



CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA EDUCAÇÃO

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambéa
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

SE
IO



LUIZ GONZAGA FONSECA MOTA
ESCOLA ESTADUAL DE EDUCAÇÃO PROFISSIONAL

Segurança em RDC

Prof. Luis Felipe Oliveira

Aula 03 - Criptografia Simétrica e Assimétrica

Por Definição

Criptografia em segurança virtual é a conversão de dados de um formato legível em um formato codificado.

Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados.

A criptografia é um elemento fundamental da segurança de dados.

CRİPTOGRAFIA

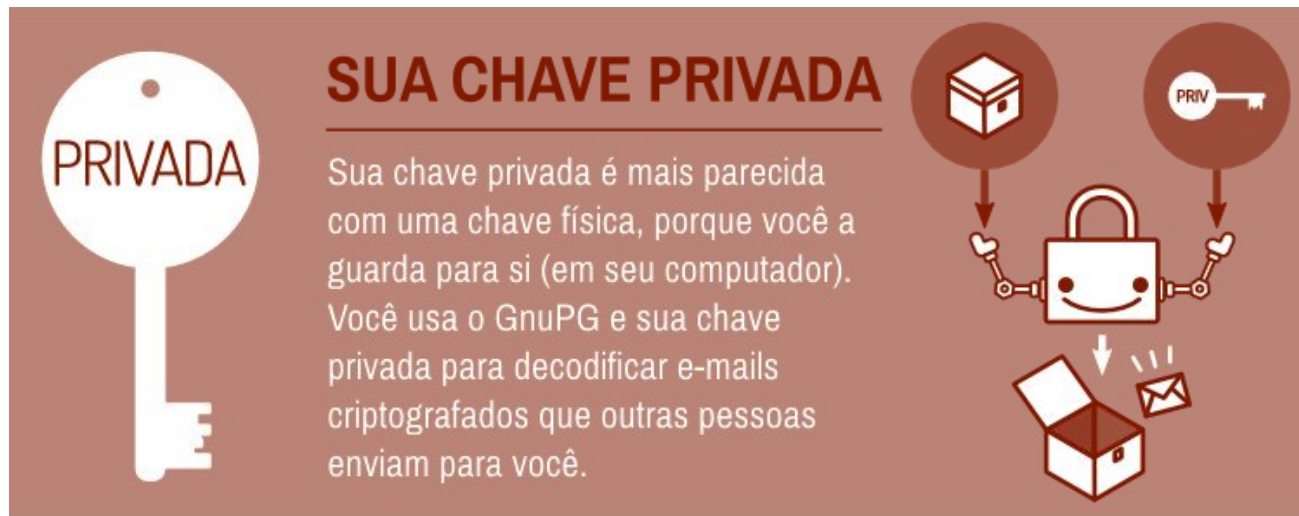
SİMÉTRICA X ASSİMÉTRICA

desenvolvedor.so

desenvolvedor

Chave Pública e Chave Privada

Chave Privada



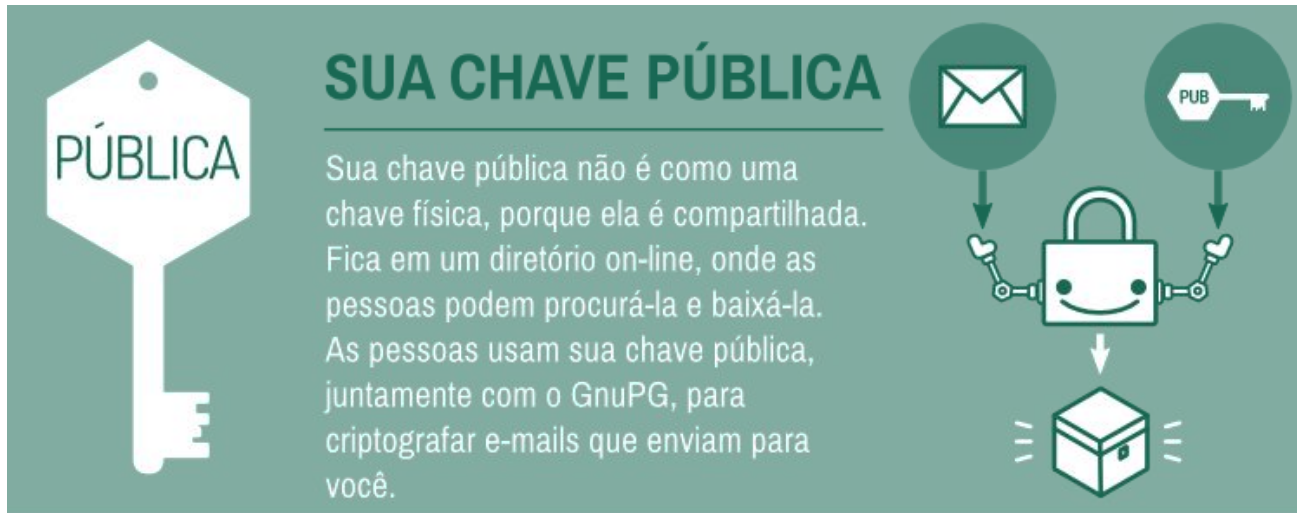
SUA CHAVE PRIVADA

Sua chave privada é mais parecida com uma chave física, porque você a guarda para si (em seu computador). Você usa o GnuPG e sua chave privada para decodificar e-mails criptografados que outras pessoas enviam para você.

O sistema de chave privada consiste em encriptar uma mensagem usando uma chave criptográfica secreta, que é apenas conhecida pelo emissor e pelo receptor da mensagem.

Chave Pública

O sistema de chave pública funciona no sentido de que cada entidade (uma pessoa ou um computador)



SUA CHAVE PÚBLICA

Sua chave pública não é como uma chave física, porque ela é compartilhada. Fica em um diretório on-line, onde as pessoas podem procurá-la e baixá-la. As pessoas usam sua chave pública, juntamente com o GnuPG, para criptografar e-mails que enviam para você.

envolvida na transmissão deve possuir duas chaves: a sua própria chave secreta (também chamada de chave privada), que não é de conhecimento de mais ninguém e uma chave pública que é de conhecimento geral, inclusive de quem não faz parte da transmissão.

Criptografia Simétrica

Criptografia Simétrica

O termo simétrico é dado porque nos dois lados da transmissão a chave que é usada para encriptar é a mesma usada para decryptar uma mensagem.

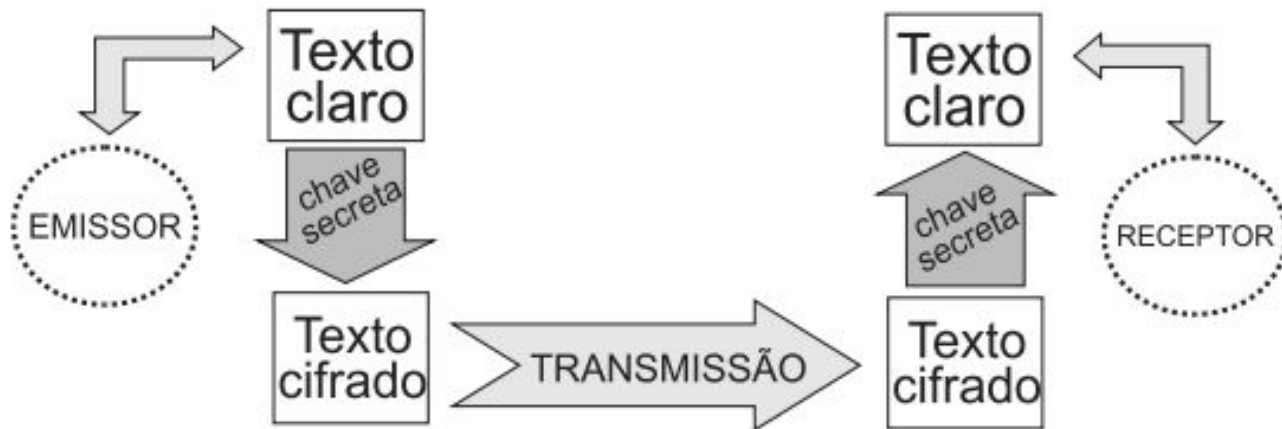


Figura 3a. Criptografia simétrica

Criptografia Simétrica

A criptografia simétrica usa a mesma chave tanto para criptografar como para descriptografar dados. Os algoritmos que são usados para a criptografia simétrica são mais simples.

Todas as partes que enviam e recebem os dados devem conhecer ou ter acesso à chave de criptografia. A criptografia simétrica fornece autorização para dados criptografados.

Por exemplo, uma organização pode estar razoavelmente certa de que apenas as pessoas autorizadas a acessar a chave de criptografia compartilhada podem descriptografar o texto codificado. No entanto, a criptografia simétrica não fornece não-repúdio.

Criptografia Simétrica

Por exemplo, em um cenário em que vários grupos têm acesso à chave de criptografia compartilhada, a criptografia simétrica não pode confirmar o grupo específico que envia os dados. Os algoritmos de criptografia usados na criptografia simétrica incluem o seguinte:

NRC2 (128 bits)

N3DES (Triple Data Encryption Standard, Padrão triplo de criptografia de dados)

NAES (Padrão de criptografia avançada)

Criptografia Simétrica

Mesma chave para cifrar e decifrar | Mais rápida | Problema de distribuição de chave



Criptografia Assimétrica

Criptografia Assimétrica

Na **criptografia assimétrica** a chave usada para encriptar uma mensagem é diferente da chave usada para decifrar, daí o termo assimétrico.

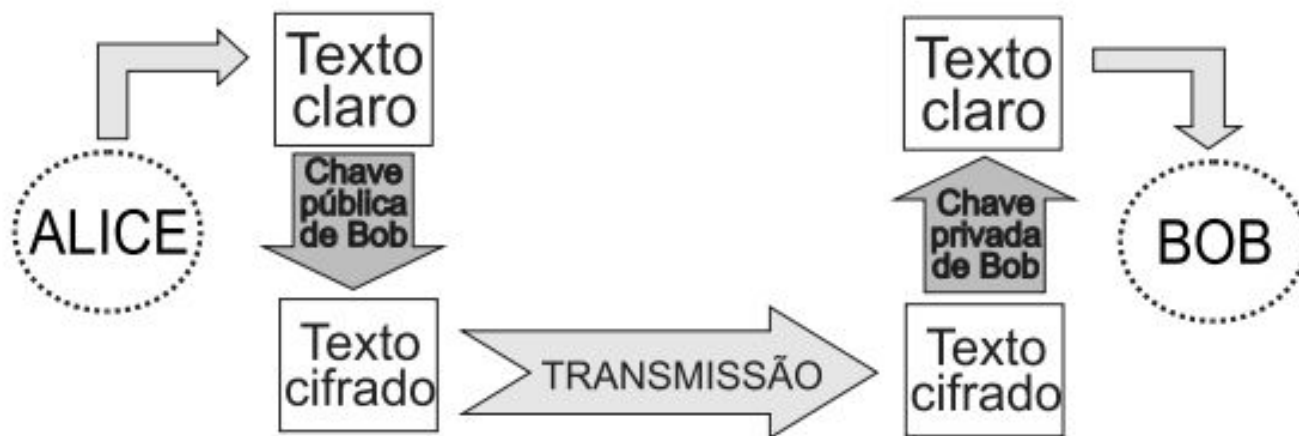


Figura 3b. Criptografia assimétrica.

Criptografia Assimétrica

A criptografia assimétrica usa duas chaves diferentes, porém matematicamente relacionadas, para criptografar e descriptografar dados

Essas chaves são conhecidas como chaves privadas e chaves públicas. Em conjunto, essas chaves são conhecidas como par de chaves.

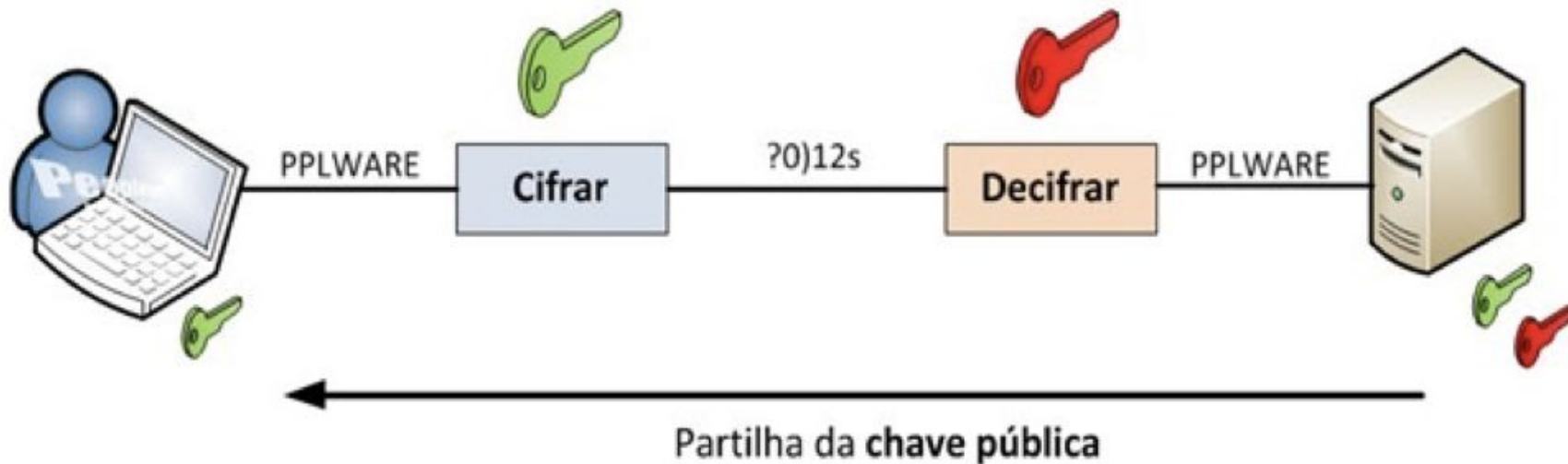
A criptografia assimétrica é considerada mais segura do que a criptografia simétrica, porque a chave usada para criptografar os dados é diferente da que é usada para descriptografá-los.

Contudo, como a criptografia assimétrica usa algoritmos mais complexos do que a simétrica, e como a criptografia assimétrica usa um par de chaves, o processo de criptografia é muito mais lento quando uma organização usa a criptografia assimétrica do que quando usa a simétrica.

Criptografia Assimétrica

Com a criptografia assimétrica, somente uma parte mantém a chave privada. Essa parte é conhecida como o **assunto**. Todas as outras partes podem acessar a chave pública. Os dados criptografados por meio da chave pública só podem ser descriptografados com o uso da chave privada. Por outro lado, os dados criptografados por meio da chave privada só podem ser descriptografados com o uso da chave pública. Por conseguinte, esse tipo de criptografia fornece confidencialidade e não-repúdio.

Criptografia Assimétrica



Criptografia Assimétrica

Os algoritmos de criptografia usados na criptografia assimétrica incluem o seguinte:

Acordo de chaves de Diffie-Hellman | NRSA (Rivest-Shamir-Adleman) | NDSA (Algoritmo de assinatura digital)

Exemplos:

Curvas elípticas Diffie-Hellman | DSA de curvas elípticas El Gamal | RSA

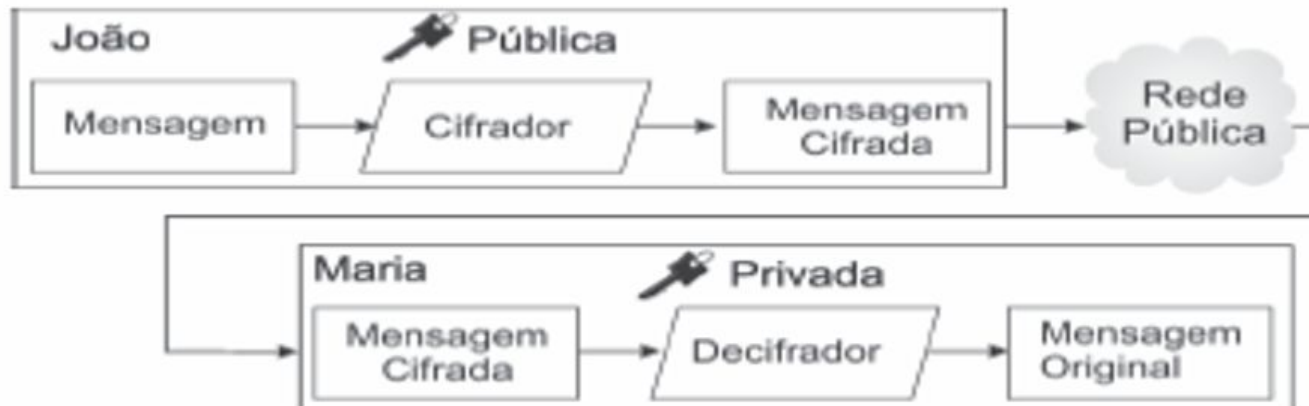
Criptografia Assimétrica

Criptografia de Chave Pública

Duas Chaves (uma privada e outra pública)

Pode garantir confidencialidade ou autenticidade

Mais lenta (Problema de desempenho)



Atividade

O que é Criptografia? Dê um exemplo simples de mecanismos primitivos de criptografia.

O que é Chave Privada? Qual a criptografia gerada por ela?

O que é Chave Pública? Qual a criptografia gerada por ela?

O que é Criptografia Simétrica. Cite exemplos

O que é Criptografia Assimétrica. Cite exemplos