Criptografia e assinatura digital com GnuPG

João Eriberto Mota Filho

Natal, RN, 18 de maio de 2019

Sumário

Sumário

Componentes da criptografia

(Do grego: kriptos=escondido, grifo=grafia/escrever)

- Autenticidade.
- Integridade.
- Confidencialidade (ou sigilo).
- Não repúdio.

Sumário

Tipos de criptografia

- Simétrica
- Assimétrica

Tipos de criptografia

Simétrica

- **Vantagens:**
  - Simplicidade no uso;
  - Grande velocidade nas operações.
- **Desvantagens:**
  - Chave única;
  - Segredo compartilhado;
  - Necessidade de uma chave para cada relação de confiança;
  - Não permite a assinatura e a certificação digital;
  - A chave não pode trafegar livre em canais de comunicação.

Tipos de criptografia

Assimétrica

- **Vantagens:**
  - Utiliza um par de chaves (privada e pública) para todas as relações de confiança;
  - O segredo pessoal (chave privada) não é compartilhado;
  - Permite a assinatura e a certificação digital;
  - A chave pública pode trafegar em canais de comunicação.
- **Desvantagens:**
  - Baixa velocidade nas operações;
  - O seu uso requer conhecimentos mais específicos.

Tipos de criptografia

Exemplo de chave privada

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEA440Is8WIpOvaJzptE91E0yCQt+TeFZIOf4KQTFOOtmwoxv77
rLkM/3QDBl5VUYo3PRE4UyV2ldH+iY77pERHDz3e5SzptFclcc41YjG4AAOAlbKx
97RMHh29qp30j5RVYo6WfS4G9+pIVbZCHt7aCVRIWMmNryIBWOLTDiwP2Be12Y0z
6AOOTmZdRdzgu0zWJfo16TqtrsA7DRMZnM63a6sn7Kjhmd4i6ptgck3RVGs0E6gQ
ZOCion9HJ14YoLPD85Mk8My8CAEI4QJ4vimbnVsawJ3725G5gAG5+l2HZHF8+YEZ
bT5jLDGWoqErZuZaz61z05TdFpsE1alZR2BSQwIBIwKCAQBoBfVZft9hVeAR7tLH
QJR9xb5/85i5Z1cVuAdzWWXPvGppmSKYGhSSCSX0SGGEXHEF+T5R5T2GUV5qxQ
VS
aFr/p0FS0rP6q37U8I1ut6SSSr5wUbBxPHqRbK554c7ijPPVSH9PKvvfDAPPaULM
SJ4wJod5C6578knCO84yXUkSUx6tp53QGEEFEsBYpBCCMkIC94UXS6yiFeGWE2DI
YmdVP9rX5ilClzHlrb5Rp7tUi+q4oTHBi6Ziy5S5huxYhl8WwuZgSvWqc8CEFwcC
wYtUHQkFuWHjV80fveOuy48g1NgiBopyEpsZi2vxbVSMO0cdH98rqeHTQc+M+khq
s74LAoGBAPP0ChzT0sEz3ANsw1HPSCdP6NA3uHHOvf1mJ5RYsvWjWQuPT+ojmGy
V
1jv6ahg7LXGvQ70bQS4pcOhWLSrGwx7Sb8xe1yDzEaoqu2fc0+3GASE5S0tx3h8j
voK5FTgRsz8wtLWNft1XP7l40ZSbrSn2O1iLrAJ3G1auDaHiPStVAoGBAO7JpG3c
+77fcVUXMqrPNr5vk/KOjLI9cmAuoSGNxH+91m2lEX00mvkuWRQlRM9QS7Dwg7Zy
PfiA8Ql7WcjYSrUfWQCfUaGwEimVVLGLTk0PWnXKzSpIY4mm09Uy6wY67KT+XhU
G
NtKNEOEJsG3Yd4VJvGMYZTyhX7gjODj7ufc3AoGBALwxSaE1sTX0zkvI7nJPciz0
gGYcWxX3QhtALSlLvUEmPWCwYjhHWFPEC6qcmvy/79tbUYNA6SOcT8ksiT5BjzUI
vKT4tJXC0xzfItsYETPEocksMsUr9H5sB/5xhWXEgvY7hBcGwPPkOHkisE4RsXgk
Waq048djMljPaZojjkX/AoGADaUfVrwrpIHL9jvXAnI9pHtnijQICi9lnxibfkKd
g6Rypy4A/9cezGkMZ40Z3/X1slbi9HuOgzqRbkGQGhr89Ggw+LillDXyaMa0Yeq0
BGdG/2qso1SX+Ty7pchlM45Wqletms0ntEKTQA8upzDw4wuHG5r+eH4/++TBYleG
+C8CgYEAv+a1mEn5UHonIUzCLg2H1UsK+XddKmuuFYtXyJiVzwbg2wVyeIXoMqrV
Qdx+XcPxLMvBLAe1lNXh5g/PouwmNWT4lGnDTI8egJyvnOn1VBAX6uCguhelmwrb
GpAkMlg1qXTLD09CoeMsfHi3W64cBxLcfuaxLmO6OchShsDNAa8=
-----END RSA PRIVATE KEY-----
```

Tipos de criptografia

Exemplo de chave pública (par da privada anterior)

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEA440Is8WIpOvaJzptE91E0yCQt+TeFZIOf4
KQTFOOtmwoxv77rLkM/3QDBl5VUYo3PRE4UyV2ldH+iY77pERHDz3e5SzptFclcc
41YjG4AAOAlbKx97RMHh29qp30j5RVYo6WfS4G9+pIVbZCHt7aCVRIWMmNryIB
WOLTDiwP2Be12Y0z6AOOTmZdRdzgu0zWJfo16TqtrsA7DRMZnM63a6sn7Kjhmd
4i6ptgck3RVGs0E6gQZOCion9HJ14YoLPD85Mk8My8CAEI4QJ4vimbnVsawJ3725
G5gAG5+l2HZHF8+YEZbT5jLDGWoqErZuZaz61z05TdFpsE1alZR2BSQw==
teste@antares

Sumário

Hash

- Hash é um algoritmo que transforma uma grande quantidade de informações em uma pequena quantidade de informações.
- Cada tipo de hash gera um resultado hexadecimal, de tamanho fixo, baseado em cálculos, bit a bit, sobre o conteúdo de um arquivo qualquer.
- Teoricamente, dois arquivos, com conteúdos diferentes, não poderiam produzir o mesmo hash. Caso essa falha ocorra, diz-se que houve uma colisão.
- Algumas aplicações: armazenamento de senhas em sistemas, tráfego de senhas, conferência rápida de dados e conteúdo.

Hash

- **Exemplo de hash MD5 (16 bytes):**

  # md5sum /etc/profile

  fc332c57412df8923bf0632bdcda30e0

- **Exemplo de hash SHA256 (32 bytes):**

  # sha256sum /etc/profile

  e4dbac2698e0e9c0248ee52bf11537ea10a65e8b64d020826d9d003f8434599e

- **Obs: os hashes MD5 e SHA1 devem ser utilizados com cautela por já terem sido quebrados.**

Sumário

Assinatura digital

- Calcula-se o hash de uma mensagem.
- O hash é assinado (criptografado com a chave privada).
- A mensagem e o hash assinado são enviados para o destinatário.
- Autenticidade, integridade e não-repúdio.
- O conceito de assinatura digital não envolve o sigilo da mensagem. No entanto, este recurso poderá ser adicionado.
- Há a possibilidade de introdução de uma autoridade certificadora (AC ou CA) no processo.

Sumário

O GnuPG

- O PGP (Pretty Good Privacy) foi criado, em 1991, por Philip Zimmermann.
- O GnuPG (GNU Privacy Guard ou GPG) é uma implementação livre do PGP.
- Segue o padrão OpenPGP (RFC 4880, de 2007).
- O GnuPG e o PGP trabalham com o fundamento de confiabilidade mútua, mediante a assinatura de chaves das pessoas pelas pessoas (não há uma CA).
- O GnuPG usa chaves assimétricas, permitindo a criptografia (sigilo) e a assinatura digital.
- Pode ser utilizado em linha de comando ou com programas especiais em inúmeros sistemas operacionais.

Sumário

A utilização do GnuPG (alguns comandos)

- $ gpg --help
- $ gpg --full-generate-key
- $ gpg --list-keys | --list-secret-keys
- $ gpg --list-sigs
- $ gpg --fingerprint
- $ gpg -a --export | --import | --export-secret-keys (perigo!)
- $ gpg --sign-key
- $ gpg -e | -d
- $ gpg --clearsign | --verify
- $ gpg --edit-key
- $ gpg --send-key | --recv-key

A utilização do GnuPG (add-ons)

- **Servidores públicos de chaves públicas.**
- **Mozilla Thunderbird (Icedove) + Enigmail.**
- **Outras opções (inclusive para Windows e Mac): http://www.gnupg.org/related_software/frontends.html**

A utilização do GnuPG (exemplo)

 # cat texto.txt

Este eh um teste.

 # gpg -ear eriberto teste.txt

 # cat teste.txt.asc

-----BEGIN PGP MESSAGE-----

Version: GnuPG v1.4.9 (GNU/Linux)

hQEMA95t4DnBz8JlAQgAjZHFIJlPK9b0aceLy0n1NkgoFbwovBsX1d/tsTzE3MU5z8FXcwo
/9+z510Sd0BEhWXJtpUCOTsG0Ej5u+aLfpgEPJ+DSQJUN1d1lhGmuQBkSHDaVcKKMt7z
FRffHABHlZ1MsfUSGzKGzelxMaIYkVyqWtBuK+JNiAO06AYWdjJHfMdIsxEFqAf/bRr55lx
+6yJa/ou96QawIET+LlrR8uNPtSFy6YjB4vvmRhVpe1y7lAtZezb3TJhzjdz91T1Tl1zWo48Z0
ciy7kVZSgqrouZPhUqfO3ZSpzmvyFDM0AevxL+r0AzNk9raDT7k3m9AOnEC+X825IO0gLo
K5fQBoJ9JRAb/89RyiRTgq4Y4+DJ47j4uqQdo9NhCDL0tGT8xi7FIIwf97XtFKN3ZeMRjd11
YnbBcqW0FO2RZ1BBq+qyWkZ+CJCGvqKiYPaZV8klfqOinu=2VbY

-----END PGP MESSAGE-----

Sumário

Como participar de uma festa GPG

- Criar um par de chaves (utilize o modo expert e RSA).
- Disponibilizar a chave pública em um servidor de chaves.
- Comparecer ao evento portando identidade ou carteira de motorista e cartões ou tiras de papel com o nome completo, e-mail e fingerprint da chave.
- Oferecer o seu documento e o seu cartão para as pessoas, solicitando uma assinatura.
- Conferir, com critério, os dados de quem lhe pedir assinaturas.
- Depois, em casa, buscar as chaves alheias em servidores públicos, assiná-las, exportá-las e enviá-las por e-mail.
- No Debian, o pacote signing-party automatiza o processo.

Como participar de uma festa GPG

- O comando caff auxilia o envio. Veja detalhes de configuração em http://bit.ly/caffexim
- Quando alguém lhe enviar a sua chave assinada, importá-la para o seu chaveiro e enviar para um servidor público.
- Utilize um cartão ou tira de papel com os seus dados para facilitar a troca de informações. Exemplo:

Como participar de uma festa GPG

- Tiras de papel com todos os dados poderão ser preparadas com o comando 'gpg-key2ps -1 <chave>'.
- O gpg-key2ps também é provido pelo pacote signing-party.

Sumário

Conclusão

- Criptografia não é sinônimo de “esconder coisas”.
- O GnuPG é uma forma simples, pessoal e rápida de utilizar a criptografia para obter o sigilo e a assinatura digital.
- O GnuPG pode ser utilizado em linha de comando ou com programas diversos, em vários sistemas operacionais.
- O GnuPG dispensa o uso de CA, uma vez que baseia-se na confiança mútua.

Esta palestra está disponível em:

http://eriberto.pro.br

Siga-me no twitter @eribertomota