Criptografia Básica

Gustavo Pinto Vilar

ITnerante

Gustavo Vilar

- Mini – CV
  - PPF / DPF – Papiloscopista Policial Federal
  - Pós-Graduado em Docência do Ensino Superior – UFRJ
  - Graduado em Ciência da Computação e Processamento de Dados – ASPER/PB
  - Aprovações: PRF 2002, PF 2004, MPU 2010, ABIN 2010

ITnerante

Gustavo Vilar

- Contatos:
  - gustavopintovilar@gmail.com
  - p3r1t0f3d3r4l@yahoo.com.br

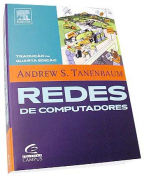
ITnerante

Escopo

- Abordar os assuntos mais recorrentes e com fortes tendências para concursos atuais
- Familiarizar o concursando com os tipos de questões mais freqüentes.
- Abordar as metodologias de resolução de questões das principais bancas

ITnerante

Bibliografia



cespeUnB

Fundação Carlos Chagas

FUNDAÇÃO CESGRANRIO

ITnerante

Criptografia Básica – Carga Horária

- 12 vídeo aulas (04h06m19s / 00h20m32s)
  - Criptografia
    - Princípios Criptográficos
    - Cifras
    - Questões
  - Criptografia Simétrica
    - Conceitos
    - Criptografia em bloco: DES, AES
      - DES– Meet in the Middle
    - Criptografia em fluxo: RC4, OTP
  - Criptografia Assimétrica
    - RSA, DH, El Gamal, ECC
  - Controle de integridade
    - Conceitos
    - MD, SHA
  - Bateria de Questões 01
  - Bateria de Questões 02

ITnerante

Criptografia

Princípios Criptográficos

ITnerante

Conceitos Iniciais

- S.O. oferecem um sistema de permissões (logon)
- Algoritmo criptográfico pode ser executado por computador genérico, hardware dedicado ou por um ser humano
- Toda criptografia pode ser quebrada

ITnerante

Esquemas de Criptografia

Computacionalmente seguro

- **Custo** para quebrar a cifra é superior ao valor da informação codificada

- **Tempo** exigido para quebrar a cifra superior ao tempo de vida útil da informação

Incondicionalmente seguro

- One-Time Pad
- Não existe no texto cifrado informações suficientes para determinar exclusivamente o texto claro correspondente

ITnerante

Princípio de A. KERCKHOFFS

- Os algoritmos devem ser de conhecimento público, as chaves devem ser secretas

ITnerante

Claude Shannon

- Difusão
  - Dissipar a estrutura estatística do bloco original por todos os bits do bloco cifrado
  - Transposição ou permutação
- Confusão
  - Complexidade no relacionamento entre o texto cifrado e texto claro
  - Substituição complexa

Claude Shannon
(1916-2001)

ITnerante

Princípios Fundamentais

Redundância

- Informações desnecessárias para compreensão da mensagem, porém necessárias para conferência de integridade

Atualidade

- Assegura que cada mensagem recebida possa ser confirmada como atual

ITnerante

Criptografia

Princípios Criptográficos

ITnerante

Propriedades obtidas com a criptografia

- Confidencialidade
- Integridade
- Autenticidade
- Irretratabilidade ou não repúdio
- ~~Disponibilidade~~

ITnerante

Classificação dos algoritmos

- Número de chaves
  - Simétricos, Assimétricos
- Métodos de operação
  - Substituição e Transposição
- Modo de processamento
  - Cifradores de Bloco, Cifradores de Fluxo

ITnerante

Ciências "do Sigilo"

- Criptologia
  - Criptografia
    - Legível → Ilegível
  - Criptoanálise
    - Arte ou ciência de quebrar textos cifrados
- Estagonologia
  - Esteganografia
    - Ocultação da informação
  - Esteganoanálise
    - Arte ou ciência de revelar informações ocultas

ITnerante

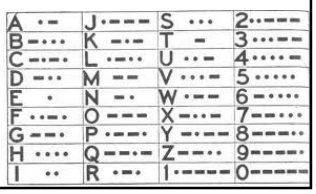
Criptografia

- Arte ou ciência de escrever em códigos ou em cifras
- Formas de criptografar
  - Códigos
  - Cifras (substituição e transposição)

ITnerante

Criptografia através de códigos

- Uso de códigos pré-definidos
- Freqüência do uso denuncia seu significado



Criptografia através de cifras

- Mensagem original é cifrada através de operações de transposição e substituição de seus caracteres, resultando numa mensagem cifrada
- Para decifração, basta aplicar o processo inverso

ITnerante

Cifras mono alfabéticas

- Cifra de César
  - Cada letra do alfabeto é deslocada da sua posição um número fixo de lugares k, tal que 1 <= k <= 25

K (3)
Concurso = Frqfwvr

ITnerante

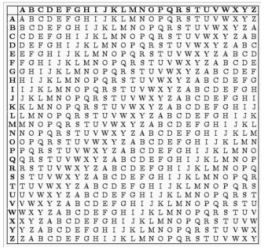
Cifras Polialfabéticas

- Cifra de Vigenère - consiste no uso de várias cifras de César em seqüência, com diferentes valores de deslocamento ditados por uma "palavra-chave"

Claro: Aprovacaoemconcurso

Chave:Itneranteitnerantei

Cifrado: IIES.....



ITnerante

Cifras Polialfabéticas

- Cifra Playfair
  - Trata digramas como unidades isoladas
  - Oculta completamente as freqüências de única letra
  - Baseado no uso de uma matriz (5x5) + palavra chave

I	T	N	E	R
A	B	C	D	F
G	H	J	K	L
M	O	P	Q	S
U	V	X	Y	Z

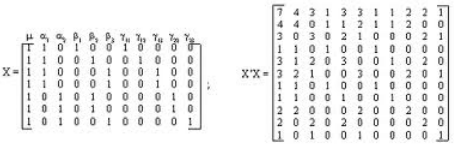
Regras:
Na mesma linha
Na mesma coluna
Em linhas e colunas diferentes

APROVACAO = CMTSUBDBMT

ITnerante

Cifras Polialfabéticas

- **Cifra De Hill**
  - Primeiro converte-se as letras em números, depois agrupa-se os números n a n e multiplica-se cada grupo por uma matriz quadrada de ordem n invertível, ou seja determinante diferente de 0
  - Os números resultantes são novamente passados para letras, e assim tem-se a mensagem codificada
  - Para decodificar a mensagem basta aplicar o mesmo processo, porém utilizando a matriz inversa.



ITnerante

Bateria de questões de aprendizagem

Fundamentos Criptográficos

ITnerante

Nossa Caixa– FCC 2011 – Analista de Sistemas I

1. Normalmente os métodos de criptografia são divididos em:

A. chave simétrica e chave assimétrica.
B. chave única e chave múltipla.
C. chave pública e chave privada.
D. cifras de substituição e cifras de transposição.
E. DES (Data Encryption Standard) e AES (Advanced Encryption Standard).

INFRAERO – FCC 2011 – Analista Superior III – Administrador de Banco de Dados

2. No contexto da criptografia, preserva todos os caracteres de uma mensagem, apenas mudando-os de lugar. É baseada no princípio matemático da permutação. Entre os diversos tipos dela está a geométrica. Trata-se de uma cifra de

A. esteganografia.
B. substituição.
C. transposição.
D. Bacon.
E. Bazeries.

TRT 19 – FCC 2011 – Analista Judiciário – Tecnologia da informação

3. Uma regra fundamental da criptografia é:

A. A chave criptográfica deve ser modificada a cada período de alguns anos.
B. Deve-se presumir que o criptoanalista conhece os métodos genéricos de criptografia e descriptografia que são utilizados.
C. Tanto os algoritmos quanto as chaves devem ser secretos, segundo o princípio de Kerckhoff.
D. O sigilo deve decorrer da presença de um algoritmo forte e secreto, independentemente do tamanho da chave.
E. Deve-se supor que, se uma cifra puder resistir a uma estratégia de texto cifrado, ela é segura.

TJ-SE– FCC 2009 – Analista Judiciário – Analise de sistemas

4. No contexto da criptografia, a difusão

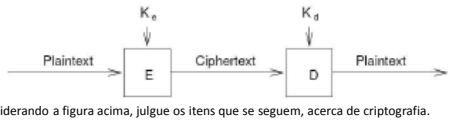
a. altera o menor número possível de bits da cifra para cada mudança de bit no texto.
b. objetiva tornar complexa a relação entre a chave e a cifra.
c. dificulta deduzir qualquer propriedade da chave a partir da cifra.
d. procura enviar numa comunicação o maior número possível de chaves.
e. procura eliminar todas as redundâncias na cifra.

MPE - PE – FCC 2006 – Técnico Ministerial - Área Administrativa

5. As cifras que reordenam as letras de um texto mas não os disfarçam são denominadas

a. monoalfabética.
b. polialfabéticas.
c. de uso único.
d. de substituição.
e. de transposição.

CTI – CESPE – Téc Pl – Seg de Sistemas de Informação



6. Considerando a figura acima, julgue os itens que se seguem, acerca de criptografia.

[108] O módulo E na figura corresponde a um algoritmo de encriptação ou codificação e o elemento Ke corresponde à chave de encriptação ou codificação.

[109] Se a decodificação do Ciphertext corresponde a Plaintext = D(K d, Ciphertext) e o módulo E corresponde a um algoritmo de encriptação, então a decodificação do Ciphertext com a chave Kd deve depender do secretismo de E ou D.

[110] Shannon identificou duas propriedades essenciais em um algoritmo criptográfico: a confusão, em que a relação entre o Plaintext e o Ciphertext se torna o mais complexa possível; e a difusão, em que se removem do Ciphertext as propriedades estatísticas do Plaintext.

TRE-RN – FCC 2006 – Analista Judiciário – Analista de sistemas

7. Um texto cifrado pelo Código de César é um exemplo de criptografia do tipo

a. Substituição mono alfabética.
b. Substituição polialfabéticas.
c. Assimétrica.
d. Transposição.
e. Quântica.

BACEN – FCC 2006 – Analista – Área 1

8. NÃO é uma cifra de César resultante da criptografia sobre uma mesma mensagem:

a. F H Q W U D O.
b. K M V C W J Q.
c. E G P V T C N.
d. I K T Z X G R.
e. G I R X V E P.

TRE-SC – FCC 2005 – Analista Judiciário – Analista de sistemas

9. Sistemas criptográficos introduziram uma nova dimensão à segurança da informação. Em relação aos sistemas criptográficos, é CORRETO afirmar que:

a. a criptografia introduziu benefícios fundamentais, como sigilo e integridade.
b. cifradores são baseados tanto no segredo da chave quanto no segredo do algoritmo.
c. cifradores são baseados em um único segredo: o segredo da chave.
d. é indiferente usar criptografia Simétrica ou Assimétrica, pois ambas oferecem os mesmos benefícios.

TRT-AL – FCC 2011 – Analista Judiciário – Analista de sistemas

10. A Cifra de César (ou código de César) é uma das mais simples e conhecidas técnicas de criptografia, o que lhe confere papel coadjuvante e freqüentemente incorporado como parte de esquemas mais complexos. Sendo um tipo de cifra de substituição mono alfabética, onde cada letra ou grupo de letras é substituído por outra letra ou grupo de letras, sua aplicação à palavra TRIBUNAL trará como resultado:

a. WULEXQDO.
b. USJCVOBM.
c. QWERTPOI.
d. ZAQXSWCD.
e. SQHATMZK.

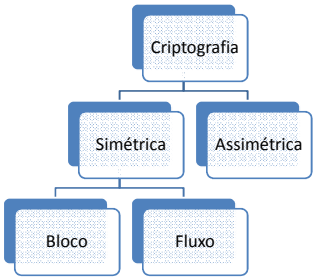
Gabarito

1. D	6. C, E, C
2. C	7. A
3. B	8. B
4. E	9. C
5. E	10. A

Criptografia

Sistemas Criptográficos

Ramificações Criptográficas



ITnerante

Sistemas de chave simétrica

- Sinônimos: Criptografia SIMÉTRICA, de chave única, chave privada, chave compartilhada, de chave secreta ou convencional
- Normalmente a chave de cifragem é igual a de decifragem.
- Transformação de caractere por caractere ou bit a bit
- Rápida execução se comparada à criptografia de chave assimétrica
- Garante
  - Confidencialidade
  - Integridade
- NÃO garante
  - Irretratabilidade
  - Autenticidade
- Principais problemas
  - Manter o sigilo da chave
  - Dificuldade no compartilhamento da chave

ITnerante

A chave

- Geralmente é um número "pequeno"
- Uso de RNG ou PRNG para sua geração
- Processo de gerenciamento de chaves complexo
- Tamanho da chave x esforço para quebra
  - 40 bits x 100 mil US$ = 2 segundos
  - 128 bits x 10 trilhões US$ = 10^11 anos

ITnerante

Alguns sistemas criptográficos simétricos

- De bloco
  - IDEA
  - TwoFish
  - Blowfish
  - Serpent
  - **DES**
  - **AES**
  - RC5
  - RC6

ITnerante

Alguns sistemas criptográficos simétricos

- De Fluxo
  - **RC4**
  - **OTP**

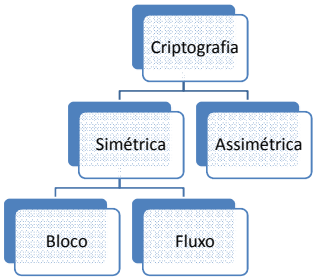
ITnerante

Criptografia

Cifragem Simétrica em Bloco

ITnerante

Ramificações Criptográficas



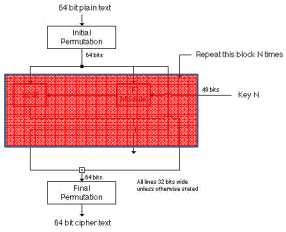
ITnerante

Fundamentos da cifragem em bloco

- Texto é dividido em blocos ANTES da cifragem
- Operação em cada bloco de forma independente
- Problema na distribuição da chave
- Permite reutilização das chaves
- Whitening
- Aspectos do tamanho do bloco

ITnerante

DES – Data Encryption Standard



- Características
  - Chave 64 bits (no disco)
  - Chave 56 bits (execução)
  - Subchaves 48 bits

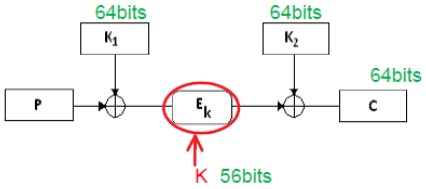
ITnerante

Problemas com o DES

- Chave relativamente pequena (56 bits)
  - Sobrevida possível através de
    - Chaves independentes
    - S-Boxes novas
    - Whitening - Viável
    - Multiplicidade - Viável

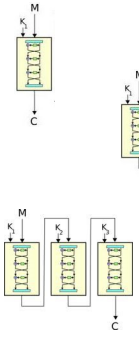
ITnerante

Whitening



ITnerante

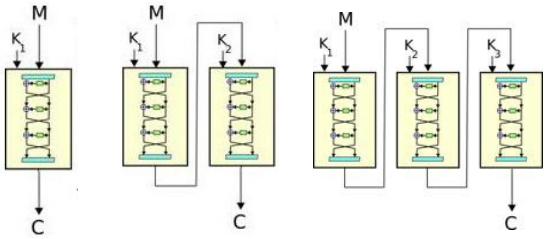
Multiplicidade



- DES
- 2DES com 2 chaves
- 3DES com 1, 2 ou 3 chaves
- Modo E-D-E
  - Força efetiva da chave reduzida pelo ataque Meet-In-The-Middle

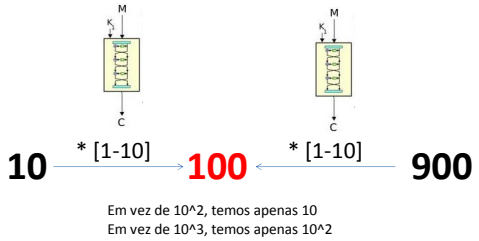
ITnerante

Meet in the Middle



ITnerante

Meet in the Middle - Simplificação



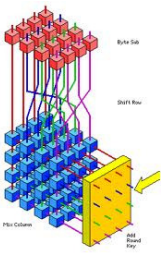
Em vez de 10^2, temos apenas 10
Em vez de 10^3, temos apenas 10^2

ITnerante

Meet in the Middle – Implicações

- **Chave Efetiva** – É o tamanho propriamente dito
- **Força Efetiva** - É a força da chave depois do Meet In The Middle
- "**Força efetiva**" - tratada como sinônimo de "chave equivalente"

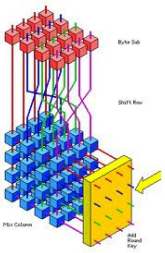
AES - Advanced Encryption Standard



- Utiliza uma rede SP
- Passos 10, 12 ou 14 para chaves de 128, 192 ou 256 bits, respectivamente.
- Cada bloco é tratado como uma matriz 4x4 de bytes

ITnerante

AES - Advanced Encryption Standard



- Padrão de criptografia pelo governo dos Estados Unidos (2002)
- substituir o DES
- Vencedor do concurso Rijndael
- Rijndael - Chave e bloco: 128,192 e 256 bits
- AES – Bloco de 128 bits, manteve as chaves em 128, 192 e 256 bits

ITnerante

Criptografia

Cifragem Simétrica em Fluxo

ITnerante

RC4

- Chave de 0 a 256 bytes
- Usado nos padrões SSL/TLS, WEP, WPA
- Primeiro algoritmo disponível nas redes sem fio
- Velocidade é importante
- É a cifragem simétrica mais usada
- Possui como princípio de funcionamento o segredo criptográfico perfeito: chave do tamanho da mensagem
- Considerado seguro num contexto prático

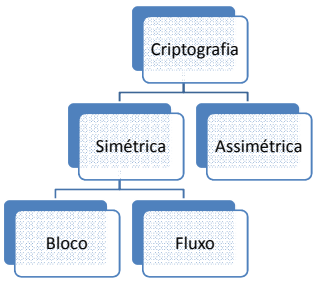
ITnerante

OTP

- Chave aleatória de mesmo tamanho da mensagem
- Se a chave for verdadeiramente aleatória, nunca reutilizada, e mantida em segredo, a one-time pad pode ser inquebrável

ITnerante

Ramificações Criptográficas



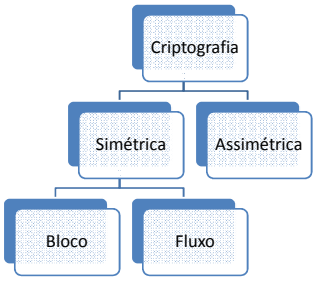
ITnerante

Criptografia

Cifragem Assimétrica

ITnerante

Ramificações Criptográficas



ITnerante

Sistemas de chave pública

- Chave de cifração diferente da de decifração e uma não pode ser facilmente gerada a partir da outra
- Relação matemática entre as chaves
  - Ek1(M)=C, Dk2(C)=M e Dk2(Ek1(M))=M
  - Ek2(M)=C, Dk1(C)=M e Dk1(Ek2(M))=M
- Alto custo computacional (comparado com a criptografia simétrica)
- Tamanho da chave grande (ou não)

ITnerante

RSA

- Uso de duas chaves: Uma para encriptação e outra para decriptação (módulo e expoente obtidos de números primos)
- Resolve o problema de distribuição de chaves da criptografia simétrica (Envelopamento Digital)
- Segurança baseada na fatoração de números EXTENSOS
- Quanto maior a chave = maior a segurança = menor velocidade de execução

ITnerante

Aplicações recorrentes do RSA

- Criptografar com a chave pública do destinatário
- Somente o destinatário pode decriptografar com a chave privada relacionada
- Garantia de confidencialidade / privacidade / sigilo

- Criptografar com a chave privada do emissor
- Qualquer um poderá decriptografar com a chave pública do emissor
- Garantia de autenticidade e integridade

ITnerante

Diffie Hellman

- Possibilita acordo de chaves sem o envio da mesma
- Uso da tecnologia de chave pública para gerar a chave de sessão simétrica em vez de envelopá-la
- Não é usado para criptografia
- Não é considerado um Criptossistema

ITnerante

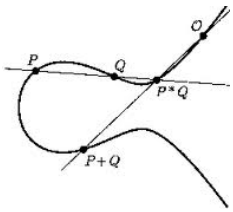
El Gamal

- Faz o mesmo que RSA, mas se baseia no problema do logaritmo discreto

ITnerante

Curvas Elípticas

- Variante da criptografia assimétrica ou de chave pública, baseada na matemática das curvas elípticas
- Provê a maioria das funcionalidades do RSA, só que utilizando menos recursos
- Chaves de 1024 RSA ou DH é equivalente a 160 bits de ECC
- concebido para ser utilizado em dispositivos wireless e telefones celulares



ITnerante

Criptografia

Controle de Integridade

ITnerante

Controle de integridade - Hash

- Unidirecionalidade
- Condensação
- Não há necessidade de chave
- Consistência, randomicidade e unicidade
- Mais próximos da criptografia simétrica do que da assimétrica

ITnerante

Controle de integridade - Hash

- Senhas criptografadas com Hash e armazenadas são vulneráveis a ataques de dicionário. Solução: SALT
- Saída é independente do tamanho de entrada
- Colisão: Duas mensagens que produzem o mesmo resumo

ITnerante

Família MD

- MD2, MD3, MD4, MD5
- Saídas de 128 bits
- Já não é mais recomendável. "Certificado com colisão" foi gerado em 2008

ITnerante

Família SHA

Algoritmo	Tamanho da mensagem (bits)	Tamanho do bloco (bits)	Tamanho da palavra (bits)	Tamanho do message digest (bits)	Segurança (bits)
SHA-1	$< 2^{64}$	512	32	160	80
SHA-224	$< 2^{64}$	512	32	224	112
SHA-256	$< 2^{64}$	512	32	256	128
SHA-384	$< 2^{128}$	1024	64	384	192
SHA-512	$< 2^{128}$	1024	64	512	256

ITnerante

Bateria de questões de aprendizagem

Criptografia simétrica, assimétrica, hash

ITnerante

MP PE – FCC 2012 – Analista Ministerial – Informática

1. Um sistema criptográfico de chaves públicas, como o RSA, permite que um usuário autentique uma mensagem com uma assinatura digital cifrando esta mensagem

A. com a sua chave privada.
B. com a sua chave pública.
C. com a chave privada do destinatário da mensagem.
D. com a chave pública do destinatário da mensagem.
E. duas vezes, uma com a chave pública e outra com a chave privada do destinatário da mensagem.

ITnerante

MP PE – FCC 2012 – Técnico Ministerial – Apoio Especializado -Informática

2. O algoritmo de criptografia ___ utiliza um bloco de 64 bits e uma chave de 56 bits. Com um tamanho de chave de 56 bits, existem ___ chaves possíveis.

As lacunas I e II devem ser preenchidas correta e respectivamente por

A. AES e 56^2.
B. DES e 2^56
C. RSA e 2^56
D. Diffie-Hellman e 2^56
E. RADIX64 e 2^128

ITnerante

MP PE – FCC 2012 – Técnico Ministerial – Apoio Especializado -Informática

3. Sobre assinaturas digitais, considere:

I. Consiste na criação de um código, de modo que a pessoa ou entidade que receber uma mensagem contendo este código possa verificar se o remetente é mesmo quem diz ser e identificar qualquer mensagem que possa ter sido modificada.

II. Se José quiser enviar uma mensagem assinada para Maria, ele codificará a mensagem com sua chave pública. Neste processo será gerada uma assinatura digital, que será adicionada à mensagem enviada para Maria. Ao receber a mensagem, Maria utilizará a chave privada de José para decodificar a mensagem.

III. É importante ressaltar que a segurança do método de assinatura digital baseia-se no fato de que a chave pública é conhecida apenas pelo seu dono. Também é importante ressaltar que o fato de assinar uma mensagem não significa gerar uma mensagem sigilosa.

Está correto o que consta em

A. I e III, apenas.
B. I, II e III.
C. II e III, apenas.
D. I, apenas.
E. I e II, apenas.

ITnerante

PETROBRÁS – CESGRANRIO 2012 – Analista de Sistemas Júnior - Infraestrutura

4. Para garantir o sigilo em uma comunicação, um emissor pode enviar uma mensagem criptografada com um algoritmo de criptografia simétrica.

Para que o receptor possa decifrar essa mensagem, é necessário obter a chave

A. privada do emissor que foi utilizada pelo algoritmo para cifrar a mensagem.
B. privada e a chave secreta do emissor que foram utilizadas pelo algoritmo para cifrar a mensagem.
C. secreta do emissor que foi utilizada pelo algoritmo para cifrar a mensagem.
D. pública do emissor que foi utilizada pelo algoritmo para cifrar a mensagem.
E. pública e a chave secreta do emissor que foram utilizadas pelo algoritmo para cifrar a mensagem.

ITnerante

TRT-23– FCC 2011 – Técnico Judiciário – Tecnologia da Informação

5. Em relação à criptografia, considere:

I. O emissor e receptor utilizam a mesma chave tanto para a cifragem como para a decifragem, portanto devem conhecer antecipadamente a chave.

II. O emissor e receptor utilizam chaves diferentes para cifrar e decifrar os dados.

III. Mensagens cifradas com a chave pública só podem ser decifradas com a chave secreta e vice versa.

IV. O DES é um algoritmo de criptografia que realiza somente duas operações sobre sua entrada: deslocamento de bits e substituição de bits.

Os itens I, II, III e IV, associam-se, respectivamente, às criptografias

A. simétrica, assimétrica, simétrica e simétrica.
B. assimétrica, simétrica, simétrica e assimétrica.
C. simétrica, assimétrica, assimétrica e simétrica.
D. simétrica, simétrica, assimétrica e assimétrica.
E. assimétrica, assimétrica, simétrica, simétrica.

ITnerante

TJ-ES – CESPE 2011 – Analista Judiciário – Análise de Banco de Dados

6. Acerca de segurança da informação e criptografia, julgue os itens seguintes

[96] A técnica de segurança de informação denominada assinatura digital permite ao receptor verificar a integridade da mensagem e a identidade do transmissor.

[97] A adição de uma assinatura digital a uma mensagem pode ser efetuada pelo seu transmissor, por meio da adição, à mensagem cifrada, de um hash (da mensagem original em claro) cifrado com sua chave privada.

[98] A distribuição de chaves é mais simples e segura na utilização de um sistema criptográfico simétrico ou de chave secreta que na utilização de um sistema criptográfico assimétrico ou de chave pública.

[99] Sistemas criptográficos assimétricos ou de chave pública oferecem melhor desempenho na cifração e decifração de mensagens que sistemas criptográficos simétricos.

[100] Considerando-se que, em um sistema de criptografia assimétrico - ou de chave pública - um usuário A deseje enviar, de forma segura, uma mensagem a um usuário B, é correto afirmar que o usuário A deverá cifrar a mensagem com sua chave privada e o usuário B, ao receber a mensagem, deverá decifrá-la com a chave pública de A.

ITnerante

INMETRO – CESPE 2010 – Pesquisador – Desenvolvimento de Sistemas

7. A assinatura digital consiste na cifração

a. do resumo criptográfico da mensagem (hash) com a chave pública do autor.
b. da mensagem com a chave privada do autor.
c. do resumo criptográfico da mensagem (hash) com a chave privada do autor.
d. da mensagem com a chave pública do autor.
e. da mensagem e do seu resumo criptográfico (hash) com a chave pública do autor.

ITnerante

INMETRO – CESPE 2010 – Pesquisador – Gestão da Informação

8. Com relação aos sistemas de criptografia, assinale a opção correta.

a. MD5 é um algoritmo de criptografia utilizado para a verificação de integridade de arquivos que são obtidos na Internet por meio de download.

b. DES é embasado no tempo necessário para que uma chave secreta seja descoberta, em função do comprimento da chave, por isso, além de ser inviolável, é um dos algoritmos de criptografia mais confiáveis.

c. SHA é um algoritmo que gera um resumo de mensagem que varia de tamanho em função do tamanho da própria mensagem.

d. O algoritmo AES, uma variação do DES, utiliza o conceito de chaves simétricas.

e. As aplicações de chave pública não permitem autenticação de usuários, pois são destinadas para uso apenas de órgãos do governo.

INMETRO – CESPE 2010 – Pesquisador – Infraestrutura e Redes de TI

9. A respeito de criptografia simétrica e assimétrica, assinale a opção correta.

a. Simetria de chaves significa que as partes têm a mesma chave para cifrar e decifrar uma mensagem.

b. A ciência da criptografia se divide em duas grandes vertentes: a criptografia de chave privada ou assimétrica e a criptografia de chave pública ou simétrica.

c. O sistema criptográfico DES opera com um bloco de 64 bits, em que, a cada 8 bits, se agrega um bit de paridade, razão por que, na prática, a chave tem somente 56 bits.

d. Privacidade e integridade são as únicas questões de segurança que requerem o uso de criptografia.

e. Classifica-se a criptografia de chave simétrica em duas famílias: criptografia simétrica de blocos (block cipher) e criptografia simétrica de via (stream cipher).

INMETRO – CESPE 2010 – Pesquisador – Ciência da Computação

10. Com relação aos sistemas criptográficos, assinale a opção correta.

a. Com os sistemas simétricos, consegue-se obter confidencialidade, integridade e disponibilidade.
b. Com os sistemas assimétricos, consegue-se obter confidencialidade, integridade, autenticidade e não repúdio.
c. O sistema RSA, com ou sem curvas elípticas, tem por base o problema do logaritmo discreto.
d. AES e 3DES são cifras simétricas que têm por base a malha de Feistel.
e. O 3DES consiste de três rodadas consecutivas do DES em que a mesma chave de 64 bits é usada.

ABIN – CESPE 2010 – Agente Técnico de Inteligência – Tecnologia da Informação

11. Julgue os itens que se seguem, relativos a sistemas de criptografia e suas aplicações.

[105] A chave assimétrica é composta por duas chaves criptográficas: uma privada e outra pública.

[106] O algoritmo de criptografia RSA (Rivest, Shamir e Adleman) é embasado no conceito de chave simétrica.

[107] Um algoritmo de criptografia eficiente impede que uma mensagem que trafega em uma rede de comunicação seja decodificada ou apagada por intrusos.

BNDES – CESGRANRIO 2010 – Profissional Básico – Análise de Sistemas e Suporte

12. O algoritmo de hash SHA-256 aplicado à frase "Para que o mal triunfe, basta que os bons não façam nada." produz como resultado

a. strings diferentes de tamanho variável conforme a semente aleatória utilizada.

b. uma string que permite a recuperação do texto original.

c. sempre a mesma string de tamanho fixo.

d. diferentes strings de 256 KB conforme a semente aleatória utilizada.

e. 2dd30740a31cd09b6e4a8ec08bc4b6d540084a2e.

MPU– CESPE 2010 – Analista de Informática – Suporte Técnico

13. Julgue os próximos itens, relativos à segurança da informação.

[140] Em processos de autenticação de mensagens, um digest MDC (modification detection code) utiliza uma função hash sem chaves. Se for assinado, o digest permite verificar a integridade de mensagem, além de sua autenticação e não-repúdio.

[141] Em sistemas criptográficos de chave pública, curva elíptica consiste na implementação de algoritmos de chave pública já existentes que provêem sistemas criptográficos com chaves de maior tamanho que os algoritmos de chaves simétricas.

[142] Para que o conteúdo de uma mensagem criptografada seja decifrado apenas pelo seu verdadeiro destinatário, é necessário que ela seja assinada digitalmente.

TRT-9– FCC 2010 – Analista Judiciário – Tecnologia da Informação

14. O primeiro protocolo de criptografia disponível para redes Wi-Fi é baseado em um algoritmo chamado

a. RC4, que é um codificador de fluxo.

b. RSA, que é um decodificador de chave pública.

c. WAP, que é um protetor de arquivos transmitidos.

d. NAT, que é um decodificador de fluxos.

e. WPA, que é um protetor de arquivos transmitidos.

BASA – CESPE 2010 – TI – Segurança da informação

15. Acerca dos sistemas criptográficos, julgue os itens.

[106] Enquanto uma cifra de bloco atua em um bit ou byte do fluxo de dados por vez, uma cifra de fluxo atua sobre um conjunto de caracteres de texto em claro, que são tratados como um todo e usados para produzir um criptograma de igual comprimento.

[107] Nos sistemas simétricos, os usuários usam a mesma chave para cifrar e decifrar mensagens, enquanto nos sistemas assimétricos mais de uma chave é usada.

[108] Em um sistema de chaves assimétricas, cada usuário tem um par de chaves, sendo que uma delas é mantida secreta e a outra é pública.

[109] Nos sistemas assimétricos, as chaves são escolhidas de forma que se uma mensagem é cifrada usando uma das chaves, o criptograma correspondente é decifrado utilizando a outra chave do par.

Gabarito

1. A
2. B
3. D
4. C
5. C
6. C, C, E, E, E
7. C
8. A
9. A
10. B
11. C, E, E
12. C
13. C, E, E
14. A
15. E, C,C,C