Um estudo do sistema criptográfico RSA

Acadêmico: Douglas Correia Salazar
Orientadora: Adriana Betânia de Paula Molgora

Agosto, 2014
Dourados, MS

Resumo

A Criptografia pode ser definida como um processo de cifrar/decifrar informações com o intuito de protegê-las de destinatários não legítimos. Existem diversos métodos de criptografia, dentre os quais figura o RSA como um dos mais importantes. Um estudo aprofundado do criptossistema RSA depende primordialmente do entendimento dos processos de cifragem e decifragem de dados inerentes ao seu funcionamento. Para isso é necessária a aquisição de conhecimentos matemáticos de teoria dos números e também de conhecimentos computacionais inerentes ao processo de implementação. Esse projeto propõe realizar um estudo teórico e prático do RSA, visando disponibilizar conhecimentos sobre o mesmo, bem como possibilitar pesquisas mais aprofundadas sobre esse assunto.

Palavras-chave: criptografia, RSA, cifragem, decifragem.

1. Introdução e Revisão de Literatura

Criptografia é a arte de escrever informações sigilosas em códigos ou cifras de forma que somente o destinatário legítimo consiga interpretá-las (Coutinho, 2000). Ela originou-se da necessidade de proteção de informações e é usada nas mais diversas situações onde o sigilo de dados é importante ou até mesmo indispensável como, por exemplo, em transações bancárias, informações militares, dados governamentais e etc (Quaresma e Pinho, 2007).

Devido à extrema importância da proteção de dados ou informações, muitos estudos têm sido realizados e diversos métodos criptográficos foram desenvolvidos. Como exemplo, podem ser citados o algoritmo de Diffie-Hellman (Diffie and Hellman, 1976), o AES (Daemen and Rijmen, 2002), o RSA (Rivest et al., 1978), o ECC (Koblitz, 1987), dentre outros. Cada um deles apresenta características peculiares de aplicações e funcionamento.

O sistema criptográfico RSA é um dos sistemas mais utilizados na atualidade. O entendimento de seu funcionamento demanda a aquisição de conhecimentos matemáticos de teoria dos números (Crandall and Pomerance, 2005, Santos, 2007) e conhecimentos computacionais envolvidos nos processos de codificação e decodificação de dados.

Esse projeto tem como objetivo geral realizar um estudo teórico e prático do sistema criptográfico RSA, compreendendo tanto os aspectos matemáticos quanto os computacionais envolvidos em seu funcionamento. Com esse estudo pretende-se disponibilizar conhecimentos sobre o assunto em questão, de forma detalhada, bem como servir como base para estudos posteriores mais avançados. Além disso, pretende-se buscar publicação na área de trabalho.

Para um melhor entendimento dessa proposta, a seguir são apresentados, de forma sucinta, os aspectos gerais relacionados com o assunto de criptografia. Na Seção 2 são citados o objetivo geral e os objetivos específicos da pesquisa. Na Seção 3 é descrita a metodologia que será utilizada durante a pesquisa e na Seção 4 um cronograma de execução das atividades que serão desenvolvidas. Por fim, a Seção 5 apresenta os resultados esperados com a pesquisa.

1.1 Criptografia – Aspectos gerais

Desde os tempos primordiais, a proteção de dados ou informações sempre foi muito importante. Em diversas situações como em assuntos relacionados a guerras, o homem precisou enviar mensagens secretas e, para isso tentou desenvolver maneiras de embaralhar essas mensagens de forma que ficassem protegidas. Dessa forma nasceu a criptografia, que pode ser definida como um conjunto métodos ou técnicas que realizam a codificação e decodificação de dados.

Os diversos métodos criptográficos existentes devem implementar as propriedades de confidencialidade, integridade, autenticidade e não repúdio (Menezes *et* al, 1997). Essas propriedades devem garantir que somente o destinatário legítimo tenha acesso à informação, e que essa não foi alterada. Além disso, deve garantir a identidade de quem produziu essa informação e impedir que alguém negue o envio ou recepção da mesma.

A criptografia pode ser classificada em simétrica ou assimétrica. A criptografia simétrica é também denominada de criptografia de chave privada, existindo uma única chave para codificação e decodificação dos dados. A assimétrica é denominada de criptografia de chave pública, onde são necessárias duas chaves, uma para codificação e outra para decodificação dos dados.

Na criptografia de chave privada a chave deve ser mantida em segredo tanto pelo emissor quanto pelo receptor da mensagem. Já na criptografia de chave pública a chave usada para codificação dos dados é de domínio público e, por essa razão é denominada de chave pública. Nesse caso, a chave usada para decodificação é denominada de chave privada sendo mantida em segredo apenas pelo destinatário legítimo.

Os métodos criptográficos são constituídos de elementos comuns como, os algoritmos de codificação e decodificação de dados, as chaves criptográficas e o texto a ser cifrado/decifrado. Em geral, o tamanho da chave é muito importante, pois quanto maior a chave, menor a chance de ser descoberta (Garfinkel & Spafford, 2003).

Com o advento do computador, as trocas constantes de informações sigilosas como as que ocorrem em operações bancárias, por exemplo, tornam imprescindível o uso de métodos criptográficos que proporcionem sua segurança. Embora muitos estudos já tenham sido realizados sobre a segurança de dados e diversos métodos criptográficos tenham sido desenvolvidos, constantemente são noticiados ataques a dados sigilosos,

muitos deles causando milhões de prejuízos. Nesse sentido, estudos sobre métodos criptográficos tornam-se imprescindíveis.

O método criptográfico RSA (Rivest et al., 1978) é um dos métodos mais utilizados na atualidade. Esse método é um dos algoritmos de criptografia de chave pública mais seguros da atualidade e é utilizado em softwares como o Netscape, um popular programa de navegação da Internet. Um estudo minucioso desse método depende do entendimento do embasamento teórico matemático e computacional envolvido nos processos de codificação e decodificação dos dados. Este trabalho propõe realizar um estudo desse método criptográfico de forma detalhada a fim de disponibilizar conhecimentos sobre o mesmo e possibilitar pesquisas posteriores mais avançadas.

2. Objetivos geral e específicos

2.1. Objetivo geral

Esse projeto tem como objetivo geral realizar um estudo teórico e prático do método criptográfico RSA, visando compreender o funcionamento de seus processos de codificação e decodificação de dados possibilitando estudos mais aprofundados sobre o mesmo.

2.2. Objetivos Específicos

- Realizar um estudo das pesquisas mais recentes relacionadas com o método criptográfico RSA;
- Estudar os conceitos matemáticos necessários para o entendimento do funcionamento do método em questão;
- Estudar os algoritmos de codificação e decodificação de dados do RSA e alternativas de implementação dos mesmos;
- Implementar o método criptográfico RSA;
- Realizar testes com a implementação;
- Documentar os estudos realizados.

3. Metodologia

Para alcançar os objetivos propostos na Seção 2, o acadêmico de iniciação científica destinará 20 horas semanais, durante um período de 12 meses, para o desenvolvimento do projeto. Todas as atividades desenvolvidas ocorrerão sob a

orientação de 02 horas semanais, pela orientadora. As atividades serão distribuídas em 4 etapas, podendo haver sobreposição entre elas. Estas etapas compreendem:

- Etapa 1: Estudo, através de pesquisa bibliográfica (livros, artigos, dissertações, teses, revistas especializadas, internet e etc.), das pesquisas mais recentes relacionadas com método criptográfico RSA;
- Etapa 2: Estudo teórico dos fundamentos matemáticos relacionados com o funcionamento do RSA bem como dos algoritmos das etapas de codificação e decodificação de dados;
- Etapa 3: Implementação do método criptográfico RSA e realização de testes;
- Etapa 4: Documentação dos estudos realizados, detalhando o funcionamento dos processos de codificação e decodificação de dados do método criptográfico RSA, a fim de possibilitar o entendimento do mesmo, viabilizando pesquisas mais aprofundadas sobre o assunto. Essa documentação deverá compor os relatórios parcial e final da pesquisa.

Para a execução dessas atividades serão utilizados os recursos materiais da Universidade Estadual de Mato Grosso do Sul como computadores, acervo bibliográfico e internet. As implementações serão realizadas utilizando-se softwares livres.

Ao longo do desenvolvimento do projeto, serão realizadas reuniões periódicas na UEMS com a orientadora e o acadêmico de iniciação científica, visando apresentar e discutir os estudos efetuados e o progresso alcançado.

4. Cronograma de atividades

	Ano: 2014				
Plano de atividades – AÇÕES - 1º semestre	**A**	**S**	**O**	**N**	**D**
- Estudo, através de pesquisa bibliográfica (livros, artigos, dissertações, teses, revistas especializadas, internet e etc.), das pesquisas mais recentes relacionadas com o método criptográfico RSA. ***(Essa atividade será desenvolvida pelo bolsista com uma carga horária de 20 horas semanais sob a orientação de 02 horas semanais.)***	**X**	**X**			
- Estudo teórico dos fundamentos matemáticos relacionados com o funcionamento do RSA bem como dos algoritmos das etapas de codificação e decodificação de dados; ***(Essa atividade será desenvolvida pelo bolsista com uma carga horária de 20***			**X**	**X**	**X**

horas semanais sob a orientação de 02 horas semanais.)					
- Elaboração do relatório parcial da pesquisa. ***(Essa atividade será desenvolvida pelo bolsista com uma carga horária de 20 horas semanais sob a orientação de 02 horas semanais.)***	**X**	**X**	**X**	**X**	**X**

	Ano: 2015						
Plano de atividades – AÇÕES 2º semestre	**J**	**F**	**M**	**A**	**M**	**J**	**J**
- Implementação do método criptográfico RSA e realização de testes; ***(Essa atividade será desenvolvida pelo bolsista com uma carga horária de 20 horas semanais sob a orientação de 02 horas semanais.)***	**X**	**X**	**X**	**X**	**X**	**X**	
- Documentação de todo o estudo realizado, detalhando o funcionamento dos processos de codificação e decodificação de dados do método criptográfico RSA, a fim de possibilitar o entendimento do mesmo, viabilizando pesquisas mais aprofundadas sobre o assunto. Essa documentação deverá compor o relatório final da pesquisa. ***(Essa atividade será desenvolvida pelo bolsista com uma carga horária de 20 horas semanais sob a orientação de 02 horas semanais.)***	**X**	**X**	**X**	**X**	**X**	**X**	**X**

5. Resultados Esperados

Espera-se, com o desenvolvimento do projeto, a disponibilização de conhecimentos sobre o método criptográfico RSA visando facilitar o entendimento dos processos de codificação e decodificação de dados envolvidos em seu funcionamento. Isso, por sua vez, poderá viabilizar pesquisas mais aprofundadas sobre o método em questão.

O desenvolvimento desse projeto beneficiará o acadêmico responsável pelo mesmo, propiciando a aquisição de conhecimentos tanto matemáticos quanto computacionais importantes para sua formação, permitindo também a aplicação de conceitos estudados durante o curso de graduação. Esse aluno também irá adquirir experiência no desenvolvimento de pesquisas científicas podendo aplicar os conhecimentos adquiridos em trabalhos posteriores.

6. Título do projeto de pesquisa aprovado pela PROPP/UEMS na condição de coordenador ou colaborador, pelo orientador.

O projeto de pesquisa aprovado pela PROPP/UEMS relacionado com a presente proposta de iniciação científica é intitulado “Um estudo sobre sistemas criptográficos”. Esta proposta de iniciação científica está em conformidade com a atuação da

orientadora e será imprescindível no desenvolvimento do projeto de pesquisa, do qual é coordenadora.

7. Referências bibliográficas

Coutinho, S. C. 2011. *Números Inteiros e Criptografia RSA*. Rio de Janeiro, IMPA/SBM. Rio de Janeiro, 2ª edição.

Crandall, R. and Pomerance, C. 2005. *Prime numbers: A Computacional Perspective*. Springer-Verlag, New York, 2nd edition.

Daemen, J., Rijmen, V. 2002. *The design of Rijndael: AES*. The advanced Encryption Standard. Spring-Verlag.

Diffie, W. & Hellman, M. 1976. *New directions in cryptography*. IEEE Transf. Inform. Theory, n. 22, p. 644 – 654.

Grafinkel, S. and Spafford, G. 2003. *Practical Unix and Internet Security*. O'Reilly and Associates. 3rd edition.

Menezes, A. J., Orschot, P. C., Vanstone, S. A. 1997. *Handbook of Applied Cryptography*. CRC Press.

Koblitz, N. 1987. *Elliptic Curve Cryptosystems*. Math. Comp., n. 28, p. 203-209.

Quaresma, P. e Pinho, A. (2007). Criptoanálise. Gazeta de Matemática, 1(157):22-31.

Rivest, R., Shamir, A. and Adleman, L. 1978. *A method for obtaining digital signatures and public-key cryptosystems.* Comm. ACM, n. 21, p.120-126.

SANTOS, J. P. O. 2007. Introdução na Teoria dos Números. Rio de Janeiro: IMPA. 3ª edicão .