



**By @kakashi\_copiador**



# SEGURANÇA DA INFORMAÇÃO: PRINCÍPIOS BÁSICOS

## IMBEL – FGV - 2021

Segundo padrões internacionais, a Segurança da Informação distingue quatro atributos básicos que orientam a implementação de políticas e procedimentos de proteção.

Assinale o atributo que não é parte desse grupo.

- A) Autenticidade.
- B) Completude.
- C) Confidencialidade.
- D) Disponibilidade.
- E) Integridade.

## IMBEL – FGV - 2021

Segundo padrões internacionais, a Segurança da Informação distingue quatro atributos básicos que orientam a implementação de políticas e procedimentos de proteção.

Assinale o atributo que não é parte desse grupo.

- A) Autenticidade.
- B) Confidencialidade.
- C) Disponibilidade.
- D) Flexibilidade.
- E) Integridade.

## TJ TO – FGV - 2022

Em segurança da informação, a criptografia de chave simétrica é utilizada para garantir o requisito básico de segurança:

- A) confidencialidade;
- B) disponibilidade;
- C) integridade;
- D) autenticidade;
- E) não repúdio.

## TJ DFT – FGV - 2022

Ana precisa enviar a mensagem  $M$  para Bráulio de forma sigilosa pela rede do Tribunal de Justiça atendendo aos requisitos de segurança: autenticidade, não repúdio, integridade e confidencialidade. Para isso, Ana deve enviar uma chave secreta  $K$  para Bráulio e gerar uma assinatura digital  $AD(M)$ .

Considerando que a chave  $K$  deve ser conhecida apenas por Ana e Bráulio, após esse processo deve-se cifrar  $K$  e  $AD(M)$  com a chave:

- A) privada de Bráulio;
- B) privada de Ana;
- C) pública de Ana;
- D) pública de Bráulio;
- E) secreta de Ana.

## AL RO – FGV - 2018

João quer enviar uma mensagem para Maria, mas assegurar que somente Maria será capaz de lê-la.

Então, João deve utilizar

- A) uma criptografia de chave pública e aplicar a chave-pública de Maria para fazer o ciframento da mensagem.
- B) uma criptografia assimétrica e aplicar a chave-privada de Maria para fazer o ciframento da mensagem.
- C) uma criptografia simétrica para fazer o ciframento da mensagem e não compartilhar a chave criptográfica.
- D) uma criptografia assimétrica para João colocar sua assinatura digital na mensagem.
- E) uma função de dispersão criptográfica para cifrar a mensagem e informar a Maria o algoritmo utilizado.

## SEFAZ BA – FGV - 2022

Os métodos criptográficos, de acordo com a chave utilizada, podem ser classificados em duas categorias: criptografia de chave simétrica e criptografia de chaves assimétricas.

Assinale a opção que indica um exemplo de método criptográfico da categoria que utiliza chaves assimétricas.

- A) Blowfish.
- B) RSA.
- C) 3DES.
- D) IDEA.
- E) AES.




# RSA (sistema criptográfico)

---

[Artigo](#) [Discussão](#)

---

Origem: Wikipédia, a enciclopédia livre.

 **Nota:** Se procura a empresa, veja [RSA Data Security, Inc.](#).

**RSA (Rivest-Shamir-Adleman)** é um dos primeiros [sistemas de criptografia de chave pública](#) e é amplamente utilizado para transmissão segura de dados. Neste [sistema de criptografia](#), a [chave de encriptação](#) é pública e é diferente da [chave de deciptação](#) que é secreta (privada). No RSA, esta assimetria é baseada na dificuldade prática da [fatorização](#) do produto de dois [números primos](#) grandes, o "[problema de fatoração](#)". O [acrônimo](#) RSA é composto das letras iniciais dos sobrenomes de [Ron Rivest](#), [Adi Shamir](#) e [Leonard Adleman](#), fundadores da atual empresa [RSA Data Security, Inc.](#), os quais foram os primeiros a descrever o algoritmo em 1978. [Clifford Cocks](#), um matemático Inglês que trabalhava para a agência de inteligência britânica [Government Communications Headquarters](#) (GCHQ), desenvolveu um sistema equivalente em 1973, mas ele não foi [revelado](#) até 1997.<sup>[1]</sup>

É considerado dos mais seguros, já que mandou por terra todas as tentativas de quebrá-lo. Foi também o primeiro algoritmo a possibilitar criptografia e assinatura digital, e uma das grandes inovações em [criptografia de chave pública](#).

## TJ TO – FGV - 2022

A equipe de segurança de um órgão público está em busca de um algoritmo de criptografia que possua as seguintes características:

- (i) duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono; e
- (ii) quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la.

De acordo com as características desejadas pela equipe de segurança, o algoritmo de criptografia que deve ser usado é o:

- A) RC4;
- B) DES triplo;
- C) SHA-256;
- D) Twofish;
- E) RSA.

## BANESTES – FGV - 2021

Uma técnica de criptografia largamente empregada para garantir segurança em transações digitais, que utiliza uma chave pública para ciframento de dados e uma outra chave privada para deciframento desses dados previamente cifrados, é:

- A) DES;
- B) AES;
- C) RSA;
- D) SHA;
- E) MD5.

## SEPOG RO – FGV - 2017

Para fazer o controle de integridade e autenticidade de uma mensagem que será enviada para o servidor S, dentre os padrões de assinatura digital, o cliente C deve calcular o resumo (digest) da mensagem e, em seguida, deve criptografar esse resumo com

- A) sua chave pública.
- B) sua chave privada.
- C) a chave pública do servidor S.
- D) a chave privada do servidor S.
- E) a chave pública do servidor S combinada com sua chave pública.

## MPE AL – FGV - 2018

Em muitas transações financeiras realizadas pela Internet é necessário que o usuário, além de fornecer o seu e-mail e senha, digite um código gerado ou recebido em seu celular. Essa tecnologia é conhecida como

- A) biometria.
- B) cartão inteligente.
- C) certificado digital.
- D) criptografia.
- E) token de segurança.

## MPE BA – FGV - 2017

Em relação à assinatura e à certificação digital, analise as afirmativas a seguir.

- I. A assinatura digital não garante o sigilo das informações.
- II. O certificado digital permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos.
- III. A assinatura digital assegura a integridade da mensagem, ou seja, sempre que houver qualquer alteração, o destinatário terá como percebê-la.

Está correto o que se afirma em:

- A) somente I;
- B) somente II;
- C) somente III;
- D) somente II e III;
- E) I, II e III.

## PGE RO – FGV - 2015

Em relação à assinatura digital, analise as afirmativas a seguir:

- I . Para que um documento ou uma assinatura adulterada não seja detectada, é necessário que o autor da alteração tenha acesso à chave pública de quem assinou a mensagem.
- II . As assinaturas digitais são passíveis de verificação por meio de chaves privadas.
- III . Uma função Message Digest pode ser utilizada para assegurar a integridade da mensagem, permitindo, desse modo, identificar se a mensagem foi modificada, mas não o que foi modificado e o quanto foi modificado.

...

## PGE RO – FGV - 2015

...

Está correto o que se afirma em:

- A) somente I;
- B) somente II;
- C) somente III;
- D) somente II e III;
- E) I, II e III.