

Criptografia Assimétrica e Gerenciando Chaves com GnuPG

[6 de julho de 2015](#) / [Methz](#)

Não é de hoje que prezamos por segurança ao compartilhar informações, desde a Roma antiga já tinham pensado em uma forma de manter suas mensagens seguras caso fossem interceptadas, dando assim origem ao que conhecemos hoje como a técnica de criptografia, Cifra de César.

Introdução

Não é de hoje que prezamos por segurança ao compartilhar informações, desde a Roma antiga já tinham pensado em uma forma de manter suas mensagens seguras caso fossem interceptadas, dando assim origem ao que conhecemos hoje como a técnica de criptografia, Cifra de César.

Criptografia

Criptografia é nome dado as diversas técnicas existentes com o propósito de cifrar uma mensagem, ou seja, transformar a mensagem original em uma cadeia de caracteres ilegível para embaralhar e confundir um possível interceptador. É nessa linha de pensamento que surgiu a **Criptografia Assimétrica**.

Criptografia Assimétrica

Conforme o avanço das tecnologias e pesquisas, foi criado a Criptografia Simétrica (e.g, AES), porém ela possui uma “falha”, a chave para codificar a mensagem é a mesma usada para decodificar, isso faz com que o remetente e o destinatário obrigatoriamente compartilhem essa chave antecipadamente, aumentando o risco da chave ser interceptada.

Para quebrar essa barreira, foi criado a Criptografia Assimétrica. Também conhecida como Criptografia de Chave Pública, ela utiliza um par de “chaves”: chave pública e chave privada. A chave pública pode ser livremente compartilhada por e-mail, mensagens ou repositórios específicos, sem medo algum. Já o conhecimento da chave privada deve ser somente do seu criador.

A chave pública tem como objetivo principal a confidencialidade da mensagem, ela que vai criptografar a mensagem e será enviada junto na própria mensagem, assim a pessoa poderá checar se a mensagem não foi alterada pelo caminho. A chave privada visa a autenticidade, isto é, somente ela poderá ser usada para decodificar a mensagem que foi feita com sua chave pública. Veja uma analogia abaixo para fixação.

- A **pessoa A** compartilha sua chave pública com a **pessoa B**;
- A **pessoa B** usa essa chave para criptografar uma mensagem e enviá-la de volta para a **pessoa A**;
- A **pessoa A** então usa sua própria chave privada para decodificar a mensagem;
- A chave pública da **pessoa B** pode ser incluída na mensagem de retorno ou publicada para ter sua mensagem respondida.

Explicaçãozinha: Chaves são um conjunto de bits ou até mesmo ‘pedaços’ de informações, que controlam a autenticidade e integridade de uma mensagem.

OBS: Esse método só garante a autenticidade e a codificação de mensagens, de forma alguma o anonimato. O fato da pessoa A se comunicar com a pessoa B não é secreto, apenas sua mensagem.

GnuPG

GnuPG conhecido também por GPG, é um software baseado no padrão OpenPGP (padrão open source baseado no PGP, licenciado sob a GPL), usado principalmente na troca de e-mails, tem o objetivo de codificar, decodificar e assinar mensagens usando a criptografia assimétrica explicada acima. Custo zero e liberdade de cópia são alguns fatores vantajosos dessa ferramenta.

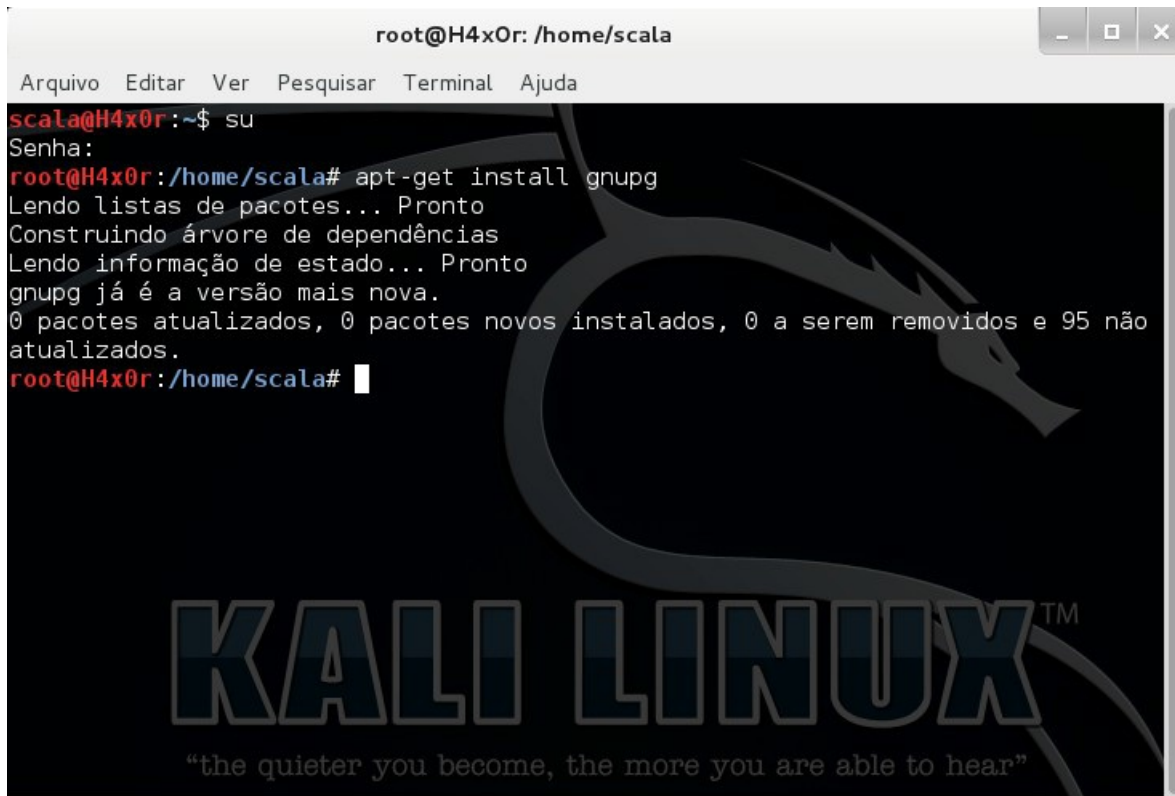
Vamos ver agora como utilizar essa super ferramenta para nos auxiliar a troca de mensagens seguras. Você só precisará de um ambiente Linux para continuar. Foi usada a distribuição **Kali** nos exemplos a seguir.

Instalando

Como usuário normal:

Digite o comando `su` para logar como root e digite a senha.
em seguida digite:

```
apt-get install gnupg
```

A terminal window titled 'root@H4x0r: /home/scala' with a menu bar (Arquivo, Editar, Ver, Pesquisar, Terminal, Ajuda). The background is a Kali Linux wallpaper featuring a dragon and the text 'KALI LINUX™' and '“the quieter you become, the more you are able to hear”'. The terminal shows the user 'scala@H4x0r' running 'su' to become root. The root prompt is '#'. The command 'apt-get install gnupg' is entered, followed by the output: 'Lendo listas de pacotes... Pronto', 'Construindo árvore de dependências', 'Lendo informação de estado... Pronto', 'gnupg já é a versão mais nova.', and '0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 95 não atualizados.' The prompt returns to root@H4x0r:~#.

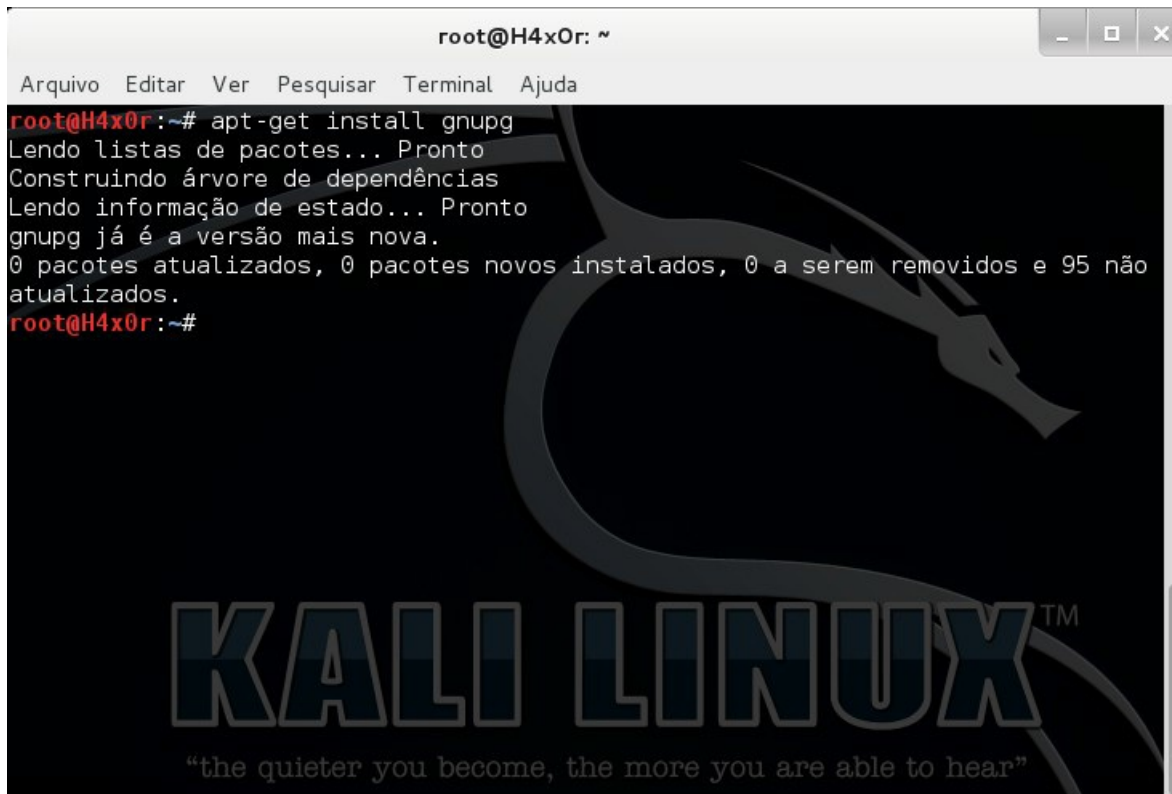
```
root@H4x0r: /home/scala
scala@H4x0r:~$ su
Senha:
root@H4x0r: /home/scala# apt-get install gnupg
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
gnupg já é a versão mais nova.
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 95 não
atualizados.
root@H4x0r: /home/scala#
```

Logando como root

Como usuário root:

Aqui um simples `apt-get install gnupg` resolve o problema

```
apt-get install gnupg
```

A terminal window titled 'root@H4x0r: ~' with a menu bar (Arquivo, Editar, Ver, Pesquisar, Terminal, Ajuda). The background is a Kali Linux wallpaper featuring a dragon and the text 'KALI LINUX™' and '“the quieter you become, the more you are able to hear”'. The terminal shows the root prompt '#'. The command 'apt-get install gnupg' is entered, followed by the output: 'Lendo listas de pacotes... Pronto', 'Construindo árvore de dependências', 'Lendo informação de estado... Pronto', 'gnupg já é a versão mais nova.', and '0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 95 não atualizados.' The prompt returns to root@H4x0r:~#.

```
root@H4x0r: ~# apt-get install gnupg
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
gnupg já é a versão mais nova.
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 95 não
atualizados.
root@H4x0r:~#
```

Instalando como root

NOTA2: Se você for usar o gpg para usar na troca de e-mails, é recomendado instalar o plugin EnigMail para o navegador Thunderbird:

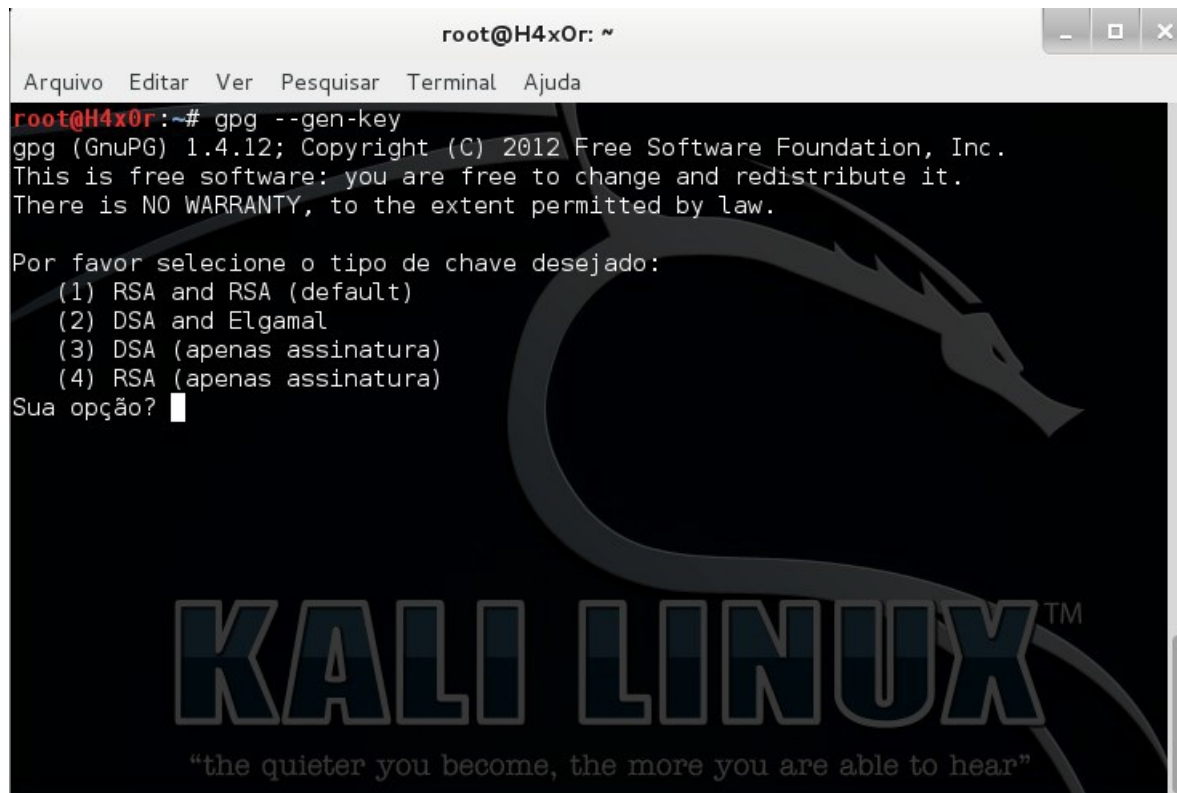
apt-get install enigmail

Criando as Chaves

Para criar as Keys(chaves) você ter fixado primeiramente o objetivo delas explicado no começo desse artigo. Vamos lá, pra gerar as Keys vamos usar o comando:

gpg --gen-key

Aqui você vai escolher o tipo de chave que irá utilizar, não vou detalhar cada uma delas, pois não é o objetivo do tópico. Por padrão foi usado a opção 1 e teclado ENTER em seguida.


A screenshot of a Kali Linux terminal window. The title bar shows 'root@H4x0r: ~'. The menu bar includes 'Arquivo', 'Editar', 'Ver', 'Pesquisar', 'Terminal', and 'Ajuda'. The terminal content shows the command 'gpg --gen-key' being executed. It displays the GnuPG version (1.4.12) and copyright information. It then prompts the user to select a key type from a list: (1) RSA and RSA (default), (2) DSA and Elgamal, (3) DSA (apenas assinatura), and (4) RSA (apenas assinatura). The prompt 'Sua opção?' is followed by a cursor. In the background, there is a large, faint Kali Linux dragon logo and the text 'KALI LINUX™' and the quote 'the quieter you become, the more you are able to hear'.

Escolhendo o Tipo de Chave

Após escolher o tipo devemos escolher o tamanho da chave, no caso da RSA utilizada no exemplo, varia de 1024 a 4096 bits. Por padrão é 2048, então só vamos teclar ENTER, caso não queira 2048, digite o tamanho desejado e tecla ENTER.

```
root@H4x0r: ~
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
root@H4x0r:~# gpg --gen-key
gpg (GnuPG) 1.4.12; Copyright (C) 2012 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.

Por favor selecione o tipo de chave desejado:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (apenas assinatura)
  (4) RSA (apenas assinatura)
Sua opção? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) █
```




Escolhendo tamanho da chave

Agora vamos escolher qual a 'data de validade' dessa chave. Por padrão ela é válida pra sempre, mas caso você queira que ela expire em certa quantidade de tempo, ou até mesmo numa data específica, pode colocar apenas o número, que vai ser relacionado há os dias. Exemplo, se você digitar **50**, a chave irá se expirar em 50(cinquenta) dias. Se colocar **10w**, irá se expirar em 10 semanas e assim por diante.

Vamos continuar no padrão e optar por nunca se expirar teclando ENTER apenas.

```
root@H4x0r: ~
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
root@H4x0r:~# gpg --gen-key
gpg (GnuPG) 1.4.12; Copyright (C) 2012 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.

Por favor selecione o tipo de chave desejado:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (apenas assinatura)
  (4) RSA (apenas assinatura)
Sua opção? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
O tamanho de chave pedido é 2048 bits
Por favor especifique por quanto tempo a chave deve ser válida.
  0 = chave não expira
  <n> = chave expira em n dias
  <n>w = chave expira em n semanas
  <n>m = chave expira em n meses
  <n>y = chave expira em n anos
A chave é válida por? (0) █
```



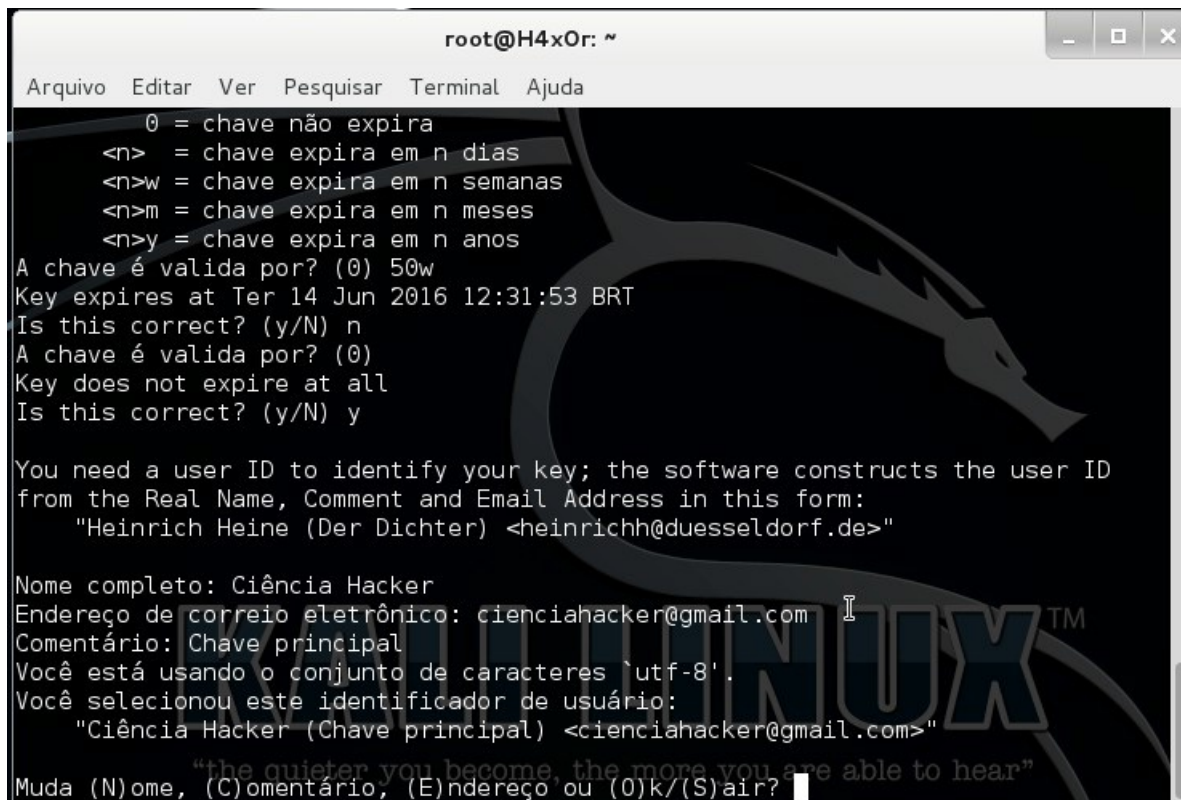
Escolhendo a data de expiração da chave

Após escolher a data, aparecerá um diálogo de confirmação, se estiver tudo correto digita 'y' e tecla ENTER para continuar, se não 'n' e repita.

Agora vamos preencher um formulário com algumas informações pessoais para sermos identificados

mais facilmente.

Nome Completo, E-mail e Comentário são as informações necessárias para preenchimento. Você irá preencher conforme seus dados e ir teclando ENTER, ao confirmar os três campos, outro diálogo irá aparecer para verificar se as informações estão corretas. Analise calmamente e caso tiver algo errado, use 'N' para mudar de nome, 'C' para mudar o comentário e 'E' para mudar o e-mail. Se tudo ocorrer bem, tecle 'o' (letra o minúsculo) para continuar.



```
root@H4x0r: ~
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

0 = chave não expira
<n> = chave expira em n dias
<n>w = chave expira em n semanas
<n>m = chave expira em n meses
<n>y = chave expira em n anos
A chave é válida por? (0) 50w
Key expires at Ter 14 Jun 2016 12:31:53 BRT
Is this correct? (y/N) n
A chave é válida por? (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>"

Nome completo: Ciência Hacker
Endereço de correio eletrônico: cienciahacker@gmail.com
Comentário: Chave principal
Você está usando o conjunto de caracteres `utf-8'.
Você selecionou este identificador de usuário:
"Ciência Hacker (Chave principal) <cienciahacker@gmail.com>"
Muda (N)ome, (C)omentário, (E)ndereço ou (O)k/(S)air?
```

Preenchendo formulário da chave

Agora é uma parte importante, você deve escolher a frase que será a base para proteção da chave privada. Assegure-se de nunca esquecê-la, pois você precisará repeti-la em seguida e outras ocasiões. Digite sua frase, tecle ENTER, redigite e tecle ENTER.

Agora irá acontecer algo curioso, uma mensagem pedindo para você gerar bytes para ajudar na codificação das suas chaves. Você deve usar o computador normalmente até liberar pra continuar. Abra o seu navegador, algum jogo, calculadora, leitor de vídeo...


```
root@H4x0r: ~
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

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>"

Nome completo: Ciência Hacker
Endereço de correio eletrônico: cienciahacker@gmail.com
Comentário: Chave principal
Você está usando o conjunto de caracteres `utf-8'.
Você selecionou este identificador de usuário:
    "Ciência Hacker (Chave principal) <cienciahacker@gmail.com>"

Muda (N)ome, (C)omentário, (E)ndereço ou (O)k/(S)air? o
Você precisa de uma frase secreta para proteger sua chave.

Precisamos gerar muitos bytes aleatórios. É uma boa idéia realizar outra
atividade (digitar no teclado, mover o mouse, usar os discos) durante a
geração dos números primos; isso dá ao gerador de números aleatórios
uma chance melhor de conseguir entropia suficiente.

Não há bytes aleatórios suficientes. Por favor, faça algum outro trabalho
para que o sistema possa coletar mais entropia!
(São necessários mais 187 bytes)

"the quieter you become, the more you are able to hear"
```

Gerando bytes para criar as chaves

DICA: Entrar em um site e abrir o VLC costuma ser o suficiente para gerar os bytes.

DICA2: Eu pessoalmente recomendo criar suas chaves somente em ambiente Linux, pelo motivo de que se alguém estiver te espionando e tiver acesso a imagens em sua tela, sua frase de segurança pode ser facilmente descoberta, já no Linux ela não aparecerá, pois é 'invisível' até pra você.

```
root@H4x0r: ~
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

uma chance melhor de conseguir entropia suficiente.

Não há bytes aleatórios suficientes. Por favor, faça algum outro trabalho
para que o sistema possa coletar mais entropia!
(São necessários mais 75 bytes)
..+++++

Não há bytes aleatórios suficientes. Por favor, faça algum outro trabalho
para que o sistema possa coletar mais entropia!
(São necessários mais 128 bytes)
+++++
gpg: /root/.gnupg/trustdb.gpg: banco de dados de confiabilidade criado
gpg: key 543D11FC marked as ultimately trusted
chaves pública e privada criadas e assinadas.

gpg: a verificar a base de dados de confiança
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 2048R/543D11FC 2015-06-30
    Key fingerprint = 2129 4BFA 5719 EF2C AA8D F816 681B 6EFB 543D 11FC
uid      Ciência Hacker (Chave principal) <cienciahacker@gmail.com>
sub 2048R/64D07F50 2015-06-30

"the quieter you become, the more you are able to hear"
root@H4x0r:~#
```

Chave criada com sucesso

Se obtiver sucesso, irá aparecer algo como a imagem acima sendo assim pode continuar.

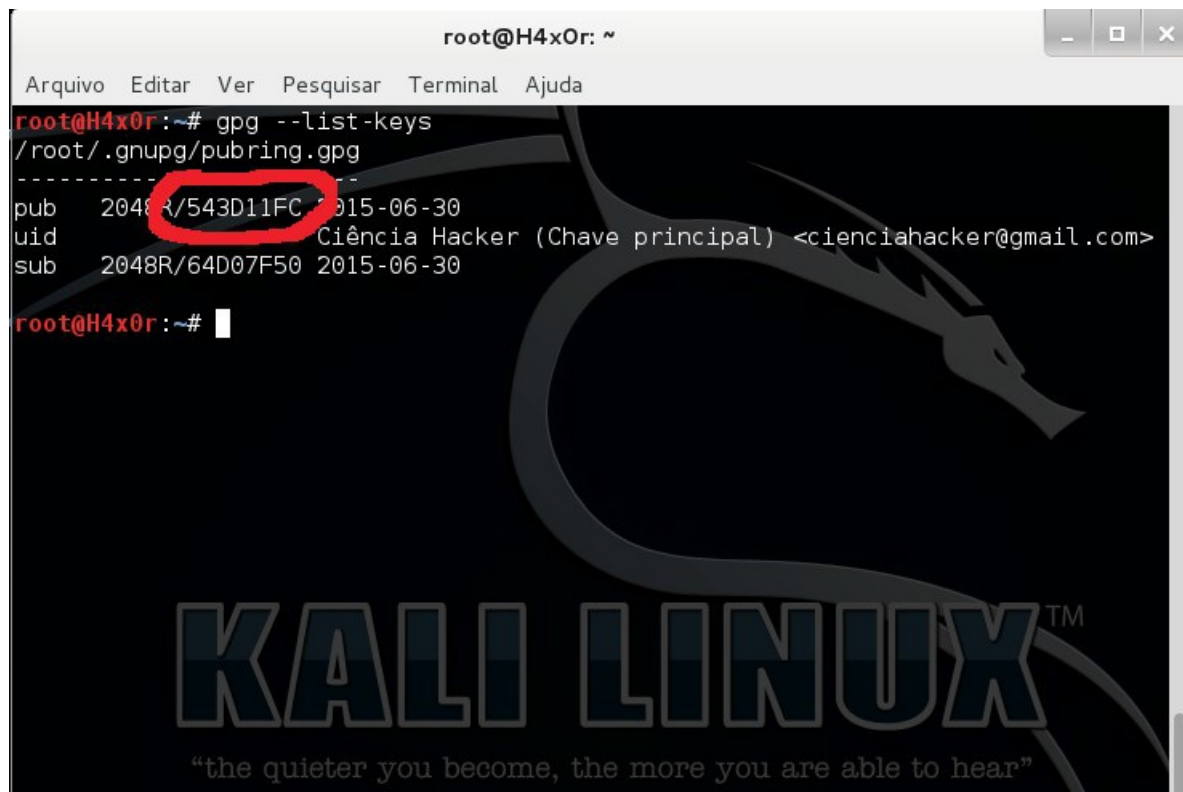
Subindo chaves públicas

Um dos modos de se compartilhar sua chave pública para troca de mensagem é subindo-as para

repositórios específicos. Eles servem para você poder achar facilmente as pessoas, cadastrar suas chaves e excluí-las se necessário. Ele funciona como uma conexão com vários outros servidores, então se você publica sua chave em um, automaticamente é compartilhado com todos participantes da rede globalmente. Para enviar sua chave pública precisamos pegar o ID dela, ou seja, o identificador.

Vamos listar suas chaves usando o comando:

```
gpg --list-keys
```



```
root@H4x0r: ~  
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda  
root@H4x0r:~# gpg --list-keys  
/root/.gnupg/pubring.gpg  
-----  
pub   2048R/543D11FC 2015-06-30  
uid           Ciência Hacker (Chave principal) <cienciahacker@gmail.com>  
sub   2048R/64D07F50 2015-06-30  
root@H4x0r:~#
```

Listando e identificando chave pública

Em destaque é o identificador da sua chave, você irá utilizar no próximo passo.

Agora vamos 'subir' a chave pelo próprio gpg usando o comando que recebe o servidor e o identificador da chave:


```
gpg --keyserver SERVIDOR --send-key ID
```

No exemplo usamos o servidor da FEUP, ficando assim.

```
gpg --keyserver keysrv.fe.up.pt --send-key 543D11FC
```

```
root@H4x0r: ~
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
root@H4x0r:~# gpg --keyserver keysrv.fe.up.pt --send-key
root@H4x0r:~# gpg --list-keys
/root/.gnupg/pubring.gpg
-----
pub   2048R/543D11FC 2015-06-30
uid   Ciência Hacker (Chave principal) <cienciahacker@gmail.com>
sub   2048R/64D07F50 2015-06-30

root@H4x0r:~# gpg --keyserver keysrv.fe.up.pt --send-key 543D11FC
gpg: sending key 543D11FC to hkp server keysrv.fe.up.pt
root@H4x0r:~#
```



KALI LINUX™
"the quieter you become, the more you are able to hear"

Enviando chave pública para serverkey

Se no final o resultado for parecido com isso significa que tudo ocorreu bem.

Links de Keyservers:

[MiT](#)

[FEUP](#)

[RNP](#)

[Surf Net](#)

[Listona](#)

, ,