Insper

E-MAIL CRIPTOGRAFADO

Tecnologias Hacker

Objetivo: Criação e-mail criptografado.

Descrição: O aluno devera gerar o seu par de chaves publicas utilizando o GNUPG e encaminhar um email criptografado para o professor.

Introdução a Criptografia

A criptografia é o processo de pegar uma mensagem em texto puro e uma chave gerada aleatoriamente e fazer operações matemáticas com as duas até que tudo que sobra é uma versão cifrada da mensagem embaralhada. Por outro lado, decriptografar é pegar o texto cifrado e a chave correta e fazer mais operações matemáticas até que o texto puro é recuperado. Esse processo é chamado criptografia. Um algoritmo de criptografia, o que as operações matemáticas fazem e como eles fazem, é chamado de cifra.

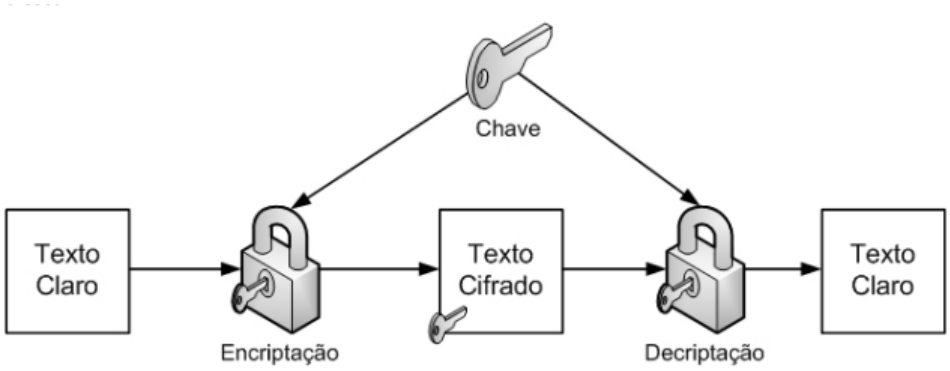
Criptografia Simétrica

Na criptografia simétrica, os participantes desta comunicação precisam acordar uma chave secreta que irá proteger as mensagens trocadas entre eles.
A criptografia simétrica utiliza a mesma chave para encriptar e para decriptar a mensagem:

- Algoritmo simples.
- Alta performance.
- Segurança baseada na confidencialidade das chaves.

Os algoritmos de chave simétrica podem ser divididos em cifras de fluxo (ou contínuas) e em cifras por bloco. As cifras de fluxo cifram os bits da mensagem um a um, enquanto que as cifras por bloco pegam um número de bits e cifram como uma única unidade.

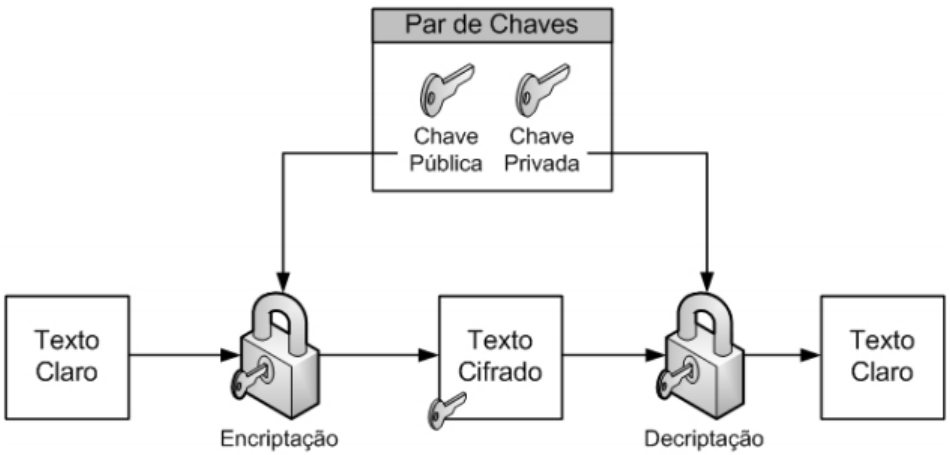
Alguns exemplos de algoritmos simétricos populares e bem reputados incluem Twofish, Serpent, AES, Blowfish, CAST5, RC4, DES, 3DES, e IDEA.



Criptografia Assimétrica

Criptografia de chave pública, também conhecida como criptografia assimétrica, é uma classe de protocolos de criptografia baseados em algoritmos que requerem duas chaves. Diferente do problema clássico de criptografia, na criptografia assimétrica as partes não compartilham uma mesma chave. Ao invés disso, cada um produz um par de chaves. A primeira parte é chamada chave secreta (privada) e deve ser mantida em sigilo. A segunda é chamada de chave pública.

Neste processo a chave pública é utilizada para criptografar uma mensagem, já a privada é usada para decriptografar a mesma.



PGP

Em 1991, Phil Zimmermann desenvolveu um software de criptografia de e-mail chamado Pretty Good Privacy, ou PGP. Ele concebeu o software para ser usado ativistas pela paz na organização do movimento anti-nuclear.

PGP (Pretty Good Privacy), não é um algoritmo de criptografia, embora muitas pessoas tendem a pensar dessa forma. PGP é na verdade um programa de criptografia que utiliza ambos os algoritmos simétricos e assimétricos para criptografar dados. Ele é mais frequentemente usado para o e-mail por existir alguns programa e plugins, mas também pode ser usado para criptografia de disco e apagar com segurança os dados de um disco.

Devido a importância mundial que o PGP obteve, muitos programadores passaram a querer escrever seus próprios softwares de criptografia de modo que fossem

compatíveis. Um grupo de membros da PGP Inc. convenceu Phill Zimmermann e os demais executivos da empresa de que um padrão aberto de PGP era imprescindível para o progresso do próprio PGP e da comunidade usuária da criptografia.

Em julho de 1997, a PGP Inc. propôs a IETF que fosse criado um padrão aberto chamado OpenPGP. Eles concederam permissão para usar esse nome para descrever o padrão e qualquer programa que funcionasse com ele. O IETF aceitou a proposta e iniciou o grupo de trabalho do OpenPGP .

A normativa técnica do OpenPGP foi descrita pela IETF através da RFC 2440 de julho de 1998.

OPENPGP

O OpenPGP é um padrão aberto de criptografia baseado no PGP e funciona por meio de chaves assimétricas, ou seja, cada usuário gera em seu computador um par de chaves, uma pública e uma privada.

A pública é distribuída livremente e permite que qualquer usuário criptografe dados de modo que só quem possui a chave secreta correspondente possa descriptografar. Já a chave secreta, além dessa capacidade de descriptografar, é capaz de assinar dados.

Quando algo é assinado com uma chave secreta, a chave pública correspondente pode verificar se o remetente é verdadeiro e se o conteúdo não foi adulterado depois de assinado. Além disso, o padrão OpenPGP conta com um sistema de cadeias de confiança.

Cada vez que um usuário obtém a chave pública de outro usuário, ao se encontrar com ele, pode verificar a impressão digital (fingerprint) da chave obtida, garantindo certeza de que a chave é a verdadeira (não foi alterada).
Ao ter certeza de que a chave é verdadeira, o usuário pode assinar a chave pública do outro usuário com a sua chave privada, atestando a outros usuários que a chave realmente pertence a quem diz pertencer.

GNU PGP

Software criptográfico compatível com o OpenPGP. A FSF desenvolveu a sua própria versão e a chamou de GNU Privacy Guard, também conhecido como GnuPG ou simplesmente GPG .

A vantagem do uso do GnuPG no lugar do PGP se deve justamente a essa licença pois permite livre cópia e publicação, garantindo que permanecerá livre e sem necessidade de pagamento de royalties. O GNU Privacy Guard (GnuPG ou GPG) é uma alternativa de software livre para a suíte de criptografia PGP, liberado sob licença GNU General Public License. O GnuPG é completamente compatível com o padrão IETF para o OpenPGP.

Insper

Tarefa

Você deverá instalar e configurar um cliente de e-mail em seu sistema operacional. Após completar este processo, instale os plugins e bibliotecas necessárias para a criação de seu par de chaves criptográficas GPG para sua conta de e-mail configurada.

Aplicativos e ferramentas necessárias:

Cliente de e-mail: Thunderbird ou Icedove

Extensão do cliente de e-mail: Enigmail

Enviar um email criptografado para: rodolfo.avelino@uol.com.br. Pegar a chave pública desta conta no Blackboard.

Indicação para pesquisa:

https://www.gnupg.org/
https://www.enigmail.net/index.php/en/
https://www.gpg4win.org/
https://www.thunderbird.net/pt-BR/