TUTORIAL GPG (LINUX) E ATIVIDADE:

Nome: Mikael Akira S. MatosRA:

Nome: Vitor Kiomassa Kina RA:

Nome: RA:

1. Criar seu par de chaves:

$ gpg --gen-key

2. Listando as chaves públicas e privadas:

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

2.1. 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), de forma que qualquer usuário conectado à Internet terá

acesso a mesma.

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

armor

Exemplo:

pub 2048R/8BFC95A3 ...................

$ gpg --keyserver pgp.mit.edu --send-keys 8BFC95A3 --armor

– A partir deste momento, sua chave pública está disponível em um KeyServer

(pgp.mit.edu) público da Internet e pode ser utilizada por outras pessoas.

- Para recuperar a chave, digite:

$ gpg --keyserver pgp.mit.edu --recv 8BFC95A3 --armor

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 A baixa chave pública de usuário B para criptografar o arquivo:

$ gpg --keyserver pgp.mit.edu --recv 8BFC95A3 –armor

$ gpg -a --export 8BFC95A3 > chave\_publica

$ ls -l

$ cat chave\_publica

7.2. Criptografando o arquivo:

$ touch arquivo.txt

$ echo “teste” > arquivo.txt

$ cat arquivo.txt

$ gpg --encrypt --armor -r 8BFC95A3 arquivo.txt

$ cat arquivo.txt.asc

$ ls -l

7.3. Usuário A envia o arquivo criptografado para o usuário B 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 A). Envio o arquivo assinado para o

usuário B.

$ gpg --sign --armor arquivo.txt

– Envie sua chave pública para um keyserver:

$ gpg --keyserver pgp.mit.edu --send-keys 8BFC95A3 --armor

8.2. O usuário B deverá recuperar a chave pública do usuário A para verificar o

documento assinado, junto do arquivo original:

$ gpg --keyserver pgp.mit.edu --recv 8BFC95A3

$ gpg --verify arquivo.txt.asc

9. Atividades para serem realizadas em grupo:

9.1. Gerar um par de chaves (um dos componentes do grupo);

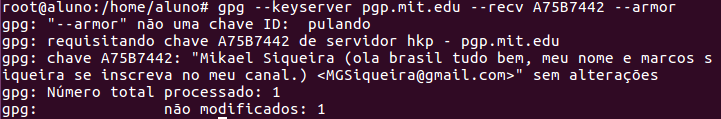






9.2. Enviar a chave pública para um servidor de chaves;

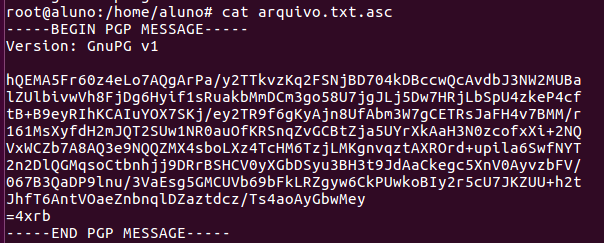


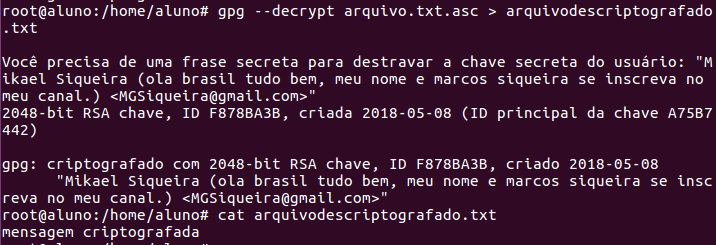


9.3. Um dos componentes do grupo deverá recuperar a chave pública e criptografar um

arquivo e enviar para o usuário do grupo que enviou a chave pública e que é dono da

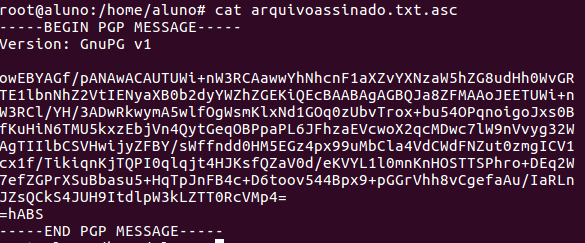
chave privada para testar o procedimento de decriptografia;

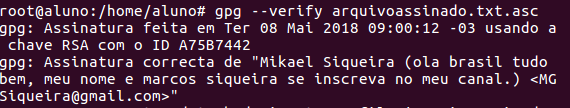




9.4. Assinar digitalmente um arquivo e enviar para outro componente do grupo que

deverá verificar a assinatura.





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