Uso de Webservices Criptográficos a partir de Dispositivos Móveis

Daniel Melo[1]

[1]Instituto de Informática – Universidade Federal de Goiás
Alameda Palmeiras, Quadra D, Câmpus Samambaia
CEP 74690-900 – Goiânia – GO – Brasil

danielmelo@inf.ufg.br

Abstract. *This meta-paper describes the style to be used in articles and short papers for SBC conferences. For papers in English, you should add just an abstract while for the papers in Portuguese, we also ask for an abstract in Portuguese ("resumo"). In both cases, abstracts should not have more than 10 lines and must be in the first page of the paper.*

Resumo. *A criptografia é uma técnica muito conhecida por usuários de software mais experientes, mas pouco difundida dentre os demais. O desenvolvimento das ferramentas e técnicas não tem sido suficiente para assegurar a sua adoção por grandes grupos de usuários. Isso se deve, em grande parte, à dificuldade de uso dessas ferramentas. Neste trabalho avaliamos o cenário de adoção da criptografia e propomos um modelo mais próximo da experiência do usuário final, utilizando dispositivos móveis como facilitadores das experiências ligadas à segurança da comunicação que usam essa tecnologia.*

INTRODUÇÃO

Um dos grandes desafios das aplicações modernas está na sua capacidade de manter a segurança dos dados de seus usuários. Um dos pilares da segurança da informação é a confidencialidade, que é manter aquilo que é privado acessível somente a quem é de direito, identificando de forma inequívoca as partes envolvidas e suas ações no seu sistema de informação. Outro conceito importante é o da integridade, que busca afirmar com precisão se determinado conteúdo se mantém sem modificações inapropriadas[Smith 2005].

Um recurso voltado para essas necessidades é a criptografia, capacidade de mascarar uma mensagem de tal forma que somente seja legível pelo destinatário. Também traz a possibilidade de assinar digitalmente os conteúdos das mensagens, sendo possível verificar posteriormente quem assinou e se o conteúdo não sofreu alteração depois disso. O uso crescente de ferramentas sociais para comunicação entre as pessoas em ambientes diversificados traz a necessidade da garantia de privacidade de forma efetiva e fácil de usar.

Apesar do uso de tais técnicas de segurança ser conhecido há muitos anos [McDonald 2009] (com a criptografia datando de 1900 A.C [McDonald 2009] e a criptografia assimétrica de 1975 [Diffie 1988]) - ele ainda é de difícil compreensão e uso para usuários finais. Visto que a facilidade de uso precede uma adoção em massa de qualquer tecnologia [Sweikata et al. 2009], existe necessidade de desenvolver formas mais simples de uso para potencializar ações de segurança da informação.

Este artigo faz uma análise do uso atual de criptografia de chaves assimétricas com PGP para troca de mensagens em algumas ferramentas e propõe um formato simplificado da gestão dos recursos privados usando webservices criptográficos oferecidos em dispositivos móveis. O objetivo principal é simplificar seu uso pelo usuário final e potencializar o uso de criptografia fim a fim.

LIMITAÇÕES DE COMUNICAÇÃO SEM CRIPTOGRAFIA FIM A FIM

A criptografia fim a fim é definida pela implementação de técnicas que garantam que somente o remetente e o destinatário tem acesso às mensagens trocadas, sendo computacionalmente inviável que alguém leia as mensagens, seja por meio de interceptação, seja por acesso indevido aos dispositivos físicos envolvidos. Esse tipo de criptografia não tem sido historicamente desenvolvida com foco no usuário final [Sheng et al. 2006].

Parte significativa da confidencialidade na troca de mensagens reside atualmente na criptografia das mensagens em trânsito através da rede. Isso é feito usando algum protocolo baseado em SSL/TLS, sigla para os padrões Secure Socket Layer e Transport Layer Security [Naylor et al. 2014]. São exemplos o HTTPS, SMTPS, para troca de hipertexto e e-mail, respectivamente. Essa estratégia busca proteger as partes envolvidas de ataques contra o sigilo das mensagens, uma vez que o conteúdo interceptado de forma indevida durante o trânsito se torna inelegível para o atacante. Também torna computacionalmente complexo introduzir nas mensagens conteúdo não legítimo.

Apesar da elevada proteção contra interceptação, estes meios não buscam resolver o problema de somente o remetente e o destinatário da mensagem poderem lê-la. No caso de provedores de e-mail comerciais, como o Gmail, Yahoo Mail e Outlook Mail o mantenedor do serviço ainda tem acesso ao conteúdo das mensagens à revelia da vontade de sigilo do usuário[Rushe 2013]. Cria-se a necessidade de confiar no provedor de e-mail para trocar uma mensagem sigilosa, o que não é suficiente em contextos sensíveis.

A criptografia assimétrica propõe um modelo de solução para este problema. Cada usuário gera um par de chaves criptográficas, sendo uma de propósito privado e a outra pública. A chave privada é usada para assinar e descriptografar as mensagens. A chave pública, por sua vez é usada para verificar assinaturas e criptografar as mensagens, que só poderão ser lidas por quem possuir a chave privada equivalente. Isso cria um mecanismo onde somente o destinatário pode ler as mensagens, promovendo a confidencialidade. Além disso, a capacidade de assinatura provê o recurso de não-repúdio e integridade da comunicação. Se esses recursos forem empregados na troca de mensagens temos um exemplo de criptografia fim a fim.

O chaveiro criptográfico tem como funções a proteção das chaves privadas, a importação de chaves públicas alheias, revogação de chaves comprometidas e configuração do nível de confiança. Sendo a camada responsável por estas tarefas, está fortemente ligado à facilidade de uso das chaves pelo usuário final. O chaveiro desempenha a função crucial de proteção das chaves privadas por meio de senha. A solução adotada em implementações como o GnuPG cria um chaveiro na estação de trabalho do usuário durante a instalação, que pode então ser usado diretamente por meio de linha de comando ou acessado por através de bibliotecas específicas por softwares de terceiros.

USO DO PGP PARA CRIPTOGRAFIA

PGP é uma família de softwares da área de segurança desenvolvidos inicialmente por Philip R. Zimmermann [Carmo et al.] e liberada como um freeware em 1991. Essa liberação foi motivo de processos movidos pelo Governo dos Estados Unidos sob a acusação da ferir as leis de exportação de tecnologia criptográfica vigentes. O caso foi encerrado em 1996 sem prejuízo à Zimmermann [Zimmermann 1996].Foi então fundada a PGP Inc - mais tarde PGP Corp - com o objetivo de manter essa tecnologia. Esta empresa foi adquirida em 2010 pela Symantec e sua versão gratuita deixou de ser oferecida.

Tendo como base esta experiência foi desenvolvido o padrão OpenPGP, que contém a mesma proposta de criptografia por meio de chaves assimétricas, uma pública e outra privada, mas agora com uma especificação publicada na RFC 4880 - OpenPGP Message Format. A publicação desta especificação permitiu o nascimento de implementações abertas. A mais conhecida para desktop é a GNUPG, ou simplesmente GPG, tanto que, por vezes, os termos PGP e GPG são usados de forma intercambiável.

PGP permite criptografar e assinar mensagens trocadas entre duas pessoas utilizando tecnologia de chaves assimétricas, sendo uma de finalidade pública e outra privada.

Esse formato de comunicação estabelece o sigilo da mensagem e o não-repúdio [Lehtonen and Parssinen 2002] - incapacidade de uma das partes de negar que assinou a mensagem se, de fato, o fez - da mensagem, tudo isso mantendo as chaves privadas - o recurso que guarda o poder de assinar e, portanto, de identificação - em sigilo.

Essa tecnologia encontrou um forte caso de uso nas trocas de e-mail, impedindo que a interceptação das mensagens comprometesse seu sigilo e, que um terceiro pudesse se passar por um dos interlocutores de forma despercebida ou, ainda, que um dos interlocutores mais tarde negasse que ele assinou a mensagem.

Outro uso facilmente identificável é na assinatura de arquivos. Dado que uma assinatura precisa da senha do chaveiro do usuário somada à posse da chave privada ela pode ser usada com propósitos legais na assinatura de documentos digitais.

GPG está disponível para todos os grandes sistemas operacionais, de estações desktop até celulares e várias bibliotecas permitem desenvolvimento sobre esta tecnologia.

AVALIAÇÃO DE FORMAS DE ACESSO AO CHAVEIRO PGP

A seguir, são feitas avaliações de formas e metodologias de acesso aos chaveiros PGP, suas dependências e considerações a respeito da facilidade de uso pelo usuário final.

PGP - PRETTY GOOD PRIVACY

Hoje o PGP compõe a suite de soluções corporativas da Symantec servindo como opção de criptografia em seus produtos [Symantec 2015]. Tais produtos compõem um ecossistema de softwares com foco na centralização dos recursos privados, como as chaves dos usuários, o que tira do usuário individual a posse sobre a sua chave, sua ativação e desativação, em prol da facilidade para o administrador da infraestrutura corporativa.

O fato de estas ferramentas somente estarem disponíveis dentro de uma grande suíte corporativa as torna financeiramente inacessíveis às aos indivíduos que desejam proteger suas comunicações e documentos digitais particulares. O fator financeiro, portanto, se torna uma barreira quanto à estes produtos. A adoção de ferramentas livres possivelmente terá mais potencial de adoção, visto o custo envolvido.

GNUPG

O GNU PG é uma implementação da RFC4880 [Callas et al. 2007], entitulada OpenPGP Message Format, que permite a geração e uso das chaves privadas em interface de linha de comando. Essa é a principal implementação do formato em uso atualmente, vindo instalada por padrão em várias distribuições linux. Também está disponível para Microsoft Windows por meio da suite Gpg4win.

Essa implementação é de interesse de quem deseja aprender com mais detalhes como se dá o uso das chaves, sua criação e as diferentes opções de configuração que estão disponíveis nas diversas operações previstas pela especificação. Isso pode ser visto na capacidade de suporte à diversos algoritmos de criptografia, como DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 e TIGER. Também comporta a adição de novos algoritmos por meio de extensões personalizadas.

MOD_AUTH_OPENPGP E ENIGFORM

A extensão Enigform [REF15] para firefox busca adicionar uma nova camada de segurança sobre as requisições HTTP assinando-as digitalmente com os recursos do chaveiro do usuário. O servidor então pode verificar a validade dessas assinaturas por meio do uso do seu próprio chaveiro, através da extensão mod_auth_openpgp [REF16].

Isso provê uma capacidade de autenticação dentro da própria comunicação estabelecida entre a aplicação cliente e o servidor, já que requisições sem assinatura ou com assinaturas geradas por chaves desconhecidas seriam facilmente identificáveis e poderiam ser adequadamente tratadas.

Essa iniciativa ainda se encontra em desenvolvimento e com a proposta de RFC em elaboração. Apesar disso, a proposta adiciona uma facilidade de uso interessante paras as comunicações baseadas em HTTP: é possível arquitetar aplicações de tal forma que seções de conteúdo restrito e/ou sensível possam ser disponibilizados sem autenticação por meio de formulários ou logins integrados à outras plataformas.

O investimento neste tipo de estratégia tem potencial para uso em ferramentas de comunicação corporativas e acadêmicas. Note-se, porém, que não lida com o mascaramento da informação em trânsito, uma vez que se limita ao escopo de autenticação via assinatura por chave privada.

Um outro empecilho é a necessidade de instalação de um plugin em cada estação de trabalho, que obrigatoriamente deve ter o Mozilla Firefox. Essa ferramenta também depende de as chaves serem transportadas entre as estações pelo próprio usuário e disponibilizadas de forma correta em seus discos-rígidos.

ENIGMAIL

O Enigmail é um plugin desenvolvido para o cliente de e-mail Mozilla Thunderbird. Este plugin estende as capacidades do Thunderbird dando-lhe a capacidade de encriptar, des-

encriptar, assinar e verificar assinatura de e-mails. O recurso padrão para estas operações é o padrão PGP, através de uma implementação aberta, o GNU PG.

Para correto funcionamento do Enigmail deve ser feita a instalação do chaveiro GNU PG e do Thunderbird. Em seguida, o chaveiro local deve ser configurado dentro do plugin. Depois disso é possível realizar as operações citadas com as mensagens, provendo sigilo e confirmação da autoria das mensagens, além de operações sobre o próprio chaveiro, como criação de novas chaves, importação de chaves públicas, modificação do nível de confiança atribuido à chaves públicas de terceiros.

O formato de uso do Enigmail é seguido por diversas outras ferramentas que buscam simplificar o uso da tecnologia PGP na comunicação, como o Evolution, Claws Mail e extensões como o WebPG para Firefox. Elas servem como clientes do chaveiro instalado localmente e traduzem as suas operações para uma interface gráfica familiar ao usuário.

Um ponto comum de dificuldade entre todas elas é a necessidade de lidar com os chaveiros pelas múltiplas estações de trabalho, como notado na avaliação do Enigform na seção anterior.

AVALIAÇÃO DA EXPERIÊNCIA DE CHAVEIROS PGP

Todas as aplicações analisadas tinham em comum o uso de chaveiros instalados localmente, com as chaves fisicamente guardadas na pasta do usuário. Este modelo existe de forma tradicional e serve bem para usuários que operam de uma mesma estação para as suas atividades cotidianas e não precisam de mobilidade.

A experiência de software contemporânea, entretanto, tem mudado. Com a adoção de computadores em vários ambientes visitados ao longo do dia e o uso crescente de dispositivos móveis nos últimos anos ficou ainda mais complexa a manutenção do chaveiro pessoal. Uma tecnologia que já não via grande adoção sofre agora com mais uma barreira de uso para o usuário final.

Além dessa dificuldade os serviços hospedados remotamente e disponibilizados através do navegador não conseguem acessar o chaveiro GPG do usuário. Essas aplicações remotas são uma parte essencial da experiência informatizada das pessoas e deveriam gozar dos mesmo nível de proteção dados à mensagens de e-mail tradicionais.

Observando esta dificuldade, este trabalho propõe uma experiência com o chaveiro capaz de se tornar mais pessoal e, ao mesmo tempo, contribuir com a mobilidade desses recursos de segurança junto com o próprio deslocamento físico do usuário.

PROPOSTA DE CHAVEIRO PESSOAL MÓVEL VIA WEBSERVICE

Neste trabalho propõe-se uma solução para este problema, dando ao usuário a capacidade de manter consigo o chaveiro PGP com seus recursos privados de criptografia e, ainda assim, ser capaz de utilizar tais recursos nas aplicações com as quais interage cotidianamente.

Isso pode ser conseguido utilizando o dispositivo móvel pessoal do usuário - seu smartphone - como recipiente físico das chaves, comportando a implementação do chaveiro. Isso traz uma melhoria na gestão desses recursos, visto que a rotina do usuário

já comporta o transporte e a guarda deste aparelho e já conta com camadas de proteção, como a senha pessoal, criptografia de disco oferecida por alguns sistemas operacionais móveis e a senha do próprio chaveiro, análoga a sua versão para desktop.

Para conseguir realizar as operações necessárias, como criptografar, assinar, descriptografar e verificar assinatura é necessário um canal de comunicação para que as aplicações localizadas nas estações de trabalho possam acessar o chaveiro e fazer uso dos recursos criptográficos agora enclausurados no dispositivo móvel. Para este fim, proponho que haja uma camada de serviço implementando estas operações como webservices.

Neste formato será possível fazer uso dos recursos independente de uma instalação na máquina cliente dedicada à manipulação das chaves conhecidas, mantendo todo o arcabouço de segurança de interesse do usuário centralizado em seu dispositivo. Com esta ação busca-se uma possível solução para o problema de gestão de chaves e da complexidade de transporte de forma segura delas pelos ambientes heterogêneos onde o usuário precisará de proteção.

Para isso será usada uma uma implementação de carteira de chaves disponível para Android chamada Open KeyChain será abordada neste trabalho. Ela consiste em um repositório de chaves PGP com uma usabilidade elevada.

Essa ferramenta de código aberto dá suporte completo à geração de chaves privadas, importação de chaves públicas de diversos servidores comunitários, criptografia, descriptografia, assinatura e verificação de assinaturas em conteúdos textuais. Ela, entretanto, tem escopo limitado à operações manuais no dispositivo.

O escopo deste trabalho está em demonstrar a viabilidade do uso de um chaveiro criptográfico em dispositivo móvel por meio de consultas HTTP aos webservices desenvolvidos através da ferramenta Rest Client. Esses serviços usam a API interna do Open KeyChain para acesso aos seus recursos de chaveiro, delegando-lhe as operações.

Essa possibilidade abre caminho para implementação de novas ferramentas que possam usar esses recursos sem que a estação de trabalho tenha uma instalação do GPG, dependendo somente do chaveiro no dispositivo móvel.

Abaixo uma representação simplificada da proposta, exibindo os principais elementos envolvidos numa operação de criptografia:

Nas subseções seguintes as operações experimentadas são detalhadas. Elas usam os headers HTTP para instruir o chaveiro no dispositivo a respeito da operação desejada. O corpo da requisição e das respostas contém a mensagem original e o resultado de tal operação. Nos exemplos abaixo o IP 192.168.1.100 pertence à um smartphone Moto XT1034 com Android 5 que contém uma instalação do Open KeyChain com chaves para os usuários representados por bob@email.com e alice@email.com. A chave privada padrão é a do usuário bob@email.com.

WEBSERVICE DE ENCRIPTAÇÃO E ASSINATURA DA MENSAGEM

Neste serviço é feita a assinatura da mensagem com a chave padrão escolhida no Open KeyChain e ela será criptografada com a chave pública adequada. O resultado da operação estará no corpo da resposta.

A operação usa uma requisição HTTP POST. O cabeçalho x-operation recebe o

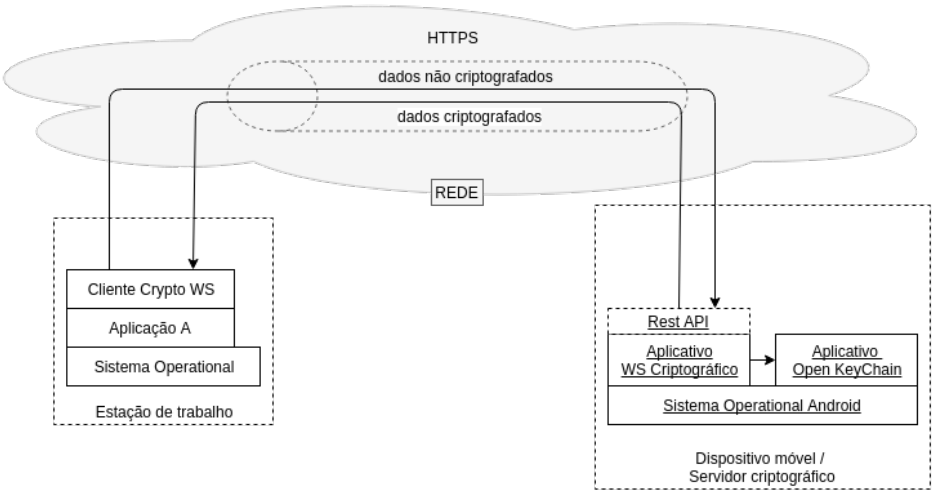

Figure 1. Representação de uma operação de criptografia com chaveiro em dispositivo móvel.

valor encrypt-and-sign. Um parâmetro necessário é o cabeçalho x-destination-mail que conterá o destinatário da mensagem, identificado através do e-mail usado na criação da chave pública.

WEBSERVICE DE DESENCRIPTAÇÃO

Neste serviço é feita a descriptografia da mensagem. Ela depende de o Open KeyChain possuir a chave privada que forma um par com a pública usada para encriptar. Neste exemplo a mensagem enviada para alice@email.com no passo anterior é desencriptada de volta para sua forma legível. A requisição deve usar o cabeçalho x-operation com o valor decrypt-message e o corpo da requisição deve conter a mensagem PGP em texto plano. O resultado é retornado no corpo da resposta, conforme imagem:

Considerações

A proposta de webservices expondo um chaveiro PGP em dispositivo móvel busca resolver alguns casos de uso de criptografia na operação cotidiana do usuário final. Assim como todas as soluções existentes hoje, não seria possível aplicá-la em todos os cenários onde criptografia por chave assimétrica é utilizada atualmente.

Um possível ponto de trabalhos futuros está no estudo do uso prático desta técnica em diferentes tipos, topologias de rede e meios de transmissão, como bluetooth, NFC ou outras tecnologias de transmissão de dados. Também é ponto de experimento futuro verificar, dentro da diversidade de cenários em que uma mensagem precisa ser protegida, quais encontram na proposta deste trabalho o melhor caso de aplicação.

A proposta iniciada pelo projeto ENIGFORM é de interesse particular para o tema deste trabalho. A facilidade de uso introduzida pela adição de assinatura nas requisições HTTP tem grande potencial para simplificar o uso de criptografia pelo usuário e existe espaço para que a proposta do uso desta técnica em conjunto com a proposta de PGP por meio de webservices aqui apresentada seja desenvolvida e evoluida.

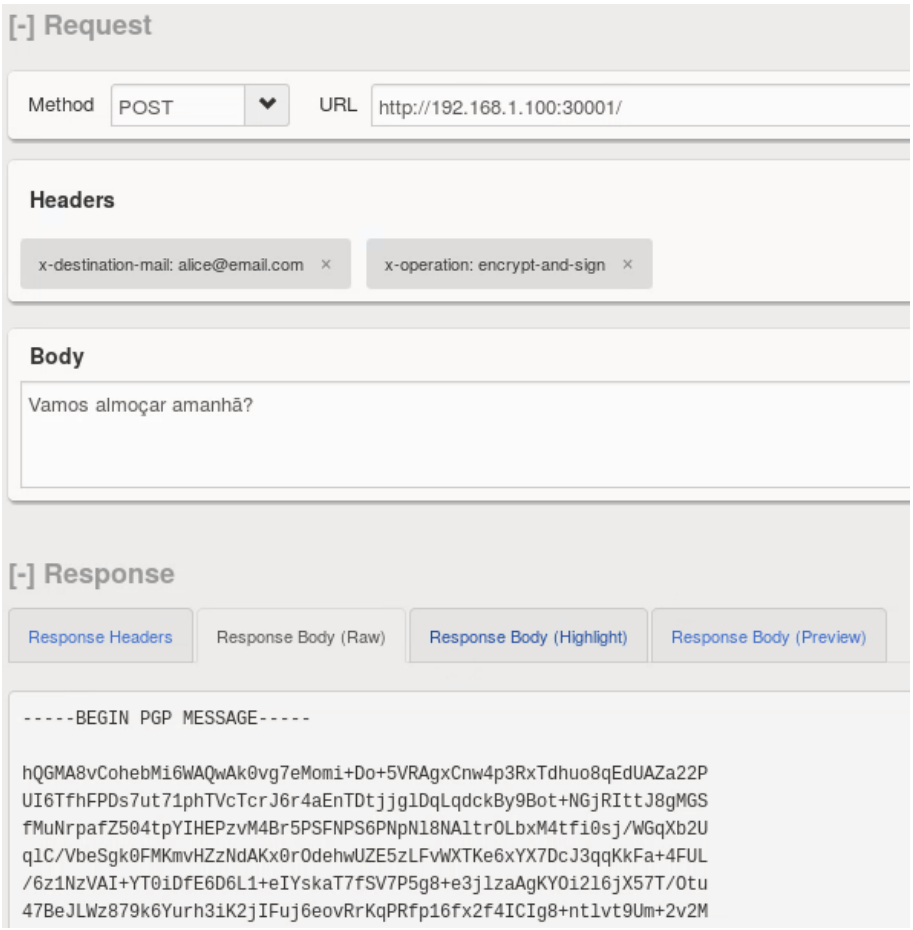

Figure 2. Requisição de criptografia de uma mensagem à ser enviada para alice@email.com.

Conclusão

A importância da criptografia cresce de forma proporcional à comunicação humana por meios digitais. Ela está associada à conceitos como identidade, e direitos como da liberdade de expressão e do sigilo da comunicação. Com isto em mente fica clara a necessidade do desenvolvimento de sistemas de informação que sejam altamente seguros e, ao mesmo tempo, que se integrem ao cotidiano do usuário. A simplicidade do uso deve ser estimulada em conjunto com o desenvolvimento de novas técnicas e ferramentas de segurança. Isso contribuirá com a adoção de práticas seguras pelos usuários dos sistemas de informação e, por consequência, com a segurança e privacidade de todos os envolvidos.

Referências

Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and Thayer, R. (2007). Openpgp message format. RFC 4880, RFC Editor. `http://www.rfc-editor.org/rfc/rfc4880.txt`.

Carmo, F. J., Lemes, P. A., and Freitas, T. H. Criptografia e PGP.

Diffie, W. (1988). The first ten years of public-key cryptography. *Proceedings of the IEEE*, 76(5):560–577.

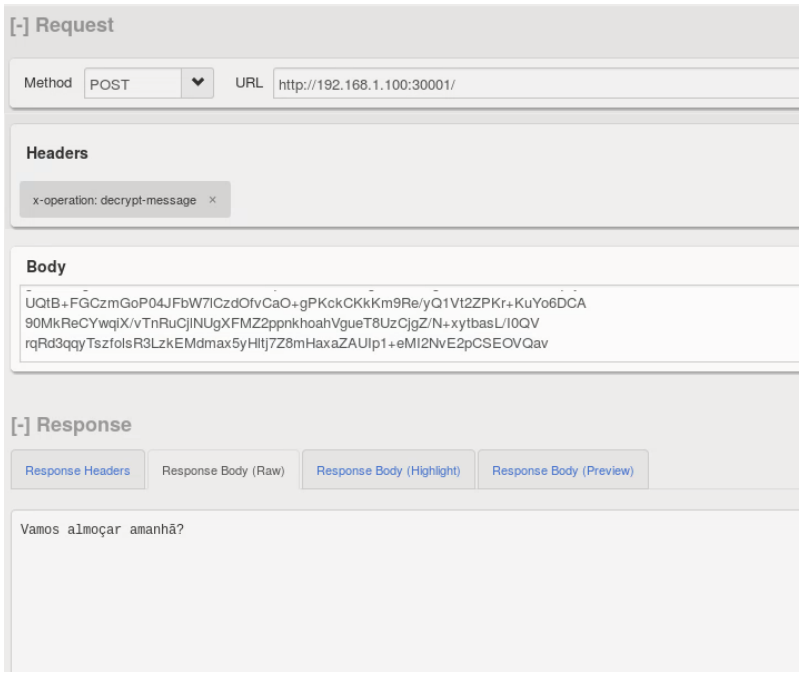

Figure 3. Exemplo de uma mensagem PGP sendo descriptografada de volta à forma legível.

Lehtonen, S. and Parssinen, J. (2002). Pattern language for cryptographic key management. In *EuroPLoP*, pages 245–258.

McDonald, N. G. (2009). Past, present, and future methods of cryptography and data encryption. *Department of Electrical and Computer Engineering, University of Utah*.

Naylor, D., Finamore, A., Leontiadis, I., Grunenberger, Y., Mellia, M., Munafò, M., Papagiannaki, K., and Steenkiste, P. (2014). The cost of the s in https. In *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*, pages 133–140. ACM.

Rushe, D. (2013). Google: don't expect privacy when sending to gmail. *The Guardian. Retrieved Dec*, 19:2014.

Sheng, S., Broderick, L., Koranda, C. A., and Hyland, J. J. (2006). Why johnny still can't encrypt: evaluating the usability of email encryption software. In *Symposium On Usable Privacy and Security*, pages 3–4.

Smith, R. F. (2005). The 3 pillars of information security. `http://windowsitpro.com/security/3-pillars-information-security`. Accessado em: 2016-10-10.

Sweikata, M., Watson, G., Frank, C., Christensen, C., and Hu, Y. (2009). The usability of end user cryptographic products. In *2009 Information Security Curriculum Development Conference*, pages 55–59. ACM.

Symantec (2015). Whitepaper - keeping your private data secure. `https://www.symantec.com/content/dam/symantec/docs/white-papers/keeping-your-private-data-secure-en.pdf`. Accessado em: 2016-10-10.

Zimmermann, P. R. (1996). Significant moments in pgp's history: Zimmermann case dropped. http://philzimmermann.com/EN/news/PRZ_case_dropped.html. Accessado em: 2016-10-10.