**ESQUEMA DE PLANO DE AULA PRÁTICA**

**TAREFAS 4a:** "Segurança de Email"

Tópico no Moodle: “Tarefa 4a – Criptografia de Chave Pública com GnuPG”

Data: 11-04-2014

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%22%20%5Co%20%22OpenPGP). GnuPG é parte da [Free Software Foundation](http://pt.wikipedia.org/wiki/Free_Software_Foundation%22%20%5Co%20%22Free%20Software%20Foundation)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%22%20%5Co%20%22Twofish).
* 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, o qual 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**

Segurança de Email: enviar e receber email criptografado e/ou assinado.

1. Instalar o GnuPG na sua máquina. Use o Windows 7 do LIICT.

[GnuPG ( gnupg-wcli32-1.4.7](http://www.inf.ufsc.br/~bosco/extensao/material-cripto-seg/windows-tools/gnupg-w32cli-1.4.7.exe) )   (Windows)
 [GnuPG v1.4.7](http://www.inf.ufsc.br/~bosco/ensino/ine5630/material-cripto-seg/Linux-Tools/gnupg-1.4.7.tar.gz)   (Linux)

1. Com o GnuPG adequadamente instalado (procure ver se já não está instalado), abra, na página da disciplina no link [**Explicando como usar o GnuPG**](http://www.eriberto.pro.br/wiki/index.php?title=Usando_o_GnuPG)ou [GRIS-2004-T-001.pdf](http://www.inf.ufsc.br/~bosco/extensao/material-cripto-seg/gris-2004-t-001.pdf)

Para conhecer o GnuPG, procure seguir as instruções do link acima. Vá até exportar sua chave pública num servidor externo, o qual guarda chaves públicas de quem as armazena num destes servidores replicados.

Agora, você precisa integrar GnuPG+Enigmail+Thunderbird. Veja os links:

[Thunderbird com Enigmail e GnuPG](https://securityinabox.org/en/thunderbird_main)

[Como usar Enigmail com GnPG em Thunderbird](https://securityinabox.org/en/thuderbird_encryption%22%20%5Cl%20%224.2)

1. **In**stalar Enigmail em sua máquina. Enigmail é uma extensão para Mozilla Thunderbird e Seamonkey. Ele habilita você a escrever e receber emails assinados e/criptografados com o padrão OpenPGP.

[Download Enigmail v 1.6 para Windows sobre Thunderbird 24.0](https://addons.mozilla.org/en-US/thunderbird/downloads/file/229990/enigmail-1.6-sm%2Btb.xpi)

1. Instalar em sua máquina, o Mozilla Thunderbird. Este vem, naturalmente, sem segurança para e-mails. Ver em: <http://www.mozilla.org/pt-BR/thunderbird/>.
2. Para obter a segurança de email no Thunderbird, você precisa instalar tal extensão. Esta, integra GnuPG no Thunderbird, fazendo aparecer neste cliente de email, os ícones OpenPGP e S/MIME. Para obter o Enigmail, vá para o link: Instale no Thunderbird, o Enigmail.
3. Depois de tudo pronto, use no Thunderbird, o ícone OpenPGP para criptografar e assinar e-mails.
4. Caso você queira usar o S/MIME (RFC 822 – Secure/Multipurpose Internet Mail Extension) , você deve:

(1) Instalar um certificado para serviço de email (conhecido como certificado de correio). Este certificado não é preciso no OpenPGP, que trabalha somente com os pares de chaves da criptografia de chaves públicas.

(2) Obter um certificado como abaixo, instalar o certificado de correio no seu cliente de email e testar o S/MIME instalado pelo Enigmail+GnuPG.
5. Para testar S/MIME, enviar outro email assinado/criptografadopara o professor. Obtendo um Certificado de Email, gratuito para email em sites de empresas especializadas em segurança.

**RESPONDA AS SEGUINTES QUESTÕES**

Você já sabe. Quando você criptografa, você garante os requisitos de segurança de CONFIDENCIALIDADE ou PRIVACIDADE. Quando você usa assinatura digital, pode garantir AUTENTICIDADE, INTEGRIDADE e NÃO-REPÚDIO.

1. Por que um email assinado garante o requisito de segurança de NÃO-REPÚDIO ?
2. Por que um email assinado garante o requisito de segurança de INTEGRIDADE ?
3. Por que um email assinado garante o requisito de segurança de AUTENTICIDADE ?
4. Se uma chave pública é distribuída, a descoberto, na Internet, que certeza você pode ter de estar recebendo a chave pública verdadeira de alguém com quem você deseja se comunicar ?

**CONCLUSÃO**

Depois da Tarefa 4a concluída, ao final da aula, você pode enviar e receber emails criptografados e assinados, usando um cliente de email em seu computador.

Com a segurança num cliente de email estabelecida para desktop, você poderá ter esta ferramenta sendo usada em seu ambiente corporativo de trabalho, caso confidencialidade e autenticação sejam necessários no seu ambiente. Num ambiente corporativo, segurança de email, pode ser necessário e a utilização de um *webmail* externo à corporação (Gmail, Hotmail, .... ), pode não garantir a segurança pretendida. Para e-mails pessoais de pessoas com cargos públicos importantes, um cliente de email de desktop pode ser muito mais conveniente no sentido de garantir segurança.

**MOSTRE SEU EXPERIMENTO**

O Moodle será fechado a partir de 22:00 na data desta aula. É a comprovação de sua participação na Tarefa 4a da disciplina.