FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE – FANESE

CURSO DE PÓS-GRADUAÇÃO *Lato Sensu*

GESTÃO DE REDES E SEGURANÇA DA INFORMAÇÃO

JOENEAS PEREIRA BARBOSA

A CRIPTOGRAFIA COMO ALIADA DA CONFIDENCIALIDADE DA INFORMAÇÃO

Aracaju

2015

JOENEAS PEREIRA BARBOSA[1]

A CRIPTOGRAFIA COMO ALIADA DA CONFIDENCIALIDADE DA INFORMAÇÃO

Artigo apresentado à Faculdade de Administração e Negócios de Sergipe – Fanese como pré-requisito parcial para obtenção da Especialização em Gestão de Redes e Segurança da Informação.

Aracaju

2015

1 Graduado em licenciatura plena em Matemática e técnico em Informática com ênfase em programação.

RESUMO

Cada vez mais comuns, as redes de computadores desempenham um papel vital nas instituições públicas e privadas. Por isso aumenta-se a preocupação com a segurança das informações transitadas por essas redes. Este artigo científico examina a Criptografia mostrando sua importância para se manter a confidencialidade da informação. A Criptografia camufla a mensagem tornando-se inelegível para um intruso que tentar furtá-la. Veremos os mecanismos da Criptografia de chave privada e da Criptografia de chave pública. Dentro de cada uma abordaremos os algoritmos criptográficos mais utilizados.

Palavras-chave: Criptografia. Criptografia de chave privada. Criptografia de chave pública.

SUMÁRIO

INTRODUÇÃO

A palavra Criptografia tem origem grega e significa escrita escondida. Ao se criptografar uma mensagem, sua leitura e, consequentemente, seu significado, deixam de ser legíveis. Por exemplo, a palavra *amor* poderia ser escrita como *bnps*, usando a lógica de se substituir cada letra por sua sucessora, um método bastante simples de criptografia.

Embora adolescentes costumem usar a criptografia para trocar mensagens ilegíveis para os adultos, o estudo da criptografia tem uma utilização séria no mundo globalizado. Ao passo que a rede mundial de computadores se expande e é utilizada para um leque maior de serviços, cada vez mais informações passam através de vários caminhos até chegarem ao seu devido destinatário.

Dentre todos esses dados e informações estão aqueles que ninguém gostaria que caíssem em mãos erradas, como por exemplo, o número e código de segurança do cartão de crédito, a senha da conta corrente, um produto inédito que será colocado no mercado, a receita secreta de uma bebida campeã de vendas, etc.

A discussão desse tema justifica-se na medida em que o uso de redes de computadores na comunicação em escala mundial tornou-se cotidiano. Ao mesmo surgiu a necessidade de manter tal troca de informação confidencial, protegida contra acesso indevido, alteração e roubo.

Dessa forma, haverá uma menor preocupação ao enviar tais informações sigilosas de forma **criptografada**, de modo que só o destinatário legítimo poderá descriptografar a mensagem recebida. Qualquer terceiro que coletasse tais dados durante o percurso da informação de seu computador ao computador final, obteria apenas um emaranhado de letras e símbolos sem sentido algum. Suas informações continuariam seguras.

Nesse estudo abordaremos os métodos de criptografia mais conhecidos, seus mecanismos e eficiência.

Objetivo Geral:

Descrever os métodos mais comumente utilizados na criptografia.

Objetivos Específicos

- Conceituar Criptografia.
- Diferenciar chave simétrica de assimétrica
- Descrever as técnicas utilizadas na criptografia.
- Avaliar a eficiência dos métodos criptográficos.

Fundamentação teórica

- Conceito de algoritmo criptográfico;
- Conceito de chave criptográfica;
- Algoritmos criptográficos simétricos;
- Algoritmos criptográficos assimétricos;

Metodologia:

- Revisão bibliográfica;
- Abordagem qualitativa.

Criptografia

A partir de 1991, com a disponibilização mundial da World Wide Web, a introdução de sistemas distribuídos e o uso de redes para a troca de informações entre terminais distantes, a segurança da informação demandou novas medidas para a proteção de dados que são transportados através desta rede sem escalas. Tais medidas deveriam permitir que tais informações se mantivessem confidenciais e íntegras.

Conforme SÊMOLA(2004) conceitou,

> "a criptografia é uma ciência que estuda os princípios, meios e métodos para proteger a confidencialidade das informações através da codificação ou processo de cifração e que permite a restauração da informação original através do processo de decifração."(p.122)

A Criptografia permite que o emissor tenha certeza que somente o destinatário legal tenha acesso ao conteúdo de sua mensagem. Também possibilita que o receptor se assegure que aquela mensagem encontra-se em sua forma original, sem alterações.

Para entendermos como isso se processa deveremos ter em mente alguns conceitos:

- Texto claro: é a mensagem legível, antes de ser criptografada;
- Algoritmo de Criptografia: sequência de procedimentos que transformam o texto claro em texto codificado;
- Texto codificado: é a mensagem criptografada, ilegível. Ele é o produto obtido após a aplicação do algoritmo de Criptografia ao texto claro de acordo com uma determinada chave criptográfica;
- Chave criptográfica: é uma sequência de bits utilizada pelo Algoritmo de Criptografia para transformar cada carácter do texto claro em carácter do Texto codificado.
- Algoritmo de descriptografia: faz o inverso do Algoritmo de Criptografia, sequência de procedimentos que transforma o texto codificado em texto claro.

Então para se criptografar uma mensagem é necessário um algoritmo de Criptografia e uma chave criptográfica. E para um mesmo algoritmo de criptografia podem ser usadas várias chaves criptográficas diferentes que produzirão vários textos codificados diferentes. Para que o destinatário legítimo possar entender o Texto Codificado, ele deverá possuir o algoritmo de descriptografia e a chave criptográfica usada pelo emissor.

Os tamanhos das chaves criptográficas são medidos em bits. Podem ser, por exemplo, 32,64,128 e assim por diante. Sabemos que com 8 bits podemos gerar 256 combinações diferentes, pois $2^8 = 256$. A quantidade de combinações torna-se exponencialmente maior com mais bits, aumentado-se as possibilidades e tornando-se mais dificultoso para um terceiro testar todas as possibilidades até conseguir transformar o texto codificado na mensagem original.

Vejamos as 2 principais técnicas criptográficas: criptografia de chaves simétricas e criptografia de chaves assimétricas.

Criptografia de chaves simétricas

Também conhecida como Criptografia de chave privada, é a técnica criptográfica em que usa-se uma única chave criptográfica tanto para a criptografia e como para a descriptografia de um texto claro. Assim, quando o emissor faz a cifragem da mensagem original e envia ao seu destinatário legítimo, também precisa enviar a chave utilizada, para que o destinatário faça o processo de decodificação. Caso o destinatário responda a esta mensagem ele fará a criptografia da resposta usando esta mesma chave e devolvendo a mensagem ao emissor.

Nesta técnica criptográfica, os dois lados da rede de comunicação, emissor e receptor compartilham a chave única, que tanto codifica como descodifica a mensagem. Se, no início da comunicação, quando o emissor original repassa a chave simétrica ao seu destinatário, algum terceiro ilegalmente capturar este fluxo de dados, ele terá posse do segredo para a quebra do sigilo desta troca de mensagens. Em vista dessa possibilidade, uma boa prática é a mudança da chave simétrica a cada período de tempo. Assim a chave capturada ilegalmente só teria um breve período de utilidade.

Um exemplo de algoritmo criptográfico que utiliza chaves simétricas é o Advanced Encryption Standard (AES), conhecido também como Rinjdael em alusão aos nomes de seus criadores, adotado como padrão de Criptografia dos Estados Unidos da América. O tamanho da chave utilizada é de 256 bits, um tamanho que aumenta o nível de segurança da cifragem, pois permite 2^{256} combinações, aproximadamente, 10^{77} de combinações.

Criptografia de chaves assimétricas

Esta técnica criptográfica proposta em 1976 por Diffie e Hellman, foi um avanço revolucionário no campo da Criptografia. Para a sua implementação são necessárias 2 chaves em vez de apenas uma. O par de chaves é composto de uma chave privada e de uma chave pública. A chave pública permitirá a transformação do texto claro em texto codificado, portanto, não requerendo que seja mantida em segredo. Quanto a chave privada, será usada na decodificação da mensagem, por isso não será distribuída publicamente, ficando apenas em poder daquele que possui o direito de ler tal mensagem. Fica claro que para cada chave pública diferente está associada uma chave privada diferente.

Assim, caso dois usuários queiram trocar mensagens através da Criptografia de chaves assimétricas, inicialmente cada um terá de criar seu par de chaves: privada e pública. Em seguida, cada um repassará ao outro, a sua chave pública, a fim de que o outro consiga criptografar a mensagem. Note que eles não precisarão enviar a chave privada pela rede de comunicação, porque esta chave estará somente com o legítimo receptor da informação, o único com o direito de descriptografar tal mensagem. Resumindo, qualquer pessoa pode fazer a cifragem da mensagem, isso é público; enquanto que só uma pessoa poderá lê-la, ou seja, possuirá a chave privada para a descriptografia.

Pelo seu mecanismo de processamento a Criptografia de chave pública, chega a consumir centenas ou milhares de vezes mais tempo que a Criptografia de chave privada ou de chave simétrica. Vale lembrar que criptografia de chave privada não tornou-se obsoleta com a chegada da Criptografia de chave pública.

Vejamos uma aplicação bastante comum da técnica criptográfica de chaves públicas.

Assinatura Digital

Este recurso permite que um usuário tenha certeza da identidade do emissor de determinada mensagem recebida. Partindo do princípio de que a chave privada não foi descoberta ou furtada, quando o receptor consegue decodificar a mensagem em texto claro, ele tem certeza que a mensagem foi realmente emitida pelo usuário esperado. Pois do contrário, se a mensagem fosse emitida por um terceiro agindo como impostor, no momento da descriptografia, não se obteria um texto legível. Isso aconteceria, visto que o par de chaves privada e pública funcionam em conjunto, uma decodifica perfeitamente o que a outra codifica.

Com a Assinatura Digital, também garante-se que a mensagem não foi adulterada, já que não é possível alterar a mensagem de maneira legível sem acessar a chave privada pertencente ao emissor. Portanto, podemos dizer que a assinatura digital valida o autor da mensagem e o seu conteúdo.

Outro benefício da Assinatura Digital, é o chamado não-repúdio ou irretratabilidade. O emitente não pode alegar que não emitiu tal mensagem, pois sua assinatura digital está presente.

Vejamos como funciona o algoritmo RSA, que utiliza criptografia de chave pública.

RSA (Rivest, Shamir and Adleman)

Trata-se de um algoritmo que usa chaves assimétricas, que leva como nome as iniciais dos sobrenomes de seus criadores: Ron Rivest, Adi Shamir e Len Adleman. Tal algoritmo baseia-se em teorias clássicas dos números, envolvendo números primos[2] e aritmética modular[3]. Nele dois números primos escolhidos são multiplicados, obtendo-se um produto. Porém fazer o contrário, a partir do produto descobrir os dois números primos multiplicados torna-se uma tarefa árdua, principalmente se forem dois números primos com muitos dígitos. Vejamos como ela funciona.

i. Escolha dois números primos: $\mathbf{p_1}$ e $\mathbf{p_2}$;
ii. Calcule $\mathbf{n} = \mathbf{p_1} \times \mathbf{p_2}$;
iii. Calcule $\mathbf{z} = (\mathbf{p_1}\text{-}1) \times (\mathbf{p_2}\text{-}1)$;

2Veja o apêndice: Números primos.
3Veja o apêndice: Aritmética modular.

iv. Escolha um número inteiro **e** que seja maior que 1 e menor que **z**, além de ser relativamente primo com **z**;
v. Calcule **d** usando a equação **de** ≡ 1 mod (**z**);

Assim, temos uma chave pública: {**n,e**} e uma chave privada: (**n,d**}.

Para transformar uma mensagem **M (M<n)** em uma mensagem codificada **C** basta resolver a equação: $\mathbf{C} \equiv \mathbf{M}^{\mathbf{e}} \bmod (\mathbf{n})$.

Para decodificar a mensagem é necessário resolver a equação $\mathbf{M} \equiv \mathbf{C}^{\mathbf{d}} \bmod (\mathbf{n})$.

Exemplificando, imagine que Obama queira receber uma informação secreta de Dilma. Obama então escolhe sigilosamente dois números primos 5 e 11($\mathbf{p_1}$ e $\mathbf{p_2}$), encontra 5x11= 55 (**n**); calcula também **z** = (5-1)x(11-1) = 40. Escolhe um número inteiro **e** que seja relativamente primo com 40 e que seja menor que ele, por exemplo, **e** = 9; e finalmente escolhe **d** que atenda a equação **d** x 9 ≡ 1 mod (40), encontrando **d** = 49.

A chave pública será {9,55} e a chave privada será {49,55}. Obama então repassará à Dilma a chave pública {9,55}.

Vejamos como ela poderia passar o seguinte dado: 13 (o dado precisa ser menor que 55 (n)). Como os dois já conhecem o algoritmo RSA, para Dilma criptografar o dado 13, usará a fórmula $\mathbf{C} \equiv \mathbf{M}^{\mathbf{e}} \bmod (\mathbf{n})$, ou seja, $\mathbf{C} \equiv 13^9 \bmod (55)$, C = 28, e repassará então a Obama o dado criptografado 28.

Ao receber 28, ele usará a fórmula decodificadora $\mathbf{M} \equiv \mathbf{C}^{\mathbf{d}} \bmod (\mathbf{n})$, $\mathbf{M} \equiv \mathbf{28}^{\mathbf{49}} \bmod (\mathbf{55})$, encontrando **M** = 13.

A segurança deste algoritmo cresce exponencialmente ao passo que se escolhe os dois números primos iniciais bastante grandes. Atualmente se escolhe números de 300 dígitos para se ter uma chave suficientemente forte. Em nosso exemplo usamos os pequeninos números primos 5 e 11.

CONCLUSÃO

Após a nossa explanação a respeito da Criptografia de chave privada e a Criptografia de chave pública, é importante frisar que uma não é mais segura que a outra, ou mais obsoleta. Ambas encontram sua utilidade em nossa atualidade. Sabemos que a criptografia assimétrica demanda maior poder computacional para a sua implementação, que é uma medida prática de segurança na criptografia simétrica a troca frequente de chaves e que a segurança de determinada técnica criptográfica depende diretamente do tamanho de sua chave. Inclusive hoje em dia o tamanho mínimo de uma chave deve ser de 128 bits. As duas técnicas não raro são combinadas como medida de segurança da informação.

Uma das técnicas mais recentes no campo da Criptografia é a Criptografia quântica, que seria aplicada exclusivamente para a distribuição de chaves simétricas com maior segurança. Sua principal vantagem é que ela não perde sua efetividade mesmo que um terceiro tenha poder de processamento ilimitado. A Criptografia quântica usa fótons em vez de bits, e explora certas propriedades do estado quântico como medida de segurança, como o Princípio da Incerteza de Heisenberg[4], que nos assegura ser impossível saber todos os estados físicos de uma partícula simultaneamente. Trata-se de um campo promissor na Criptografia, com amplo espaço para pesquisa e desenvolvimento.

4Veja o anexo: Princípio da incerteza de Heinsenberg.

REFERÊNCIAS

Advanced Encryption Standard. Disponível em: <http://pt.wikipedia.org/wiki/Advanced_Encryption_Standard> Acesso em 4 de Abril de 2015.

Criptografia. Disponível em: <http://pt.wikipedia.org/wiki/Criptografia> Acesso em 4 de Abril de 2015.

Criptografia. Disponível em: <http://www.infowester.com/criptografia.php> Acesso em 4 de Abril de 2015.

Criptografia quântica. Disponível em: <http://pt.wikipedia.org/wiki/Criptografia_qu%C3%A2ntica> Acesso em 4 de Abril de 2015.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. *Política de Segurança da Informação – Guia Prático para Elaboração e Implementação*. 2ª edição revisada. Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.

GONÇALVES, Adilson. *Introdução à Álgebra*. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2003.

Princípio da incerteza de Heisenberg. Disponível em: <http://pt.wikipedia.org/wiki/Princ%C3%ADpio_da_incerteza_de_Heisenberg> Acesso em 4 de Abril de 2015.

RSA. Disponível em: <http://pt.wikipedia.org/wiki/RSA> Acesso em 4 de Abril de 2015.

SÊMOLA, Marcos. *Gestão da segurança da informação: uma visão executiva*. 2ª edição. Rio de Janeiro: Editora Elsevier, 2004.

STALLINGS, William. *Redes e sistemas de comunicação de dados: teorias e aplicações corporativas*. 5ª reimpressão. Rio de Janeiro: Editora Elsevier, 2005.

APÊNDICE

A – Números primos

Dizemos que um número inteiro ***p*** é primo, se for diferente de 1, e possuir unicamente dois divisores: ele mesmo e o número 1.

B – Aritmética modular

Dizemos que um número ***p*** atende a equação $\mathbf{p} \equiv \boldsymbol{q} \bmod (\boldsymbol{m})$ (lê-se p é congruente a q módulo m), se (***p-q***) é divisível por ***m.***

Uma propriedade que ajuda bastante os cálculos é a seguinte:

$\mathbf{X} \equiv \mathbf{M}^{\mathbf{a+b+c}} \bmod (\mathbf{n})$

$\mathbf{M}^{\mathbf{a+b+c}} \bmod (\mathbf{n}) = [(\mathbf{M}^{\mathbf{a}} \bmod (\mathbf{n})) \times (\mathbf{M}^{\mathbf{b}} \bmod (\mathbf{n})) \times (\mathbf{M}^{\mathbf{c}} \bmod (\mathbf{n}))] \bmod (n).$

Por exemplo:

$\mathbf{X} \equiv \mathbf{2}^{7} \bmod (\mathbf{5})$

$\mathbf{2}^{7} \bmod (\mathbf{5}) = [\mathbf{2}^{4} \bmod (\mathbf{5}) \times \mathbf{2}^{2} \bmod (\mathbf{5}) \times \mathbf{2}^{1} \bmod (\mathbf{5})] \bmod (5) =$

$= [16 \bmod (5) \times 4 \bmod (5) \text{ X } 2 \bmod (5)] \bmod (5) =$

$= [1 \times 4 \times 2] \bmod (5) =$

$= 8 \bmod (5) =$

$= 3$

ANEXOS

A – Princípio da incerteza de Heinsenberg

O Princípio da incerteza de Heinseberg consiste num enunciado da mecânica quântica, formulado inicialmente em 1927 por Werner Heinsenberg, impondo restrições à precisão com que se podem efetuar medidas simultâneas de uma classe de pares observáveis em nível subatômico. (Fonte: Wikipedia).