Criptografia e PGP

Fernando J. Carmo, Pedro A. Lemes, Tiago H. Freitas

Faculdade de Tecnologia de Guaratinguetá
Guaratinguetá – SP – Brasil

fdesenvolvedor@hotmail.com, pedro.lemes@gmail.com
tiagofreitas12@gmail.com

Abstract. *This article aims to present a definition of encryption, introducing a brief history and contextualizing it within the area of Information Technology. The main focus of this paper is the encryption software known as PGP and its derivatives, widely used today. Will be introduced a concept about the history and implementation of PGP, and a small tutorial on its use in practice.*

Resumo. *Este artigo tem por objetivo apresentar uma definição sobre criptografia, introduzindo um breve histórico e contextualizando-a dentro da área de Tecnologia da Informação. O foco principal deste documento é o software de criptografia conhecido como PGP e seus derivados, amplamente utilizados atualmente. Será introduzido um conceito sobre a história e aplicação do PGP, além de um pequeno tutorial de sua utilização na prática.*

1. Conceito e breve histórico da Criptografia

Desde o advento da Tecnologia da Informação, diversas ferramentas vêm sendo desenvolvidas ou adaptadas para aperfeiçoar os métodos de proteção que visam garantir a Segurança da Informação, uma das áreas mais importantes da TI. Entre esses diversos métodos, encontra-se a criptografia, que por definição é o estudo da transformação do texto claro ou aberto em texto não legível (cifrado). A palavra Criptografia é derivada das palavras gregas “Kryptos” que significa “secreto” e “Graphein” que significa “escrita”. É comum que a criptografia seja confundida com criptoanálise (a tentativa de descobrir um texto cifrado) e criptologia (estudos matemáticos, computacionais, psicológicos entre outros, necessários à criptoanálise e criptografia).

Apesar de ser uma ferramenta amplamente utilizada no mundo contemporâneo, a criptografia possui origem milenar, tendo sido utilizada inclusive no Antigo Egito, cerca de 1900 A.C. onde há relatos de sua primeira aplicação de forma documentada. Os egípcios aplicavam a criptografia desenhando hieróglifos fora dos padrões.

Com o passar dos séculos, diversas técnicas de criptografia foram sendo desenvolvidas pelas nações, tornando-se também uma importante ferramenta militar na transmissão de mensagens confidenciais, como exemplo dessa aplicação, pode-se citar a máquina Enigma G, inventada na Alemanha na década de 20.

Já no início da criptografia na Era da Informação, o primeiro importante marco desta ferramenta foi o advento da criptografia DES (Data Encryption Standard) em 1976, por uma equipe da organização IBM.

O DES foi um dos principais padrões de criptografia a serem utilizados pelo governo dos Estados Unidos, tendo sido aplicado entre a década de 70 e o final da

década de 90, quando foi substituído por um novo padrão conhecido como AES (Advanced Encryption Standard), mais complexo e também considerado mais seguro.

2. Chaves criptográficas

Para uma melhor compreensão de como funciona um sistema de criptografia, é importante conhecer inicialmente o conceito das chaves criptográficas, que são utilizadas para realizar a encriptação de uma mensagem simples (inteligível) ou a decriptação de uma mensagem codificada. A chave é responsável por controlar o algoritmo que fará a conversão do texto, e é formada por uma combinação de bits (0 ou 1). Uma chave de 8 bits possui um total de 256 combinações diferentes de valores 0 e 1 que cada bit pode assumir. Considera-se que, quanto maior o número de bits de uma chave, mais segura ela será, pois haverá um aumento considerável no número de combinações de bits, tornando impossível o cálculo de todas as possibilidades por um ser humano, e demorado para uma máquina.

Estas 256 possibilidades de chaves diferentes dentre as quais podemos escolher uma, é chamado de *keyspace* de 8 bits.

Supondo que uma criptografia possibilite 65536 combinações de chaves (ao invés de 256 combinações), teremos um keyspace de 16 bits. Note que o número de chaves possíveis é 256 vezes maior que o keyspace de 8 bits, enquanto que a chave propriamente dita é apenas 8 bits maior (duas vezes maior).

Um exemplo que simplifica o entendimento de chave criptográfica é a comparação de uma chave pertencente ao padrão DES com uma do padrão AES. Onde o primeiro, em sua versão primitiva, possuía uma chave de apenas 56 bits e o segundo possui chaves de 128, 192 ou 256 bits. Essa comparação demonstra que a criptografia DES em sua primeira versão pode ser considerada fraca frente à criptografia AES, muito mais difícil de ser decifrada.

2.1 Chave simétrica

A chave simétrica é aplicada em padrões de criptografia simples, onde uma mesma chave é utilizada tanto para realizar a encriptação de uma mensagem quanto para a sua decriptação. É considerada vulnerável, pois exige que o emissor de uma mensagem confidencial criptografada repasse sua única chave para os destinatários de sua mensagem, a fim de que possam realizar o processo inverso e entender o conteúdo da mensagem, também possui a desvantagem de não garantir autenticidade. No processo de distribuição da chave, existe o risco de sua interceptação, fazendo com que todo o processo de segurança possa se tornar inútil. Há também uma necessidade de constante troca dessa chave única, para possibilitar um aumento na segurança das trocas de informação.

Alguns exemplos de algoritmos que utilizam chave simétrica são: DES, IDEA e RC.

Figura 1. Chave simétrica

2.2 Chave assimétrica

O mecanismo da chave assimétrica utiliza um par de diferentes chaves (chave pública e chave privada) que são utilizadas para cada etapa do processo de criptografia. Para a encriptação de uma mensagem, é utilizada a chave pública, para a decriptação é utilizada a chave privada. Desta forma, um remetente que deseja enviar uma mensagem cifrada, deve criar em primeiro plano essas duas chaves, enviando sua chave pública para os destinatários de sua mensagem e mantendo a chave privada para si. Esse sistema de chaves é considerado seguro, pois garante autenticidade e confidencialidade.

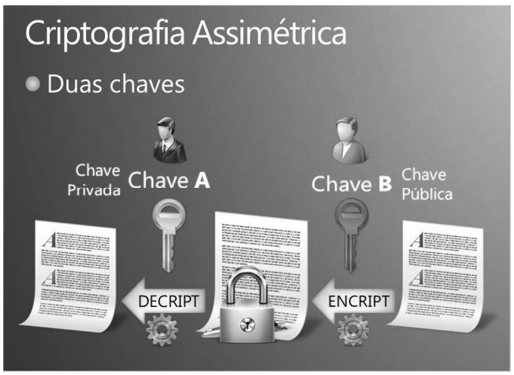

Figura 2. Chave assimétrica

Na figura acima observa-se o processo de utilização das chaves, onde um emissor de uma mensagem criptografada deve possuir a chave pública do destinatário, a fim de realizar a encriptação da mensagem, após o envio da mesma, o destinatário deve utilizar sua chave privada para decodificar a mensagem. Esse sistema garante que uma mensagem cifrada somente será lida pelo destinatário desejado.

Alguns exemplos de algoritmos que utilizam chave simétrica são: RSA, ELGALAM e DSS.

3. Histórico do PGP

O Pretty Good Privace foi criado no início da década de 90 e muitas vezes é confundido como um algoritmo de criptografia, um conceito equivocado. O PGP é um software inicialmente desenvolvido por Phil Zimmermann nos Estados Unidos, que adaptou conceitos já existentes da criptografia, no intuito de criar um sistema de fácil utilização, possibilitando até mesmo para uma pessoa comum a utilização da criptografia em seu dia-a-dia, desde que tivesse em mãos um computador.

Devido às diversas questões relacionadas à lei americana que estavam em discussão na época (o governo dos EUA, que não gostou de ver um sistema que permitia a qualquer um se comunicar sem risco de ser monitorado pelas agências governamentais. Depois de responder a vários processos, Zimmermann acabou inocentado.), Phil teve de driblar restrições que o impediam de compartilhar este software além das fronteiras norte-americanas, tendo que distribuir um livro com o código-fonte de sua criação, ao invés de distribuir o próprio software. Desta forma, o PGP começou a angariar usuários ao redor do mundo, principalmente devido ao fato de Zimmermann ter passado por problemas judiciais com a sua distribuição.

Como o PGP utiliza algoritmos de criptografia patenteados, ele se transformou em seguida em um sistema fechado, e em 1998 a empresa de Zimmermann, PGP Corporation lançou um sistema totalmente livre para usuários que dispensam a necessidade de pagar pelo software, chamado OpenPGP.

Os dois sistemas se diferenciam em características como suporte, algoritmos de criptografia e transparência (código-fonte).

Em 1999, a Free Software Foundation desenvolveu o GNU Privacy Guard (GPG), sistema que se popularizou rapidamente, e atualmente possui diversas interfaces gráficas que podem ser utilizadas com o mesmo, já que é um sistema de linha de comando. Dentre as interfaces gráficas que trabalham com GPG, uma das mais utilizadas é o WinGPG, software de fácil usabilidade e que será utilizado nos exemplos deste artigo.

É importante destacar que, o sistema GPG é totalmente compatível com o seu predecessor OpenPGP, desta forma, caso o emissor de uma mensagem utilize um sistema, e seu receptor o outro, não haverá problemas na transmissão da mesma.

4 Os pilares do PGP

Os PGP é baseado em três pilares que juntos garantem a autenticidade de uma determinada mensagem. Estes pilares são: Confidencialidade, Integridade e Não Repúdio.

4.1 Confidencialidade

Visa garantir que ninguém que não possua as chaves criptográficas possa visualizar o conteúdo de uma determinada mensagem. Esse pilar define o segredo que a mensagem cifrada se torna ao esconder o texto simples. Não é difícil que uma mensagem seja interceptada durante a sua transmissão, o PGP deve impedir que o conteúdo da mesma seja inteligível para quem não deve.

4.2 Integridade

Este pilar estabelece de que uma mensagem não sofrerá alterações durante a sua transmissão, a forma que ela foi enviada será exatamente a forma que ela será recebida. O sistema OpenPGP possui um mecanismo de notificação que avisa o destinatário caso a mensagem tenha sofrido alguma alteração após o seu envio.

4.3 Não repúdio

Este fundamento procura evitar que uma mensagem recebida com a assinatura digital do remetente não possa ser negada por ele, em outras palavras, a partir do momento em que se assina digitalmente uma mensagem com uma chave privada, está sendo comprovado de que o remetente da mensagem é a mesma pessoa que a escreveu, e ela não pode repudiar este fato. É recomendável que as mensagens cifradas sempre sejam assinadas digitalmente para prevenir possíveis tentativas de envio de mensagens falsas.

4.4 Autenticidade

A união dos três pilares descritos acima, se aplicada de forma correta numa transmissão de mensagem, garante a autenticidade da mesma, ou seja, o destinatário pode ter certeza de que foi alguém conhecido que lhe enviou a mensagem, através da assinatura, pode comprovar que a mensagem não foi vista em sua transmissão ou adulterada.

O PGP é muito utilizado em mensagens enviadas via e-mail, tanto que boa parte de seus softwares derivados possuem plug-ins para se adaptarem aos gerenciadores de e-mail de seus usuários.

5 PGP na prática

Os softwares baseados em PGP trabalham com o sistema de chaves assimétricas. Quando um usuário inicia o sistema, é solicitado que assimile uma conta de e-mail às suas chaves criptográficas (pública e privada). Este processo é bem simples, e o sistema gera as chaves automaticamente. Além das chaves, o usuário terá de registrar uma palavra-chave, que será utilizada sempre que o usuário quiser realizar uma operação de decodificação de mensagem ou de aplicação de assinatura digital para uma determinada chave pública de outro usuário. Neste exemplo, foi utilizado a interface gráfica de GPG chamada WinGPG.

Ao terminar o processo de registro no sistema, o usuário poderá fazer na tela principal o gerenciamento de chaves públicas de outros usuários e de sua própria chave. Os três principais botões a serem utilizados para um envio ou recebimento de mensagem criptografada serão: *Import*, *Export* e *Clipboard*.

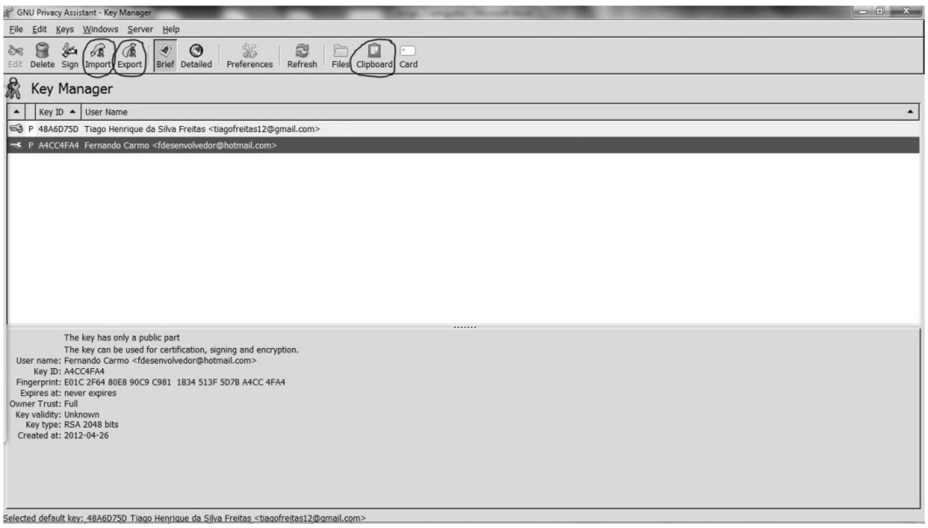

Figura 3. Tela principal do WinGPG

Para poder enviar uma mensagem cifrada, o usuário terá de importar (*Import*) a chave pública do usuário de destino da mensagem. Este por sua vez, deve exportar a sua chave pública (Export) em um arquivo e enviá-lo para os usuários de quem deseja receber mensagens. Neste arquivo gerado pelo software, há um texto cifrado que é efetivamente uma chave pública.

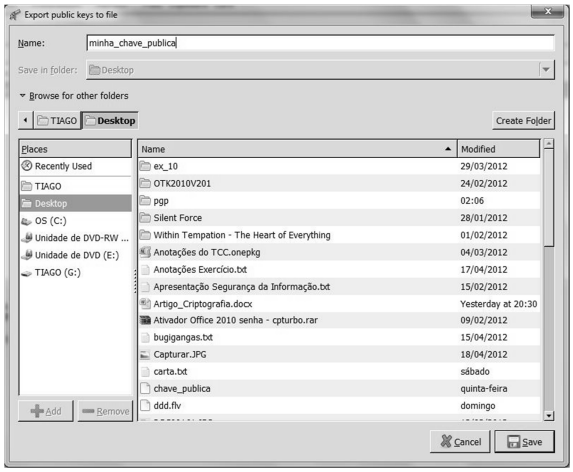

Figura 4. Tela de exportação da chave pública

Dentro da janela *Clipboard*, o usuário poderá digitar seu texto simples, ou colá-lo de algum editor de texto. Ao término da construção da mensagem, bastará clicar no botão *Encrypt* e selecionar qual das chaves públicas previamente importadas deve ser utilizada para criptografar o texto, lembrando que essa escolha depende de qual é o usuário destinatário da mensagem.

Figura 5. Tela de edição e encriptação de texto

Ao término da encriptação da mensagem, bastará ao usuário selecionar o texto cifrado e copiá-lo para sua página de envio de e-mail e enviá-lo.

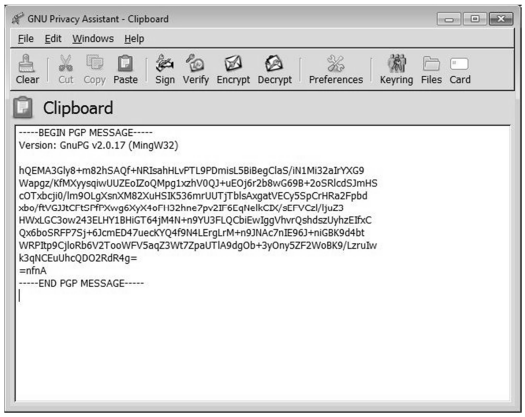

Figura 6. Texto criptografado

O usuário receptor desta mensagem deverá seguir os mesmos passos, com exceção de que, na tela Clipboard, ele deverá colar o texto e utilizar o botão Decrypt, selecionando em seguida sua chave privada para a efetivação do processo, será necessário auditar a utilização desta chave através da confirmação da palavra-passe, previamente cadastrada.

6 Conclusão

Através do estudo realizado para a confecção deste artigo, foi possível compreender a tamanha importância da utilização da Criptografia como uma ferramenta de confidencialidade, não apenas na Segurança da Informação em TI, como também fora dela, como foi visto no breve histórico descrito. Pode-se concluir que a TI tornou a utilização da criptografia uma ferramenta não apenas de uso militar ou para super máquinas, mas também para usuários comuns que necessitem de uma maior confidencialidade e autenticidade em suas trocas de informações. Esta abertura que o PGP proporcionou à sociedade é de extrema importância, e garantirá desta forma que com o passar dos anos, todos poderão contribuir para a evolução do estudo da criptografia.

Foi visto também a facilidade na utilização de um sistema baseado no PGP, indicando que estes tipos de software possuem interface amigável e de fácil manuseio, fazendo que poucas etapas garantam a proteção de uma determinada informação.

Assim, podemos afirmar que a criptografia pode garantir um segredo, garantir que uma mensagem não foi alterada enquanto em trânsito, implicitamente, autenticar o remetente da mensagem. Da mesma forma, a criptografia definitivamente não pode proteger contra informantes, espionagem, grampos, evidencia fotográfica ou delação.

Fica claro que a criptografia é apenas uma pequena parte do conjunto de proteções e cuidados necessários para a garantia de um segredo absoluto.

7 Referências

Lucas, M. W. (2006), PGP & GPG: email for the pratical paranoid, No Starch Press, 1ª edição.

Castelló, T. e Vaz, V. “Assinatura Digital”, http://www.gta.ufrj.br/grad/07_1/ass-dig/TiposdeCriptografia.html.

Alecrim, E. (2009) “Criptografia”, http://www.infowester.com/criptografia.php.

Ritter, T. (1999) “Aprendendo Criptografia: Uma introdução básica às cifras Cripto A”, http://pt.scribd.com/doc/7086265/Aprendendo-Criptografia