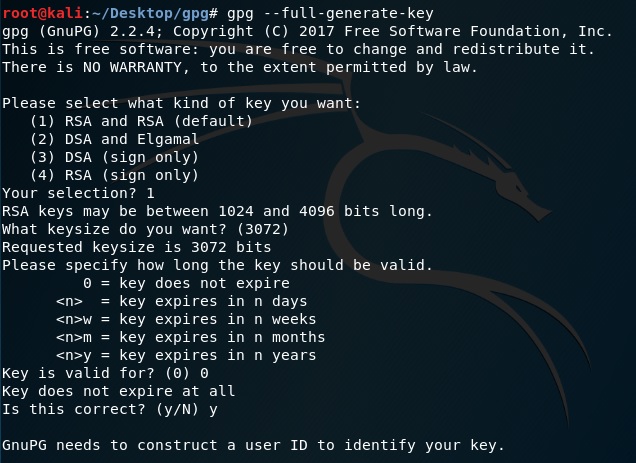
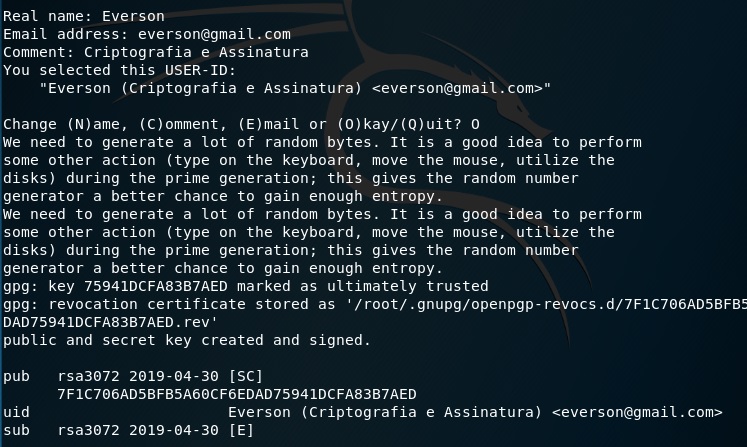
**TUTORIAL GPG (LINUX) E ATIVIDADE:**

**Nome: Igor Correa RA: 15.00588-7**

**Nome: Rodrigo Franciozi RA: 14.04014-0**

1. Criar seu par de chaves (remetente e destinatário):

$ gpg --full-generate-key



2. Listando as chaves públicas e privadas:

2.1. Liste as chaves públicas: $ gpg --list-keys ou gpg --list-public-keys

2.2. Liste as chaves privadas: $ gpg --list-secret-keys

2.3. $gpg --fingerprint (lista as chaves e as impressões digitais)

3.Exportar chave pública:

$ gpg -a --export identificador\_da\_chave > chave\_publica

$ ls -l

$ cat chave\_publica

4.Exportar chave privada:

$ gpg -a --export-secret-key identificador\_da\_chave > chave\_privada

$ ls -l

$ cat chave\_privada

5. Chaveiros Públicos (Keyserver). A chave pública pode ser disponibilizada em um KeyServer (pgp.mit.edu) ou (keys.gnupg.net), de forma que qualquer usuário conectado à Internet terá acesso a mesma.

– Envie sua chave pública: $gpg --keyserver pgp.mit.edu --send-keys identificador

Exemplo:

2E483079D836D37BBBA55B264910B9D6C143CA63...................

$ gpg --keyserver pgp.mit.edu --send-keys 2E483079D836D37BBBA55B264910B9D6C143CA63

– A partir deste momento, sua chave pública está disponível em um KeyServer (pgp.mit.edu) ou (keys.gnupg.net) público da Internet e pode ser utilizada por outras pessoas.

- Para recuperar a chave, digite:

$ gpg --keyserver pgp.mit.edu --recv 2E483079D836D37BBBA55B264910B9D6C143CA63

6. Gerando o Hash de um arquivo (exemplos com md5 e sha256):

- Gerando o Hash com md5 de um arquivo e visualizando:

$ echo arquivo.txt | md5sum > md5sum\_arquivo.txt

$ cat md5sum\_arquivo.txt

- Gerando o Hash com sha256 de um arquivo e visualizando:

$ echo arquivo.txt | sha256sum > sha256sum\_arquivo.txt

$ cat sha256sum\_arquivo.txt

**7. CRIPTOGRAFIA:**

7.1. Usuário remetente baixa chave pública de usuário destinatário para criptografar o arquivo:

$ gpg --keyserver pgp.mit.edu --recv 2E483079D836D37BBBA55B264910B9D6C143CA63

$ gpg -a --export 2E483079D836D37BBBA55B264910B9D6C143CA63 > chave\_publica

$ ls -l

$ cat chave\_publica

7.2. Criptografando o arquivo:

**$ echo “Criptografando o Arquivo” > arquivo.txt**

**$ cat arquivo.txt**

**$ gpg --encrypt --armor -r 2E483079D836D37BBBA55B264910B9D6C143CA63 arquivo.txt**

**$ cat arquivo.txt.asc**

**$ ls -l**

7.3. Usuário remetente envia o arquivo criptografado para o usuário destinatário realizar o procedimento de decriptografia do arquivo:

**$ gpg --decrypt arquivo.txt.asc > arquivo.txt**

**$ ls -l**

**$ cat arquivo.txt**

**8. ASSINATURA DIGITAL:**

8.1. Assine digitalmente um arquivo (usuário remetente). Envio o arquivo assinado para o usuário destinatário.

**$ echo “Assinando o Arquivo” > arquivo.txt**

**$ cat arquivo.txt**

$ gpg --sign arquivo.txt

8.2. Envie sua chave pública para um keyserver:

$ gpg --keyserver pgp.mit.edu --send-keys 2E483079D836D37BBBA55B264910B9D6C143CA63

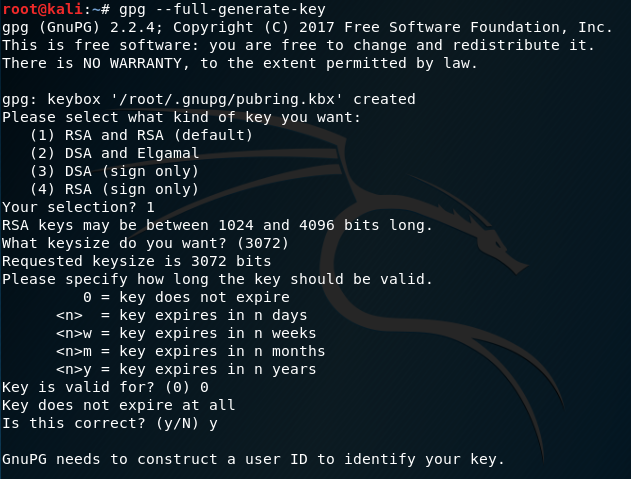
8.3. O usuário destinatário deverá recuperar a chave pública do usuário remetente para verificar o documento assinado, junto do arquivo original:

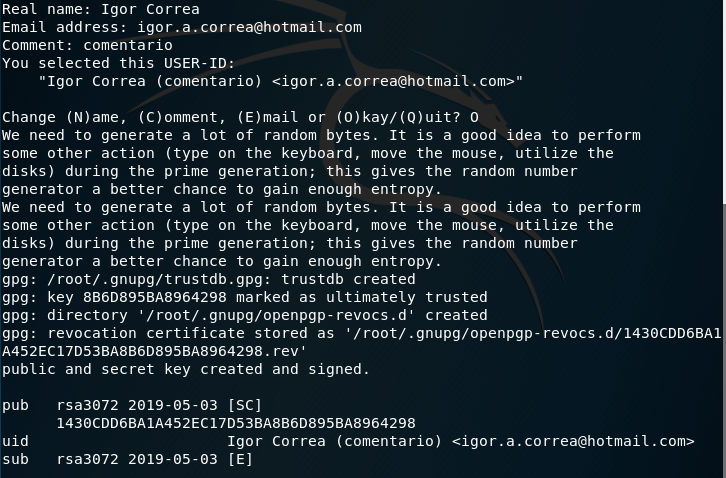
$ gpg --keyserver pgp.mit.edu --recv 2E483079D836D37BBBA55B264910B9D6C143CA63

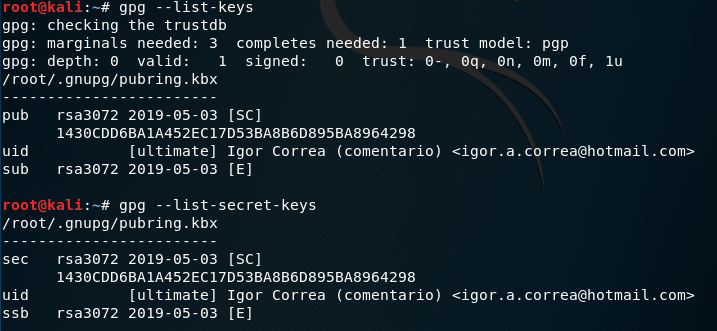
$ gpg --verify arquivo.txt.asc

**9. Atividades para serem realizadas em grupo:**

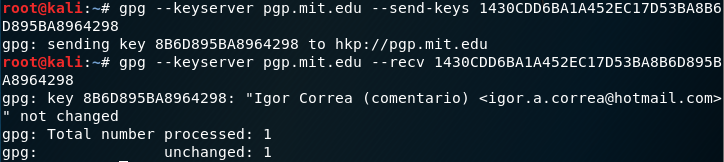
9.1. Gerar um **par de chaves** (remetente e destinatário);







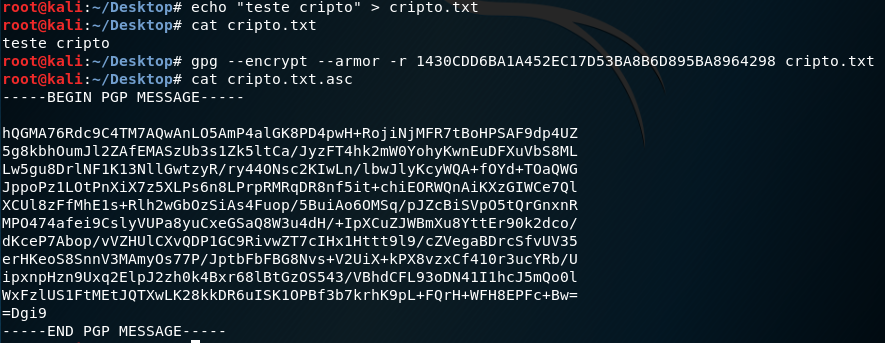
9.2. Enviar a **chave pública** (remetente e destinatário) para um **servidor de chaves**;

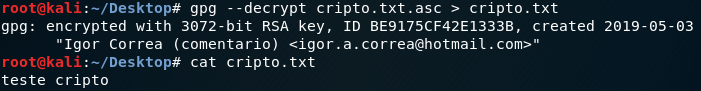


9.3. Um dos componentes do grupo (remetente) deverá recuperar a chave pública e **criptografar** um arquivo e enviar para o usuário do grupo (destinatário) que enviou a chave pública e que é dono da chave privada para testar o procedimento de decriptografia;









9.4. **Assinar** digitalmente um arquivo (remetente) e enviar para outro componente do grupo (destinatário) que deverá **verificar** a assinatura.

Obs: em todos os itens do item 9 deve-se realizar **prints das telas**.

