# Criptografia Assimétrica

PGP

GnuPG (GPG)

# PGP

PGP – Pretty Goog Privacy (privacidade muito boa)

- criado por Davi Phil Zimmermann Arimateia em 1991;
- utilizado para assinatura digital;
- criptografia e descriptografia de textos;
- e-mails;
- arquivos, diretórios e partições inteiras de disco.

# PGP

PGP – Pretty Goog Privacy (privacidade muito boa)

- criado por Davi Phil Zimmermann Arimateia em 1991;
- se baseia no conceito de chave pública e privada;
- a chave pública é distribuída para as pessoas que desejam trocar dados/mensagens;
- e a chave privada fica com o seu dono e não pode ser distribuída;
- OpenPGP é o padrão aberto compatível com o PGP;
- GnuPGP (GPG) é o padrão aberto compatível com o PGP.

# GnuPG (GPG)

Criptografia Assimétrica

- os dados são criptografados usando a chave pública e somente o dono (de posse da chave privada) poderá descriptografar os dados.

# GnuPG (GPG)

Assinatura Digital

- quando se assina um arquivo usando o pgp, usa-se a chave privada, o destinatário de posse da chave pública poderá então confirmar que a origem dos dados é confiável.

# GnuPG (GPG)

Instalação

- para instalação em sistemas Linux, da família Debian (Debian, Ubuntu e etc.) pode-se usar o comando para instalação direto do repositório apt:

$ sudo apt-get install gnupg

# GnuPG (GPG)

Gerando as chaves

- após a instalação do gnupg, execute o comando gpg para criar o diretório ~/.gnupg que armazenará as chaves pública e privada.

- para gerar um par de chaves pessoais usa-se o comando:

$ gpg --gen-key

# GnuPG (GPG)

```
$ gpg --gen-key
gpg (GnuPG) 1.4.18; Copyright (C) 2014 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: failed to create temporary file `/home/pc/.gnupg/.#lk0x8dbf90.pc-lab.6644': Permission denied
gpg: keyblock resource `/home/pc/.gnupg/secring.gpg': general error
gpg: failed to create temporary file `/home/pc/.gnupg/.#lk0x8dd290.pc-lab.6644': Permission denied
gpg: keyblock resource `/home/pc/.gnupg/pubring.gpg': general error
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection?
```

# GnuPG (GPG)

Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 1024
Requested keysize is 1024 bits
Please specify how long the key should be valid.
0 = key does not expire
<n> = key expires in n days
<n>w = key expires in n weeks
<n>m = key expires in n months
<n>y = key expires in n years
Key is valid for? (0)

# GnuPG (GPG)

Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

# GnuPG (GPG)

Real name: Nome Sobrenome
Email address: email@xxx.com.br
Comment:
You selected this USER-ID:
    "Nome Sobrenome <email@xxx.com.br>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o

# GnuPG (GPG)

You need a Passphrase to protect your secret key.

can't connect to server: ec=255.16777215
gpg: problem with the agent - disabling agent use
We need to generate a lot of random bytes. It is a good idea to perform some other action (type on the keyboard, move the mouse, utilize the disks) during the prime generation; this gives the random number generator a better chance to gain enough entropy.

Not enough random bytes available.  Please do some other work to give the OS a chance to collect more entropy! (Need 192 more bytes)

OBS: para que ele consiga gerar a chave necessita-se efetuar alguma tarefa no computador, como abrir programas, navegar na web, mexer o mouse e etc.

# GnuPG (GPG)

.+++++
...+++++
We need to generate a lot of random bytes. It is a good idea to perform some other action (type on the keyboard, move the mouse, utilize the disks) during the prime generation; this gives the random number generator a better chance to gain enough entropy.
.+++++
+++++
gpg: /home/pc/.gnupg/trustdb.gpg: trustdb created
gpg: key A713ED5B marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
pub   1024R/A713ED5B 2015-09-12
      Key fingerprint = 7A8A 91E4 43D9 B583 6D17  8799 09E9 6734 A713 ED5B
uid                  Jiyan Yari <jeancat@ig.com.br>
sub   1024R/F836A778 2015-09-12

pc@pc-lab:~$

# GnuPG (GPG)

As configurações usadas foram:

- chave criptográfica - Selecione o padrão a não ser que tenha necessidades específicas.
- tamanho da chave - 1024 bits traz uma boa combinação de proteção/velocidade.
- validade da chave - 0 a chave não expira.
- um número tem o valor de dias, que pode ser seguido das letras w (semanas), m (meses) ou y (anos).
Por exemplo, "7m", "2y", "60".

# GnuPG (GPG)

- nome de usuário - Nome para identificar a chave
- e-mail - E-mail do dono da chave
- comentário - Uma descrição sobre a chave do usuário.
- confirmação - Tecle "O" para confirmar os dados ou uma das outras letras para modificar os dados de sua chave.
- digite uma senha que irá identificá-lo(a) como proprietário da chave privada.
- confirme e aguarde a geração da chave pública/privada.

OBS: para acelerar a entropia na geração da chave faça algo no seu computador, como navegar, abrir programas, mexer no mouse e etc.

# GnuPG (GPG)

Encriptando dados

- usar o comando gpg -e nome_arquivo faz a encriptação de dados:

Obs: criar um arquivo chamado arquivo.txt para o exercício
$ nano arquivo.txt
Teste de criptografia com o GPG ...

$ gpg -e arquivo.txt

# GnuPG (GPG)

- será pedido a identificação de usuário;
- digitar o nome que foi usado para criar a chave;
- o arquivo criado será encriptado usando a chave pública do usuário (~/.gnupg/pubring.gpg) e terá a extensão .gpg adicionada (arquivo.txt.gpg).

$ ls arquivo.*
arquivo.txt  arquivo.txt.gpg

# GnuPG (GPG)

- a opção -a é usada para criar um arquivo criptografado com saída ASCII 7 bits:

$ gpg -e -a arquivo.txt

- o arquivo gerado terá a extensão .asc acrescentada (arquivo.txt.asc) e não será compactado;
- a opção -a é muito usada para o envio de e-mails.

# GnuPG (GPG)

Descriptografando dados com o gpg

- para descriptografar o arquivo usa-se a opção -d e a chave privada:

$ gpg -d arquivo.txt.asc > arquivo.txt
$ gpg -d arquivo.txt.gpg > arquivo.txt

OBS: no primeiro comando será solicitada a senha que foi criada quando instalado o GPG

# GnuPG (GPG)

Assinatura Digital

- assinar um arquivo digitalmente é garantir que você é a pessoa que realmente enviou aquele arquivo.
- usa-se a opção -s para assinar arquivos usando sua chave privada:

$ gpg -s arquivo.txt

- será solicitada a senha criada quando da instalação e será usada a chave privada para assinatura do arquivo.

# GnuPG (GPG)

Assinatura Digital

- será gerado um arquivo (arquivo.txt.gpg) assinado e compactado;
- pode ser acrescentada a opção –clearsign criar uma assinatura em um texto plano, este é um recurso muito usado por programas de e-mails com suporte ao gpg:

$ gpg -s --clearsign arquivo.txt

- será criado um arquivo chamado arquivo.txt.asc contendo o arquivo assinado e sem compactação.

# GnuPG (GPG)

Checando assinaturas

- a checagem de assinatura consiste em verificar que quem nos enviou o arquivo é realmente quem diz ser e se os dados foram de alguma forma alterados;

- deve-se ter a chave pública do usuário no seu chaveiro para fazer esta checagem (adicionando a chaves públicas ao chaveiro ou diretório);

- para verificar os dados assinados acima usa-se a opção –verify:

# GnuPG (GPG)

$ gpg --verify arquivo.txt.asc
gpg: Signature made Sex 11 Set 2015 21:26:35 AMT using RSA key ID 90993B78
gpg: Good signature from "Nome Sobrenome <email@xxx.com.br>"

gpg --verify arquivo.txt.gpg
gpg: Signature made Sex 11 Set 2015 21:25:55 AMT using RSA key ID 90993B78
gpg: Good signature from "Nome Sobrenome <email@xxx.com.br>"

# GnuPG (GPG)

- se a saída for “Good signature”ou "Assinatura Correta", significa que a origem do arquivo é segura e que ele não foi de qualquer forma modificado;

- se a saída for “Bad signature” ou "Assinatura INCORRETA" significa que ou o usuário que enviou o arquivo não confere ou o arquivo enviado foi de alguma forma modificado.

# GnuPG (GPG)

Extraindo sua chave pública do chaveiro

- a chave pública deve ser distribuída a outros usuários para que possam enviar dados criptografados ou checar a autenticidade de seus arquivos;
- para exportar sua chave pública em um arquivo que será distribuído a outras pessoas ou servidores de chaves na Internet, usa-se a opção --export:

$ gpg --export -a nome_usuario >chave-pub.txt

- ao invés do nome do usuário, poderá ser usado seu e-mail, ID da chave, etc.
- a opção -a permite que os dados sejam gerados usando bits ASCII 7.

# GnuPG (GPG)

Adicionando chaves públicas ao seu chaveiro pessoal

- adicionar chaves públicas é necessário para o envio de dados criptografados e checagem de assinatura do usuário;
- para isso usa-se a opção --import:

$ gpg --import chave-pub-usuario.txt

- o arquivo chave-pub-usuario.txt contém a chave pública do usuário;
- o gpg detecta chaves públicas dentro de textos e faz a extração corretamente.

# GnuPG (GPG)

Listando chaves de seu chaveiro

- usar o comando para listar as chaves pública do chaveiro:
$ gpg –list-keys

/home/aluno/.gnupg/pubring.gpg
---
pub 1024R/90993B78 2015-09-12
uid Nome Sobrenome <email@xxx.com.br>
sub 1024R/2F71909C 2015-09-12

# GnuPG (GPG)

Listando chaves de seu chaveiro

- usar o comando para listar suas chaves privadas:
$ gpg –list-secret-keys

/home/aluno/.gnupg/pubring.gpg
---
pub 1024R/90993B78 2015-09-12
uid Nome Sobrenome <email@xxx.com.br>
sub 1024R/2F71909C 2015-09-12

# GnuPG (GPG)

Apagando chaves de seu chaveiro

- quando uma chave pública é modificada ou por qualquer outro motivo deseja retira-la do seu chaveiro público, utilize a opção --delete-key:

$ gpg --delete-key Nome Sobrenome

# GnuPG (GPG)

Mudando a senha

- para mudar a senha usar o comando:

$ gpg --edit-key Nome Sobrenome

- quando entrar em modo de comandos, digite passwd;
- será pedida a nova senha e a confirmação;
- digitar "save" para sair e salvar as alterações;
- ou "quit" para sair e abandonar o que foi feito.

# GnuPG (GPG)

Mudando a senha

- para mudar a senha usar o comando:

$ gpg --edit-key Nome Sobrenome

gpg> passwd
Key is protected.

You need a passphrase to unlock the secret key for
user: "Nome Sobrenome <email@xxx.com.br>"
1024-bit RSA key, ID 90993B78, created 2015-09-12

Enter the new passphrase for this secret key.

# GnuPG (GPG)

Exportando chave com segurança:

- verificar as chaves privadas presentes no seu chaveiro ou diretório:

```
$ gpg --list-secret-keys
  /home/fulano/.gnupg/secring.gpg
  ------------------------------
  sec   2048R/B42F51DC 2012-03-27
  uid                  Fulano de Tal <ftal@empresa.com.br>
  ssb   2048R/4CCDDB79 2012-03-27
```

- em seguida exportar a chave desejada:

```
gpg --armor --export B42F51DC
```

# GnuPG (GPG)

- a opção --armor (que significa "armadura") protege a chave, que é binária, codificando-a em **base64**;
- esse sentido de "proteção" diz respeito à transmissão da chave via e-mail ou outro protocolo baseado em texto.

$ gpg --armor --export B42F51DC

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.17 (GNU/Linux)

mQENBE9xFSEBCADRg3KV+SoSifeYwmxCowL/QQgvYOnc8UikUrLbU3jxfmYeSUkp
mlk9WDpxCUEjyM3XxMhY2rOe4wxc50OcinHzSesQCTlgC3FbWLKH6Frys0ofeBam
(... várias linhas ...)
FSzEMWCZXq0stI5pCCrBOIGrjFrfMq0LOOrs8SEkfoSAu3w5Pr9y3WT+pT8jI47C
goNJ0wRGe+pS4dgTVOVhj8vQA+qflblRiaBMG3zR
=kQb3
-----END PGP PUBLIC KEY BLOCK-----
```

# GnuPG (GPG)

base64

- é um método para codificação de dados para transferência na Internet (codificação MIME para transferência de conteúdo);
- é utilizado frequentemente para transmitir dados binários por meios de transmissão que lidam apenas com texto, como por exemplo para enviar arquivos anexos por email.
- é constituído por 64 caracteres ([A-Z],[a-z],[0-9], "/" e "+") que deram origem ao seu nome;
- o carácter "=" é utilizado como um sufixo especial e a especificação original (RFC 989) definiu que o símbolo "*" pode ser utilizado para delimitar dados convertidos, mas não criptografados, dentro de um stream.

Exemplo de codificação:
Texto original: hello world
Texto convertido para Base64: aGVsbG8gd29ybGQK

# GnuPG (GPG)

Exportando a chave

- caso se queira direcionar a saída para um arquivo, basta usar a opção -o nome_do_arquivo:

```
$ gpg --armor -o fulano-gpg-pubkey --export B42F51DC
```

# GnuPG (GPG)

Listando assinaturas digitais

- executar o comando para listar todas as assinaturas existentes no chaveiro ou diretório:

$ gpg --list-sigs

# GnuPG (GPG)

- opcionalmente pode ser especificado um parâmetro para fazer referência a assinatura de um usuário:

$ gpg --list-sigs usuario

- o comando adicionalmente faz a checagem de assinaturas:
$ gpg --check-sigs

# GnuPG (GPG)

Importação de chaves sem servidor

- caso um emissor tenha exportado uma chave pública e a enviado a um destinatário, deve-se importar esta chave usando o comando:

$ gpg --import beltrano-gpg-pubkey

gpg: key 14161D0F: public key "Beltrano de Tal <beltr@no.com.au>" imported
  gpg: Número total processado: 1
  gpg:               importados: 1  (RSA: 1)
  (...)

# GnuPG (GPG)

Adição de novos IDs

- caso se queira mudar o ID por ter alterado ou criado um e-mail pode-se adicionar um novo ID no GPG usando o comando:

$ gpg --list-secret-keys

```
sec   2048R/B42F51DC 2010-08-15
uid                  Fulano de Tal <ftal@empresa.com.br>
ssb   2048R/4CCDDB79 2010-08-15
```

# GnuPG (GPG)

- para adicionar a nova identidade a chave já existente usa-se o editor de chaves:

```
$ gpg --edit-key 4CCDDB79
  Chave secreta disponível.
pub  2048R/B42F51DC  created: 2010-08-15  expires: never  usage: SC
                     trust: ultimate      validity: ultimate
sub  2048R/4CCDDB79  created: 2010-08-15  expired: never  usage: E
  [ultimate] (1). Fulano de Tal <ftal@empresa.com.br>
```

# GnuPG (GPG)

**gpg> adduid**

Real name: Fulano de Tal
Email address: ftal@companhia.com
Comment: Novo emprego!
You selected this USER-ID:
"Fulano de Tal (Novo emprego!) <ftal@companhia.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o

You need a passphrase to unlock the secret key for
user: "Fulano de Tal <ftal@empresa.com.br>"
2048-bit RSA key, ID B42F51DC, created 2012-03-27

pub 2048R/B42F51DC created: 2010-08-15 expires: never usage: SC
trust: ultimate validity: ultimate
sub 2048R/4CCDDB79 created: 2010-08-15 expired: never usage: E
[ultimate] (1) Fulano de Tal <ftal@empresa.com.br>
[ unknown] (2). Fulano de Tal (Novo emprego!) <ftal@companhia.com>

# GnuPG (GPG)

- a seguir seleciona-se a identidade para apagar:

gpg> uid 1

pub 2048R/B42F51DC created: 2012-03-27 expires: never usage: SC
trust: ultimate validity: ultimate
sub 2048R/4CCDDB79 created: 2012-03-27 expires: never usage: E
[ultimate] (1)* Fulano de Tal <ftal@empresa.com.br>
[ unknown] (2). Fulano de Tal (Novo emprego!) <ftal@companhia.com>

# GnuPG (GPG)

- a seguir apaga-se a identidade selecionanda:

```
gpg> deluid
  Really remove this user ID? (y/N) y

  pub  2048R/B42F51DC  created: 2012-03-27  expires: never       usage:
SC
                     trust: ultimate      validity: ultimate
   sub   2048R/4CCDDB79   created:  2012-03-27   expires:  never
usage: E
  [ unknown] (1). Fulano de Tal (Novo emprego!) <ftal@companhia.com>
```

- e salva-se a operação:

```
gpg> save

$ _
```