
Brasiljurídico
CURSOS JURÍDICOS

INFORMÁTICA - 03

PROF. RAYMUNDO PENNA

Segurança da Informação

ELEMENTOS DA SEGURANÇA DA INFORMAÇÃO

Serviço	Descrição
Disponibilidade	**Garante que as informações estarão sempre disponíveis para atender às requisições.**
Privacidade (Sigilo ou Confidencialidade)	**Impede que pessoas não autorizadas tenham acesso ao conteúdo da mensagem.**
Autenticidade	**Garante a identidade do remetente.**
Integridade	**Garantia de que o conteúdo da mensagem não foi alterado.**
Não-Repúdio (Irretratabilidade)	**Previne que o remetente negue a autoria do envio da mensagem.**
Confiabilidade	**Garantia de que os sistemas funcionarão como esperado pelo usuário,**

PRINCIPAIS CARACTERÍSTICAS

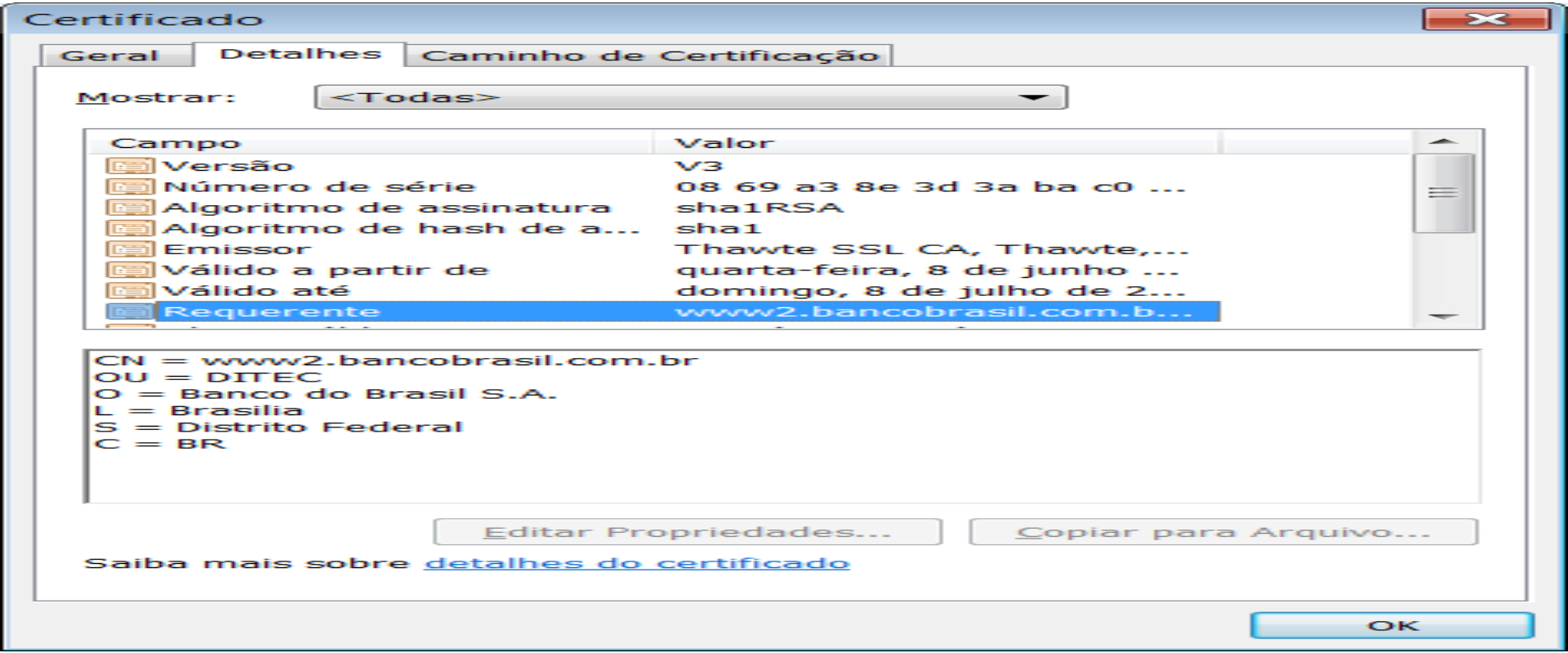
Certificado Digital

- Algoritmo de Chave Assimétrica
- Criptografia
- Assinatura Digital

Assinatura Digital

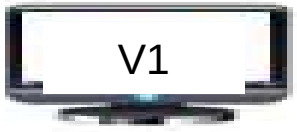
- Autenticidade
- Integridade
- Não-Repúdio

Certificado do Banco do Brasil

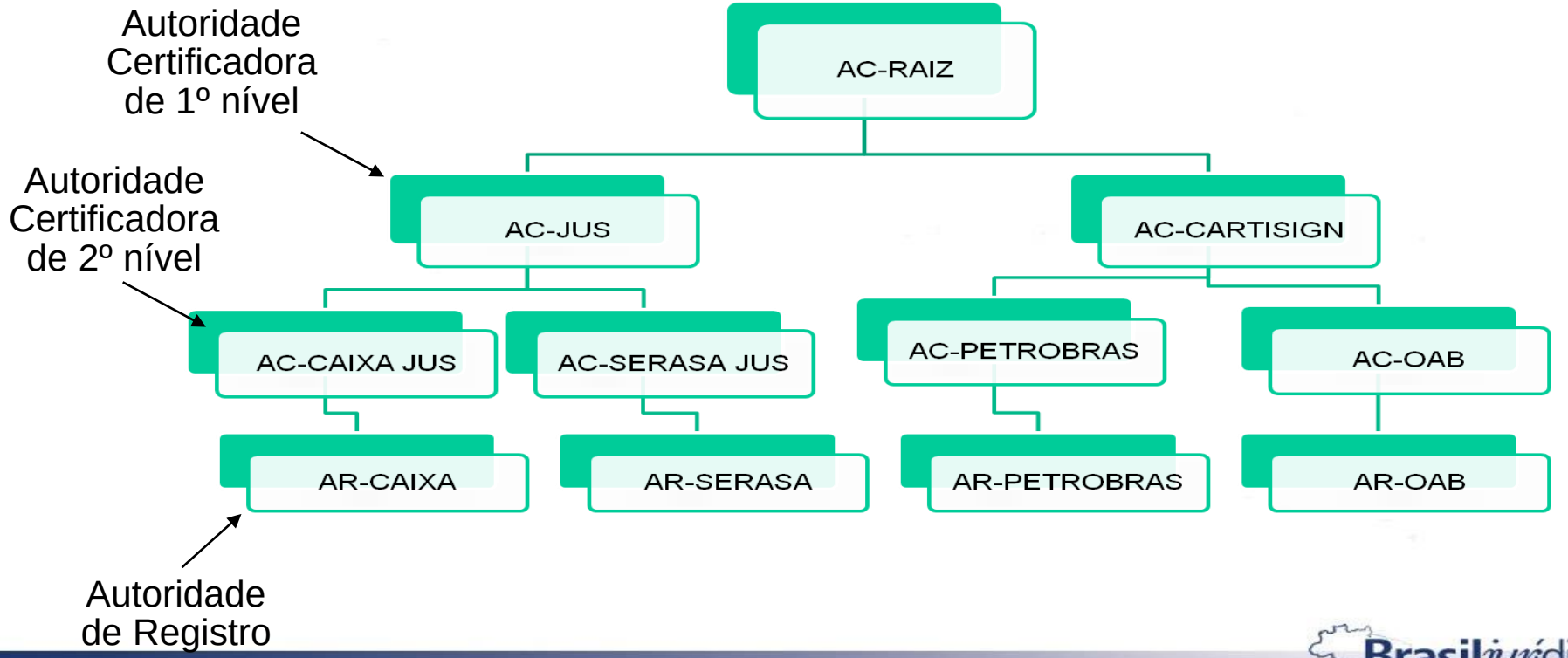


TIPOS DE CERTIFICADOS DIGITAIS

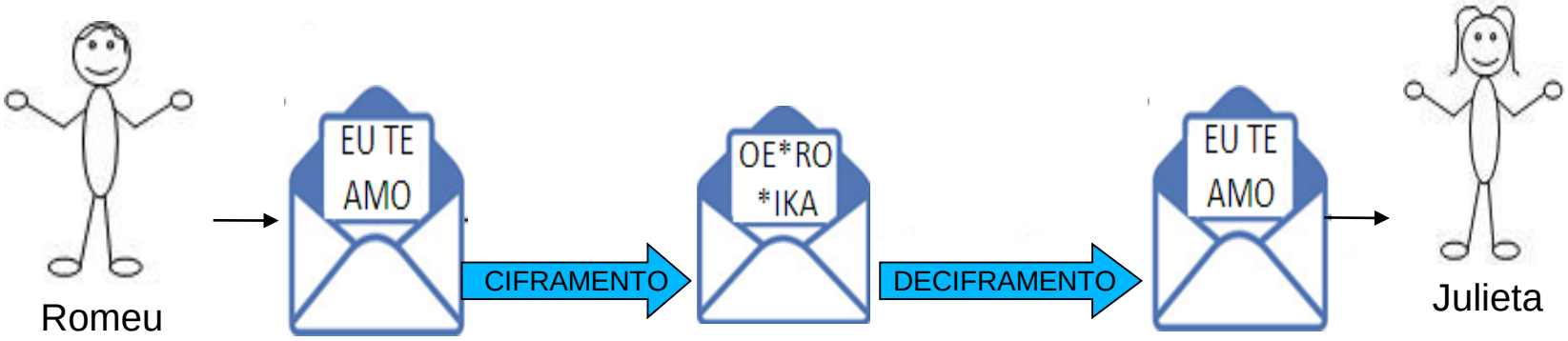
Tipos de Certificados	Local de Armazenamento	Validade do Certificado	Tamanho da Chave
V1	Repositório (normalmente no HD do usuário)	Máxima 1 ano	Até 1024 bits
V2	Token ou Smart Card	Máxima 2 anos	Mínimo de 1024 bits
V3	Token ou Smart Card	Máxima 3 anos	Mínimo de 1024 bits
V4	Token ou Smart Card	Máxima 3 anos	Mínimo de 2048 bits



ICP-Brasil: Infra Estrutura de Chaves Públicas Brasileiras

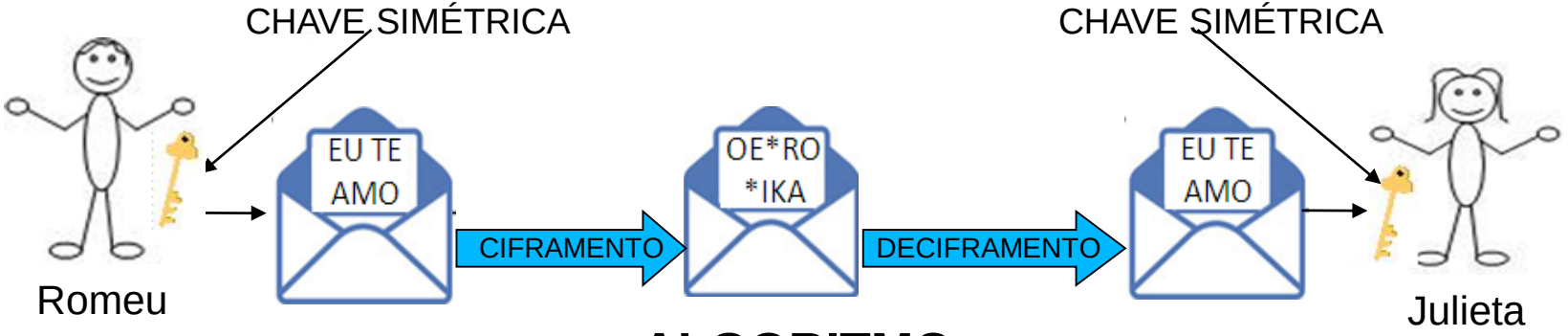


ALGORITMO DE CRIPTOGRAFIA



ALGORITMO:
VOGAIS: + 2 POSIÇÕES
CONSOANTES: - 2 POSIÇÕES
ESPAÇO: *

ALGORITMO DE CRIPTOGRAFIA E UMA CHAVE SIMÉTRICA



ALGORITMO:

VOGAIS: + 2 POSIÇÕES

CONSOANTES: - 2 POSIÇÕES

ESPAÇO: *

CHAVE SIMÉTRICA DE 56 BITS (72 quadrilhões de Combinações)

00111000101011100000011110001010011111100011110000011 1

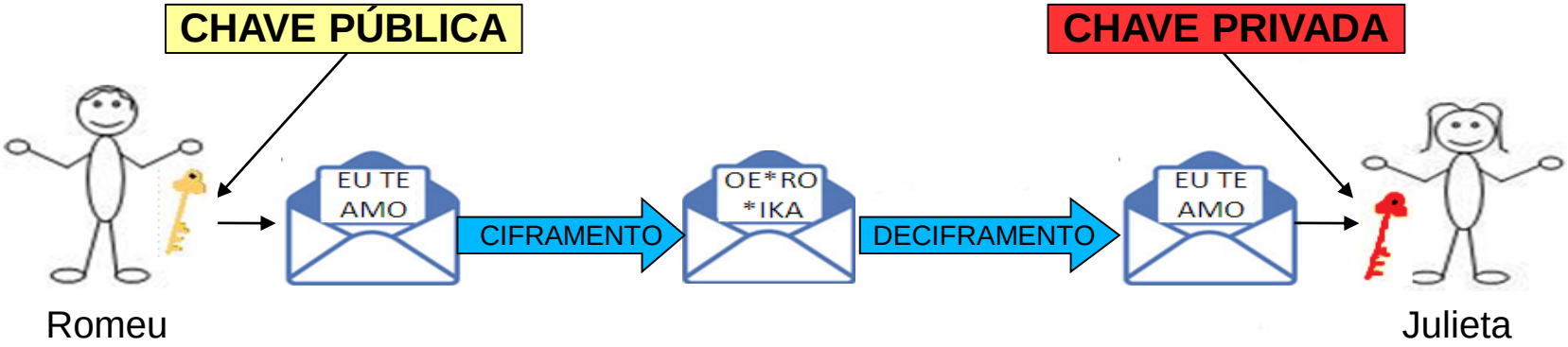
CHAVE SIMÉTRICA

POSSUI UMA ÚNICA CHAVE COMPARTILHADA

CRIPTOGRAFAR MENSAGENS
ASSINAR DIGITALMENTE AS MENSAGENS

DECRIPTOGRAFAR MENSAGENS
VALIDAR A ASSINATURA DIGITAL DAS MENSAGENS

ALGORITMO DE CRIPTOGRAFIA E UMA CHAVE ASSIMÉTRICA



ALGORITMO:
VOGAIS: + 2 POSIÇÕES
CONSOANTES: - 2 POSIÇÕES
ESPAÇO: *
CHAVE ASSIMÉTRICA DE 1024 OU 2048 BITS OU MAIOR

CHAVES ASSIMÉTRICAS (PÚBLICA)

POSSUI UM PAR DE CHAVES DISTINTAS

CHAVE PÚBLICA

CRIPTOGRAFAR MENSAGENS
VALIDAR A ASSINATURA DIGITAL DAS MENSAGENS

CHAVE PRIVADA

DECRIPTOGRAFAR MENSAGENS
ASSINAR DIGITALMENTE AS MENSAGENS

COMPARAÇÃO ENTRE CHAVES: SIMÉTRICA X ASSIMÉTRICA

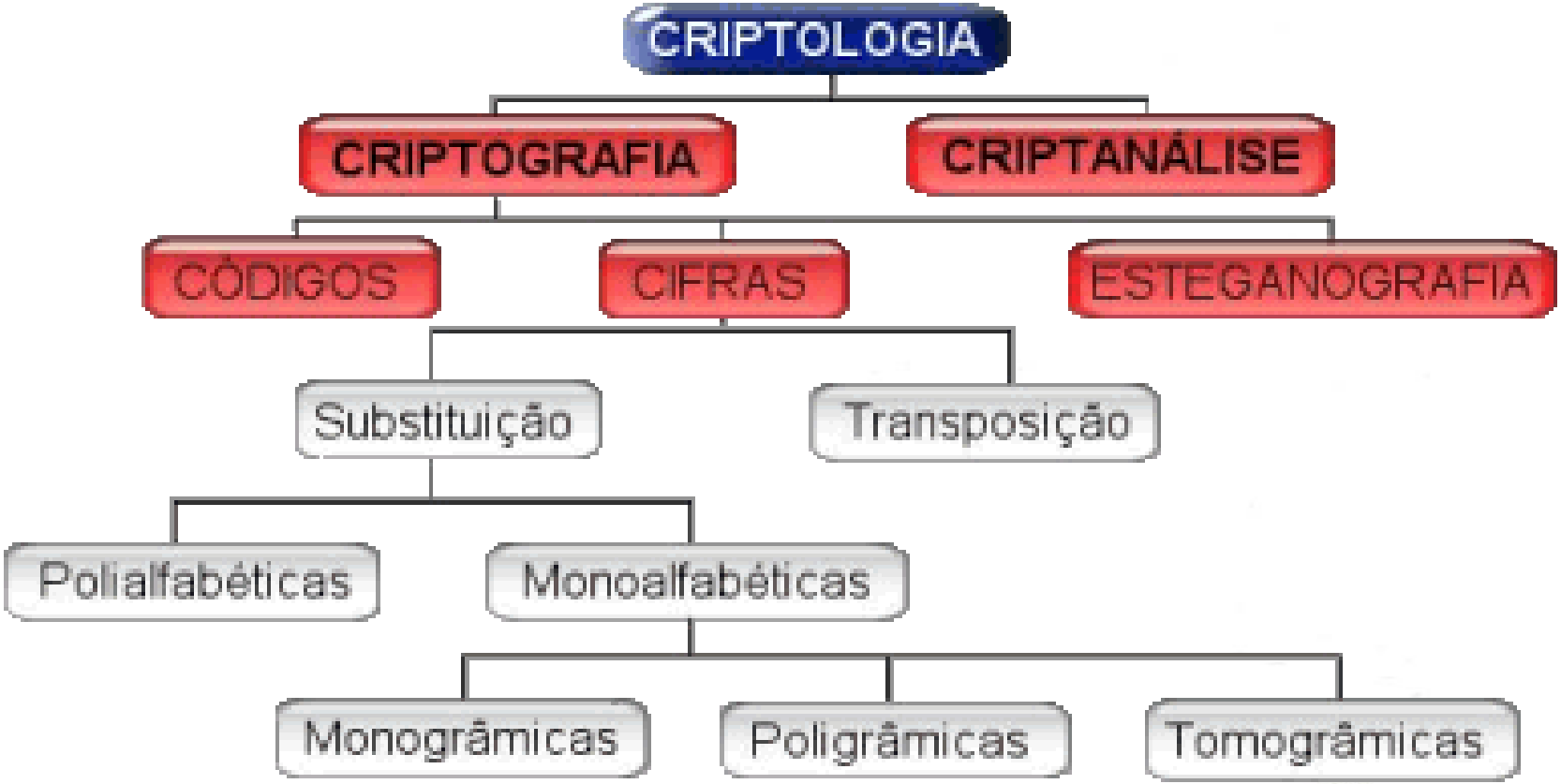
SIMÉTRICA	ASSIMÉTRICA
RÁPIDA	LENTA
GERÊNCIA E DISTRIBUIÇÃO DE CHAVES COMPLEXA	GERÊNCIA E DISTRIBUIÇÃO SIMPLES
NÃO OFERECE ASSINATURA DIGITAL SEGURA	OFERECE ASSINATURA DIGITAL SEGURA

QUESTÃO SOBRE CRIPTOGRAFIA: A RESPOSTA SEMPRE SERÁ UMA DAS CHAVES DO RECEPTOR

CRIPTOGRAFAR CHAVE PÚBLICA DO RECEPTOR
DECRIPTOGRAFAR CHAVE PRIVADA DO RECEPTOR

QUESTÃO SOBRE ASSINATURA DIGITAL: A RESPOSTA SEMPRE SERÁ UMA DAS CHAVES DO EMISSOR

CHAVE PRIVADA DO EMISSOR PARA ASSINAR
CHAVE PÚBLICA DO EMISSOR PARA VALIDAR


CRIPTOLOGIA
CRIPTOGRAFIA
CRIPTANÁLISE
CÓDIGOS
CIFRAS
ESTEGANOGRAFIA
Substituição
Transposição
Polialfabéticas
Monoalfabéticas
Monogrâmicas
Poligrâmicas
Tomogrâmicas

Questão 01

A Disponibilidade do sistema, a Integridade dos dados e a Confidencialidade dos dados são objetivos de segurança dos sistemas, respectivamente, sujeitos às ameaças de

(A) Adulteração dos dados, Recusa de serviço e Exposição aos dados.

(B) Recusa de serviço, Exposição aos dados e Adulteração dos dados.

(C) Exposição aos dados, Recusa de serviço e Adulteração dos dados.

(D) Recusa de serviço, Adulteração dos dados e Exposição aos dados.

(E) Exposição aos dados, Adulteração dos dados e Recusa de serviço.

Questão 02

Analise as seguintes afirmações relativas ao esquema de codificação criptográfica ou criptosistema:

I. Se em um criptosistema a chave de codificação criptográfica "e" é sempre igual à chave de decodificação criptográfica, então o criptosistema é chamado simétrico.

II. Se uma pessoa A deseja receber mensagens criptografadas utilizando um criptosistema assimétrico, ela publica uma chave de codificação criptográfica "e" e mantém secreta a correspondente chave "d" de decodificação criptográfica. Outras pessoas podem usar "e" para cifrar mensagens e enviá-las para a pessoa A.

III. Nos criptosistemas assimétricos, as chaves "d" e "e" são distintas e qualquer mensagem cifrada com a chave "e" pode ser decifrada utilizando- se tanto a chave "d" como a chave "e", da mesma forma que qualquer mensagem cifrada com a chave "d" pode ser decifrada utilizando-se tanto a chave "e" como a chave "d".

IV. Os criptosistemas simétricos também são chamados de criptosistemas de chave pública.

A QUANTIDADE DE ITENS CORRETOS É:

a) 1 b) 2 c) 3 d) 4 e) nenhum

Questão 03

As características da assinatura digital na criptografia de chave pública são:

a) **Integridade, privacidade, não repúdio e autenticidade.**

b) **Integridade, não repúdio e autenticidade.**

c) **Integridade, privacidade e autenticidade.**

d) **Integridade, privacidade, não repúdio, disponibilidade e autenticidade.**

e) **Integridade, confidencialidade, não repúdio e autenticidade.**

04 -Analise as seguintes afirmações relacionadas à segurança em redes de computadores:

I – A criptografia de chave pública baseia-se na utilização de uma mesma chave para codificar quanto para decodificar os dados.

II – No método de assinatura digital, a chave utilizada pelo signatário para assinar uma mensagem deve acompanhá-la obrigatoriamente para que o destinatário possa utilizá-la, em conjunto com sua chave pública, para verificar a validade da assinatura da referida mensagem.

III – No método de criptografia assimétrica, a chave utilizada para criptografar um texto é diferente da chave utilizada para decodificar o mesmo texto.

IV – No método de assinatura digital, o procedimento de verificação envolve a utilização de um método e uma chave pública para determinar se a assinatura foi produzida com a informação privada do signatário, isto é, com sua chave privada.

Assinale a quantidade de itens certos:

a) 1 **b) 2** **c) 3** **d) nenhum**

05 - Considerando uma comunicação segura entre os usuários A e B, garantir confidencialidade indica que

a) cada usuário deve confirmar a identidade da outra parte envolvida na comunicação.

b) apenas A e B podem modificar, intencionalmente ou não, o conteúdo da comunicação.

c) apenas A e B devem compreender o conteúdo da comunicação.

d) cada usuário deve provar que uma dada mensagem foi enviada pela outra parte envolvida na comunicação.

e) os recursos necessários à comunicação devem estar disponíveis e acessíveis aos usuários.

06 - Uma assinatura digital é um meio pelo qual

a) o gerador de uma mensagem, de um arquivo ou de outras informações codificadas digitalmente vincula sua identidade às informações.

b) os servidores de e-mail substituem uma mensagem pelo equivalente codificado.

c) os servidores de páginas da Web identificam o endereço IP do site de destino.

d) os servidores de páginas da Web identificam o endereço IP do site de origem.

e) os *Firewalls* utilizam para garantir o repúdio da informação.

07 - Em assinaturas digitais, utilizando o sistema de chave pública, a chave criptográfica usada para a verificação da autenticidade de um dado emissor por um receptor é a chave

a) privada do emissor.

b) pública do emissor.

c) pública do receptor.

d) privada do receptor.

e) simétrica compartilhada entre emissor e receptor.

08 - Analise as seguintes afirmações relacionadas à segurança na Internet:

I. Um *WORM* é um sistema de segurança que tem como principal objetivo bloquear todo o tráfego, que utilize o protocolo http, aos servidores WWW de uma corporação.

II. Configurando um *firewall*, instalado entre uma rede interna e a Internet, para bloquear todo o tráfego para os protocolos HTTP, SMTP, POP e POP3, os usuários da referida rede interna terão acesso à Internet, com um nível de segurança aceitável, a sites como os de bancos, servidores de e-mail e de entidades que utilizem sites seguros.

III. Uma *VPN* é formada pelo conjunto de tunelamento que permite a utilização de uma rede pública para o tráfego de informações e, com o auxílio da criptografia, permite um bom nível de segurança para as informações que trafegam por essa conexão.

IV. O *firewall* é um programa que tem como objetivo proteger uma rede contra acessos e tráfego indesejado, proteger serviços e bloquear a passagem de conexões indesejáveis, como por exemplo, aquelas vindas da Internet com o objetivo de acessar dados corporativos ou seus dados pessoais.

Assinale a quantidade de itens certos:

a) 1 b) 2 c) 3 d) nenhum

09 - Analise as seguintes afirmações relacionadas à Segurança da Informação:

I. Um *Firewall* de estado controla o tráfego para evitar pacotes ilegítimos, guardando o estado de todas as últimas transações efetuadas.

II. Um *Spyware* é um programa que recolhe informações sobre o usuário e sobre seus costumes na Internet e transmite estas informações a uma entidade externa na Internet sem o conhecimento ou consentimento do usuário. Diferem dos cavalos de Tróia por não terem como objetivo que o sistema do usuário seja dominado ou manipulado.

III. Nos sistemas de Segurança da Informação existem alguns métodos que verificam se uma mensagem em trânsito foi alterada. Este procedimento visa garantir o não-repúdio.

IV. O foco principal dos sistemas de Segurança da Informação para a Internet são os desastres, como incêndio ou falhas elétricas e os erros dos usuários.

Assinale a quantidade de itens certos:

a) 1 b) 2 c) 3 d) nenhum