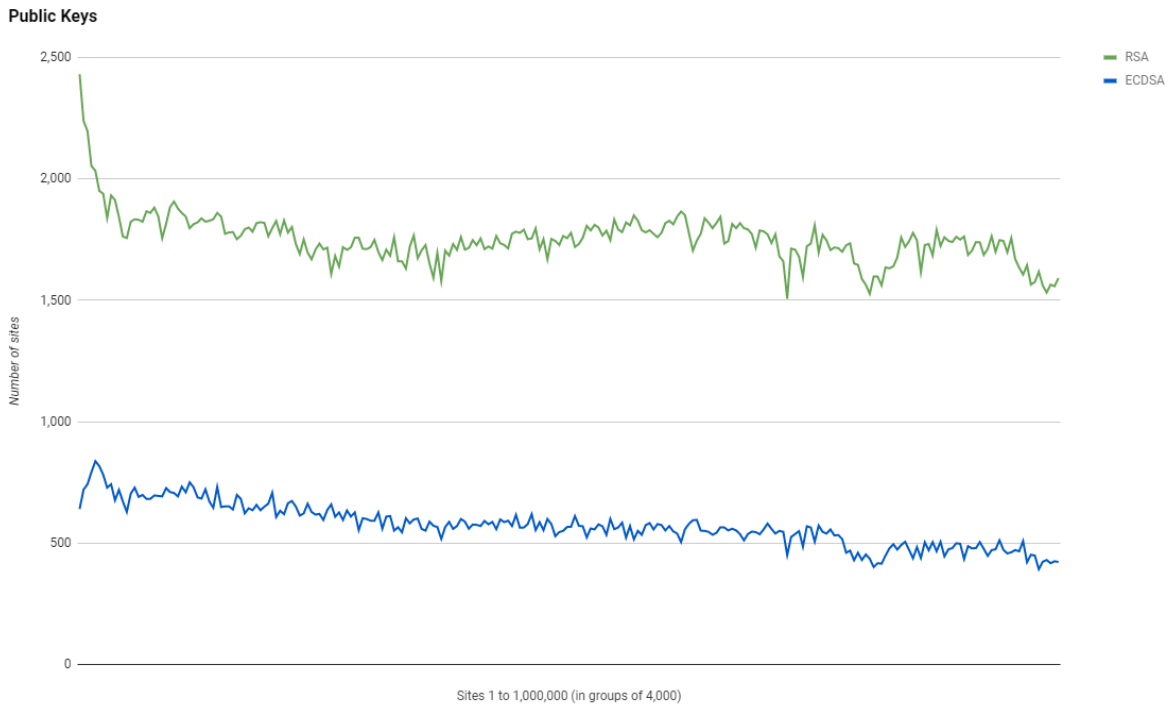

Figura 1: Comparação de uso da RSA e ECDSA

A criptografia RSA é uma criptografia assimétrica (chave pública), que se utiliza de duas chaves distintas, uma pública que fica à disposição de qualquer um que queira criptografar uma mensagem e uma privada que fica em posse do proprietário, sendo o único a conseguir descriptografar a mensagem, o algoritmo foi explicado pelos criadores em 1977 publicamente.

Constituindo uma das técnicas de segurança mais robustas da atualidade, é conhecida por ter sido desenvolvida com base na teoria dos números, especificamente na complexidade da fatoração de números em seus primos constituintes. Esta técnica foi utilizada pelos fundadores da empresa RSA Data Security, Inc., sendo eles Ron Rivest, Adi Shamir e Leonard Adleman, sendo o nome RSA derivado das primeiras letras de seus sobrenomes.

3. TIPOS DE CRIPTOGRAFIA

A contextualização das diferentes formas de criptografia é extremamente importante porque, atualmente, nós temos uma grande variedade.

3.1 CRIPTOGRAFIA SIMÉTRICA

A criptografia simétrica constitui de somente uma única chave, compartilhada entre o emissor e destinatário do conteúdo específico. A sua vantagem e a performance e a capacidade de manter uma comunicação entre vários usuários simultaneamente, sua segurança também varia dependendo do tamanho da chave utilizada. Mesmo com seu alto desempenho, a criptografia simétrica possui algumas falhas graves que tornam mais difíceis sua implementação de forma segura, esse problema se dá ao número de chaves que precisam ser criadas conforme o aumento de número de pessoas que utilizam da comunicação. Outro grave problema é a impossibilidade da verificação de identidade de quem recebe ou envia informações.

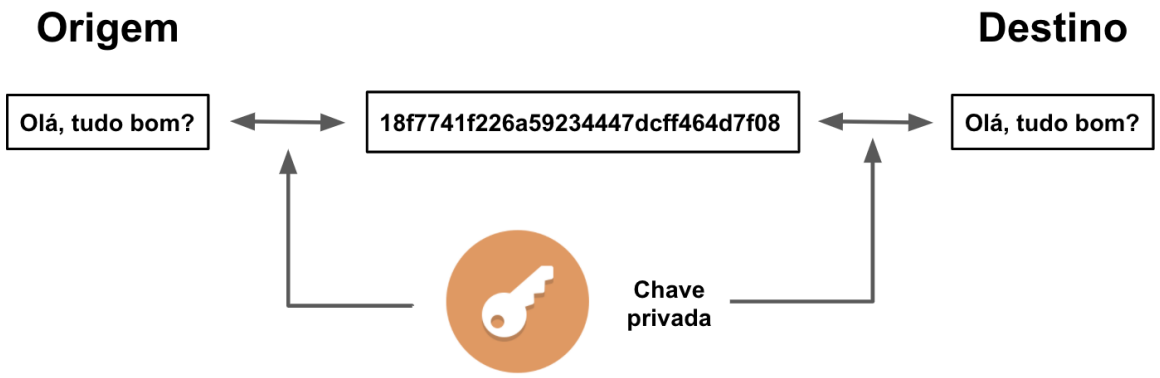

Figura 2: Exemplo visual da criptografia simétrica

Exemplos de criptografias simétricas:

- AES (Advanced Encryption Standard)

  Chave: Pode ser de 128, 192 ou 256 bits, dependendo do nível de segurança desejado.
  Exemplo de chave AES-128: 0x2b7e151628aed2a6abf7158809cf4f3c

- DES (Data Encryption Standard):

  Chave: 56 bits (embora o tamanho efetivo seja de 64 bits, com 8 bits sendo usados para verificação de paridade).
  Exemplo de chave DES: 0x0123456789ABCDEF

- 3DES (Triple Data Encryption Standard):

  Chave: 168 bits (3 chaves DES de 56 bits cada).
  Exemplo de chave 3DES:
  0x0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF

3.2 CRIPTOGRAFIA ASSIMÉTRICA

Criptografia assimétrica ou chave pública, é baseada em 2 níveis de segurança, uma privada e outra pública, elas são usadas para cifrar e verificar mensagens e a identidade do usuário. O papel da chave privada é decodificar o conteúdo, por isso o motivo dela ser privada, para que ninguém tenha o acesso para decodificação do conteúdo, já a chave pública é usada para a criação da mensagem que será codificada pela privada. Esse sistema torna a troca de dados muito mais segura, mantendo a privacidade dos usuários, pelo motivo das chaves privadas serem de acesso restrito a apenas algumas pessoas.

Figura 3: Exemplo visual da criptografia assimétrica

Exemplos de criptografias assimétricas:

- RSA (Rivest-Shamir-Adleman):
  Um dos algoritmos de criptografia assimétrica mais conhecidos e amplamente utilizados, o tema do nosso TDE.

- DSA (Digital Signature Algorithm):
  Amplamente usado para assinaturas digitais.

- ECDSA (Elliptic Curve Digital Signature Algorithm):
  Usa curvas elípticas para segurança eficiente.

Para a criação de chaves, usamos uma quantia de operações matemáticas.

4. CRIPTOGRAFIA RSA

O método de RSA é feito por vários cálculos matemáticos para as criações de chaves, criptografia e descriptografia.

4.1 CRIAÇÃO DE CHAVE PUBLICA E PRIVADA

1) o primeiro passo é a geração da chave pública, que se baseia na escolha de dois números primos grandes p e q, o recomendado sendo chaves de no mínimo 100 caracteres para grandes empresas.

2) Calculamos o produto de p e q, sendo n=p*q, esta será a fórmula usada na criptografia e descriptografia.

3) Calculamos a função totiente de Euler, φ(n), que é o número de inteiros positivos menores que n que são coprimos (não têm fatores comuns) com n. Para RSA, φ(n) = (p - 1) * (q - 1).

4) Escolha um número inteiro positivo e coprimo. Calcule o inverso multiplicativo modular de e, denotado como d, onde (d * e) % φ(n) = 1. com φ(n), geralmente chamado de "e" (exemplo comum: e = 65537), este será o expoente de criptografia.

5) A chave publica e privada se constituem de (n, e) e (n, d) respectivamente.

4.2 CRIPTOGRAFIA

1) Converta a mensagem em um número inteiro M, de acordo com um esquema de codificação.

2) Calcule C, a versão criptografada de M, usando a fórmula C = M^e % n.

3) C é a mensagem criptografada, que pode ser transmitida de forma segura.

4.3 DESCRIPTOGRAFIA

1) Receba a mensagem criptografada C.

2) Calcule M, a versão descriptografada de C, usando a fórmula M = C^d % n.

3) Converta o número M de volta para o texto original usando o esquema de codificação utilizado anteriormente.

4) Lembre-se de que a segurança do algoritmo RSA depende da dificuldade de fatorar o produto n (p * q) em seus números primos p e q. Quanto maiores forem p e q, mais segura será a criptografia.

5. JUSTIFICATIVA DE PESQUISA

Embora o algoritmo RSA seja reconhecido como uma opção de criptografia segura, não é considerado o padrão máximo de segurança quando comparado aos algoritmos de curva elíptica (ECSDA). Os algoritmos de curva elíptica oferecem um desempenho superior e níveis mais elevados de segurança. Isso se deve em grande parte ao fato de que o RSA enfrenta desafios em termos de escalabilidade, uma vez que a quantidade de poder de processamento necessário não aumenta na mesma proporção que a qualidade das chaves geradas, tornando necessário o uso de chaves de no mínimo 2048 bytes para garantir a segurança. Essa limitação torna o RSA menos vantajoso a longo prazo em comparação com alternativas como o ECSDA, que se destaca pela dificuldade em reverter o conteúdo da chave, graças à natureza das curvas elípticas. Apesar dessas considerações, o RSA continua sendo um algoritmo valioso tanto para uso quanto para estudo devido à sua sólida capacidade de criptografia e à rica história por trás de sua criação.

6. OBJETIVO GERAL

Investigar a criptografia RSA como um sistema de segurança da informação, analisando sua eficácia, suas implicações em cenários de ameaças cibernéticas emergentes e a evolução de medidas de segurança relacionadas, visando contribuir para uma compreensão abrangente e atualizada da importância do RSA na proteção de dados sensíveis em um ambiente digital em constante evolução, e através de um código mostrar na pratica como funciona o algoritmo de uma criptografia RSA em menor escala, demostrando as fórmulas matemáticas necessárias para se criptografar um mensagem.

7. OBJETIVOS ESPECÍFICOS

7.1 Mostrar através de um código em C o funcionamento de uma criptografia RSA em menor escala, demonstrando as fórmulas matemáticas necessárias para a criptografia de uma mensagem através da chave pública e o método para se descriptografar essa mesma mensagem pela chave privada.

7.2 Responder se atualmente a criptografia RSA é segura e confiável para uso, até onde vai suas limitações e se é a mais indicada para a proteção de dados.

8. REFERÊNCIAS BIBLIOGRÁFICAS

Relatório Venafi
https://venafi.com/blog/crawler-report-top-1-million-analysis-2021/

Matéria sobre o relatório da Venafi
https://www.cisoadvisor.com.br/metade-dos-sites-ainda-usa-chaves-criptograficas-legadas/

Matéria sobre a segurança do RSA
https://www.thesslstore.com/blog/is-it-still-safe-to-use-rsa-encryption/

Outra matéria sobre a segurança do RSA
https://www.helpnetsecurity.com/2023/01/25/chinese-researchers-rsa-is-breakable-do-not-panic/

Passo a passo sobre a utilização da RSA
https://www.lambda3.com.br/2012/12/entendendo-de-verdade-a-criptografia-rsa/

Trabalho sobre a eficiência longo prazo RSA

https://eprint.iacr.org/2012/064.pdf

Trabalho brasileiro sobre o método RSA

https://lume.ufrgs.br/bitstream/handle/10183/110014/000951896.pdf

Página da Wikipédia sobre a RSA

https://pt.wikipedia.org/wiki/RSA_(sistema_criptográfico)