**ESQUEMA DE PLANO DE AULA PRÁTICA**

**TAREFAS 2b e 2c :** "Email Seguro"

Tópico no Moodle: “Tarefa 2b – Criptografia de Chave Pública com GnuPG”

Data: 30-08-2013  
  
Tempo de Aula: 2 horas-aula  
  
Grupo: <Aluno\_1> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Aluno\_2> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# 

**ASSUNTO**   
  
Esta é uma tarefa de segurança de aplicação. No caso, é uma aplicação de email, materializada por um cliente de email para máquinas desktop. Você trabalhará, agora, com a ferramenta GnuPG.

**GNU Privacy Guard** (**GnuPG**) é uma alternativa [GPL](http://pt.wikipedia.org/wiki/GNU_General_Public_License) ao aplicativo [PGP](http://pt.wikipedia.org/wiki/Pretty_Good_Privacy) de [criptografia](http://pt.wikipedia.org/wiki/Criptografia). GnuPG é compatível com a [RFC 4880](http://tools.ietf.org/html/rfc4880), o padrão da [IETF](http://pt.wikipedia.org/wiki/Internet_Engineering_Task_Force) para a especificação do [OpenPGP](http://pt.wikipedia.org/wiki/OpenPGP" \o "OpenPGP). GnuPG é parte da [Free Software Foundation](http://pt.wikipedia.org/wiki/Free_Software_Foundation" \o "Free Software Foundation)e do projeto de software [GNU](http://pt.wikipedia.org/wiki/GNU).

# O GnuPG é um programa de código-fonte aberto, disponível gratuitamente para segurança de email. Ele oferece confidencialidade e autenticação, pelo uso de criptografia de chave pública. Assim, o GnuPG trabalha com chaves públicas e chaves privadas, para fazer a segurança de emails.

GnuPg criptografa mensagens utilizando a [criptografia de chaves assimétricas](http://pt.wikipedia.org/wiki/Criptografia_de_chaves_assim%C3%A9tricas). O resultado é que chaves públicas podem ser trocadas com outros usuários de várias maneiras, uma delas são os [servidores de chaves](http://pt.wikipedia.org/w/index.php?title=Servidores_de_chaves&action=edit&redlink=1). As chaves devem sempre ser trocadas com cuidado para evitar o roubo de identidade. É possível também adicionar uma [assinatura digital](http://pt.wikipedia.org/wiki/Assinatura_digital)a mensagem de maneira que a integridade da mensagem e do remetente possam ser verificadas. GnuPG também suporta algoritmos de [criptografia simétrica](http://pt.wikipedia.org/wiki/Criptografia_sim%C3%A9trica). Por padrão GnuPG usa o algoritmo simétrico [CAST5](http://pt.wikipedia.org/wiki/CAST5).

GnuPG não utiliza algoritmos patenteados ou restritos, como por exemplo o algoritmo [IDEA](http://pt.wikipedia.org/wiki/International_Data_Encryption_Algorithm) utilizado no PGP (Na verdade é possível utilizar o IDEA no GnuPG fazendo o download de um plugin, entretanto isso pode requerer a compra de licença em alguns países aonde o IDEA é patenteado). Ao invés disso, GnuPG usa uma variedade de outros algoritmos não patenteados, incluindo:

* Cifras de bloco (algoritmos de criptografia simétrica): [CAST5](http://pt.wikipedia.org/wiki/CAST5), [Camellia](http://pt.wikipedia.org/w/index.php?title=Camellia_(cipher)&action=edit&redlink=1" \o "Camellia (cipher) (página não existe)), [Triple DES](http://pt.wikipedia.org/w/index.php?title=Triple_DES&action=edit&redlink=1), [AES](http://pt.wikipedia.org/wiki/Advanced_Encryption_Standard), [Blowfish](http://pt.wikipedia.org/w/index.php?title=Blowfish_(cipher)&action=edit&redlink=1" \o "Blowfish (cipher) (página não existe)), and [Twofish](http://pt.wikipedia.org/wiki/Twofish" \o "Twofish).
* Cifradores de criptografia de chave pública: [El Gamal](http://pt.wikipedia.org/w/index.php?title=ElGamal&action=edit&redlink=1) and [RSA](http://pt.wikipedia.org/w/index.php?title=RSA_(algorithm)&action=edit&redlink=1)
* Cryptographic hashes: [RIPEMD-160](http://pt.wikipedia.org/wiki/RIPEMD-160), [MD5](http://pt.wikipedia.org/wiki/MD5), [SHA-1](http://pt.wikipedia.org/wiki/SHA-1), [SHA-2](http://pt.wikipedia.org/w/index.php?title=SHA-2&action=edit&redlink=1), and [Tiger](http://pt.wikipedia.org/w/index.php?title=Tiger_(cryptography)&action=edit&redlink=1)
* Digital signatures: [DSA](http://pt.wikipedia.org/w/index.php?title=Digital_Signature_Algorithm&action=edit&redlink=1) and [RSA](http://pt.wikipedia.org/w/index.php?title=RSA_(algorithm)&action=edit&redlink=1)

Você pode, nesta tarefa usar El Gamal para criptografia de chave pública, como uma alternativa ao RSA, que só existe no GnuPG para assinar. Mas use o DSA (Digital Signature Algorithm) para realizar assinaturas digitais.

GnuPG é um software de criptografia hibrido que utiliza a combinação de [criptografia de chaves simétricas](http://pt.wikipedia.org/w/index.php?title=Criptografia_de_chaves_sim%C3%A9tricas&action=edit&redlink=1) para velocidade e [criptografia de chaves publicas](http://pt.wikipedia.org/w/index.php?title=Criptografia_de_chaves_publicas&action=edit&redlink=1) para a troca de mensagens seguras. Isso é conseguido utilizando a criptografia de chave pública para encriptar uma [chave de sessão](http://pt.wikipedia.org/w/index.php?title=Chave_de_sess%C3%A3o&action=edit&redlink=1) que é utilizada apenas uma vez. Esse modo de operação é parte do padrão OpenPGP e é parte do PGP desde sua primeira versão.

# 

**BIBLIOGRAFIA BÁSICA**

<http://www.eriberto.pro.br/wiki/index.php?title=Usando_o_GnuPG>

**OBJETIVOS DA AULA**

Conhecer a ferramenta GnuPG para ser integrada a um cliente de email.

**SELEÇÃO DE CONTEÚDO – A PRÁTICA**

Com o GnuPG adequadamente instalado no Windows 7 (procure ver se já não está instalado), abra, na página da disciplina, correspondente a Aula 3, o link [**Explicando como usar o GnuPG**](http://www.eriberto.pro.br/wiki/index.php?title=Usando_o_GnuPG)

Procure seguir as instruções do link (Eriberto), só não se preocupando com remoção/revogação de chaves. Vá até exportar sua chave pública num servidor externo, o qual guarda chaves públicas de quem as armazena num destes servidores replicados.

Uma vez preparadas as chaves, você pode partir para a Tarefa 2c, no que segue:

Tarefa 2c : Segurança de Email: enviar email criptografado e assinado.

Instalar o GnuPG para segurança em correio eletrônico no cliente de email.

1. Instalar em sua máquina, o Mozilla Thunderbird Ver em: <http://www.mozilla.org/pt-BR/thunderbird/>.
2. (b) Instalar o GnuPG para obter o Thunderbird Email com OpenPGP e S/MIME, usando o complemento Enigmail: <http://enigmail.mozdev.org/download/index.php.html> ou em

Para obter o Thunderbird + Enimail-PT-BR:  
<http://rpmfind.net/linux/RPM/mandriva/2010.0/x86_64/media/main/testing/mozilla-thunderbird-enigmail-pt_BR-3.0.4-0.2mdv2010.0.x86_64.html>

1. Use no Thunderbird, o ícone OpenPGP para criptografar e assinar emails. Teste um email com OpenPGP, com criptografia e sua assinatura, para o professor [bosco@inf.ufsc.br](mailto:bosco@inf.ufsc.br).
2. Caso você queira usar o S/MIME (RFC 822 – Secure/Multipurpose Internet Mail Extension) , você deve:   
   (1) Instalar certificado para serviço de correio.  
   (2) (3) Obter um certificado como abaixo, instalar o certificado de correio no seu cliente de email e testar o S/MIME instalado pelo GnuPG.
3. Para testar S/MIME, enviar outro email assinado/criptografadopara o professor (pode ser em momento fora da aula). Obtendo um Certificado de Email, gratuito para email em sites de empresas especializadas em segurança.

**MOSTRE SEU EXPERIMENTO**

Depois da Tarefa 2c, Ao final da aula, envie um email criptografado e assinado para [bosco@inf.ufsc.br](mailto:bosco@inf.ufsc.br) . Este será o comprovante da realização da tarefa 2b e 2c.

O Moodle será fechado a partir de 22:15 na data desta aula. É a comprovação de sua participação na Tarefa 2a da disciplina.

**CONCLUSÃO**

Com a segurança num cliente de email estabelecida para desktop, você poderá ter esta ferramenta sendo usada em seu ambiente de trabalho, caso confidencialidade e autenticação sejam necessários no seu ambiente. Imagino que num ambiente corporativo, esta tenha mais utilidade do que a utilização de um *webmail*, que a exemplo do Gmail, já tem os recursos de segurança necessários.