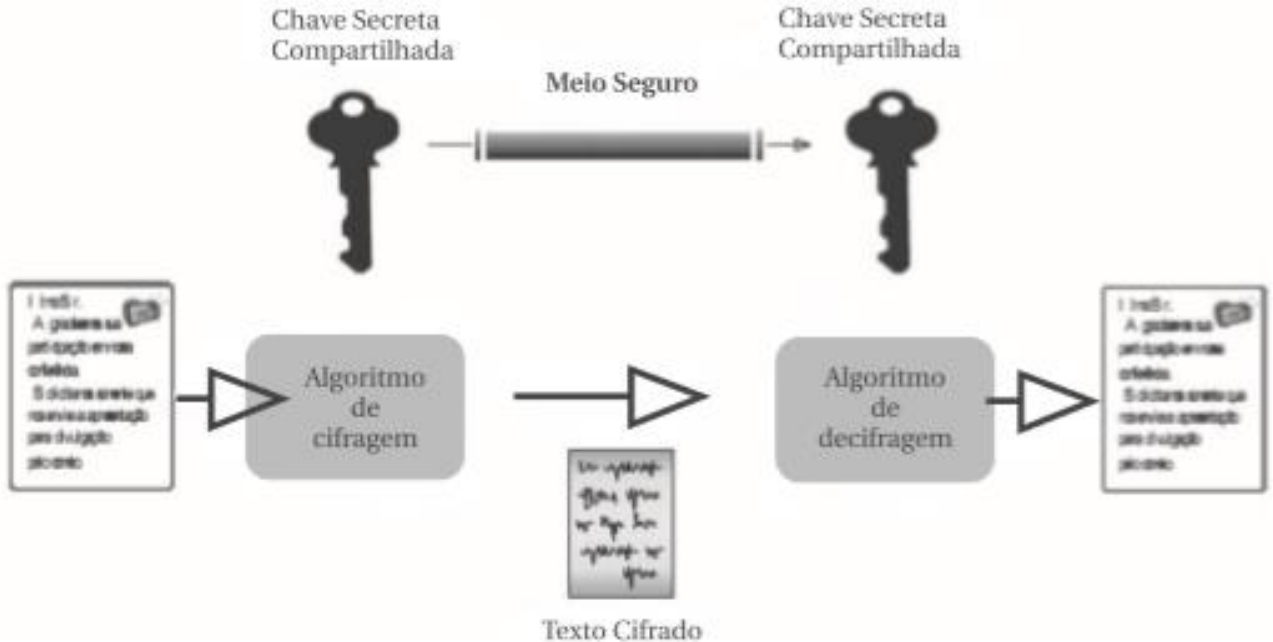
By @kakashi_copiador

Segurança da Informação: Criptografia

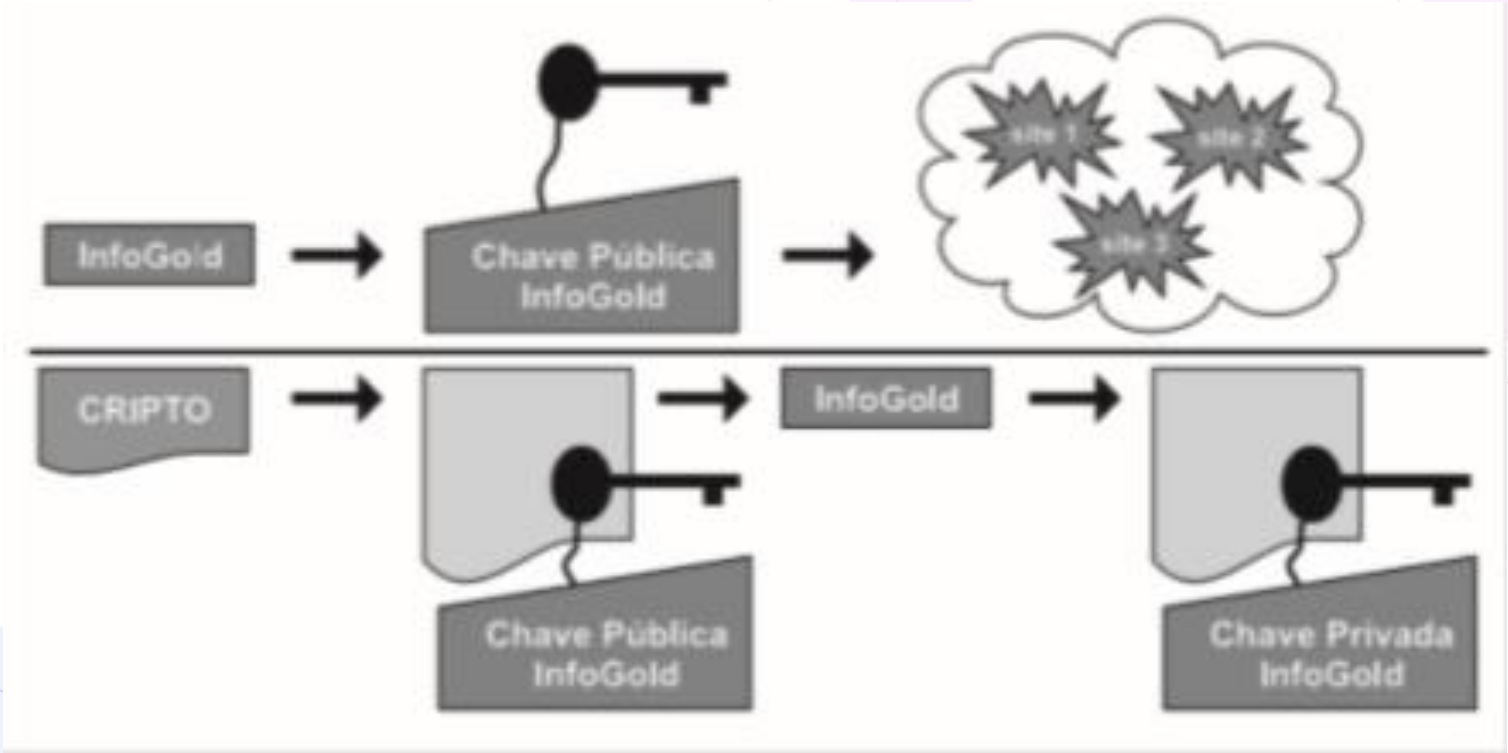
Prof. Renato da Costa

Criptrografia Simétrica



Retirada do livro "Introdução à Certificação Digital da Criptografia ao Carimbo de Tempo"

Criptrografia Assimétrica



Prefeitura de Boa Vista - 2020

Um método de criptografia possui as características listadas a seguir.
É similar ao processo de assinatura digital, existindo uma função matemática que criptografa a mensagem. As chaves usadas para criptografar e decriptografar são diferentes. A mensagem é criptografada com a chave pública do destinatário, para que qualquer entidade possa lhe enviar mensagens criptografadas. A mensagem cifrada é decriptografada com a chave privada do destinatário, para que apenas ele possa abrir a mensagem. A relação matemática entre as chaves precisa ser bem definida para que se possa criptografar a mensagem sem o conhecimento da chave que irá decriptografá-la.
Esse método é denominado criptografia de chave:

...

Prefeitura de Boa Vista - 2020

...

A) reversa

B) cruzada

C) simétrica

D) assimétrica

Abin

No modelo de criptografia simétrica, o texto encriptado poderá ser lido sem que se tenha a chave de encriptação utilizada.
( ) CERTA ( ) ERRADA

Abin

Na criptografia assimétrica, as duas partes comunicantes compartilham a mesma chave, que precisa ser protegida contra acesso por outras partes.

( ) CERTA ( ) ERRADA

PC MG

A criptografia simétrica é um método de codificação que utiliza

A) chaves públicas e privadas para encriptar e desencriptar as mensagens.

B) duas chaves privadas para encriptar e desencriptar as mensagens.

C) duas chaves públicas para encriptar e desencriptar a mesma mensagem.

D) uma única chave para encriptar e desencriptar as mensagens.

Auditor PB

Criptografia simétrica é um método de codificação que utiliza
(A) uma chave pública e uma chave privada para encriptar e decodificar a mesma mensagem.
(B) duas chaves públicas para encriptar e decodificar a mesma mensagem.
(C) uma só chave para encriptar e decodificar a mesma mensagem.
(D) duas chaves privadas para encriptar e decodificar a mesma mensagem.
(E) uma chave pública e duas chaves privadas para encriptar e decodificar a mesma mensagem.

Banco do Brasil

Uma mensagem enviada de X para Y é criptografada e decriptografada, respectivamente, pelas chaves:

a) publica de Y (que X conhece) e privada de Y.
b) pública de Y (que X conhece) e privada de X.
c) privada de X (que Y conhece) e privada de Y.
d) privada de X (que Y conhece) e pública de X.
e) privada de Y (que X conhece) e pública de X.

DETRAN ACRE

Roni deseja enviar uma mensagem confidencial (encriptada) ao seu colega de trabalho Luiz. Para obter essa propriedade, Roni deve utilizar a

(A) chave privada de Luiz.
(B) chave pública de Luiz.
(C) chave privada dos dois.
(D) sua própria chave privada.
(E) sua própria chave pública.

IFF

Determinada forma de criptografia, conhecida como criptografia de chave pública, transforma o texto claro em texto cifrado usando uma chave e um algoritmo, e pode ser usada tanto para confidencialidade quanto para autenticação. Essas são características da

a) criptografia que utiliza o algoritmo DES.
b) criptografia simétrica.
c) criptografia assimétrica.
d) criptografia que utiliza o algoritmo AES.
e) criptografia que utiliza a cifra de César.

Prefeitura de Pilõezinhos

Sobre criptografia simétrica e assimétrica, considere as afirmações a seguir:
I- Na criptografia simétrica, a mesma chave é usada para criptografar e descriptografar.
II- Na criptografia assimétrica, há chaves diferentes para criptografar e descriptografar.
III- Algoritmos como DES, 3DES, AES e RC4 são de criptografia simétrica.
Está CORRETO o que se afirma em

a)I e II.
b)I e III.
c)II e III.
d)I, II e III.
e)II.

Prefeitura de Niterói

A criptografia é considerada a ciência e a arte de escrever mensagens em forma cifrada ou em código, constituindo um dos principais mecanismos de segurança que se pode usar para se proteger dos riscos associados ao uso da internet. De acordo com o tipo de chave usada, os métodos criptográficos podem ser subdivididos em duas grandes categorias, descritas a seguir.

...

Prefeitura de Niterói

...

(1) Utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados. Casos nos quais a informação é codificada e decodificada por uma mesma pessoa, não há necessidade de compartilhamento da chave secreta. Entretanto, quando estas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro (para não comprometer a confidencialidade da chave). Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, RC4, 3DES e IDEA.

...

Prefeitura de Niterói

...

(2) Utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade ou autenticação, integridade e não repúdio. A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um smartcard ou um token. Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA, ECC e Diffie-Hellman.

...

Prefeitura de Niterói

...

Os métodos descritos em (1) e em (2) são denominados, respectivamente, criptografia de chave:

a)direta e indireta
b)digital e analógica
c)hashing e hamming
d)reservada e secreta
e)simétrica e assimétrica

STJ

Na troca de mensagens entre duas empresas parceiras, a autenticidade e o sigilo das informações trocadas podem ser garantidos com o uso de criptografia simétrica.

( ) CERTA ( ) ERRADA