Criptografia Intermediária

Certificação Digital / Modos de Operação das Cifras

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

Gustavo Vilar

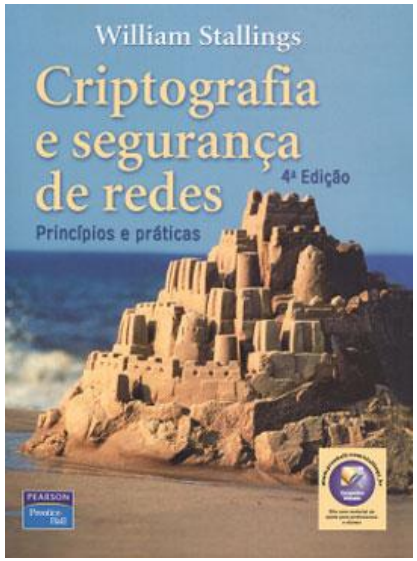
- Contatos:
  - gustavopintovilar@gmail.com
  - p3r1t0f3d3r4l@yahoo.com.br

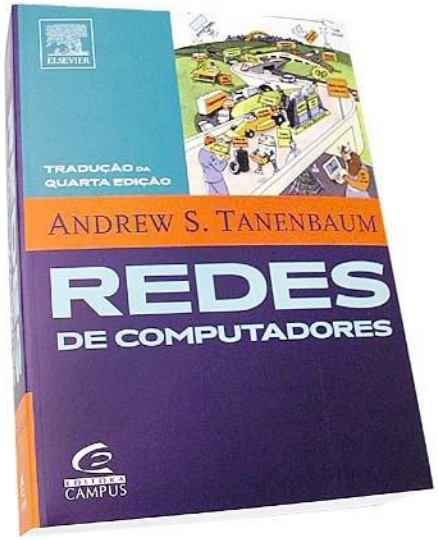
ITnerante

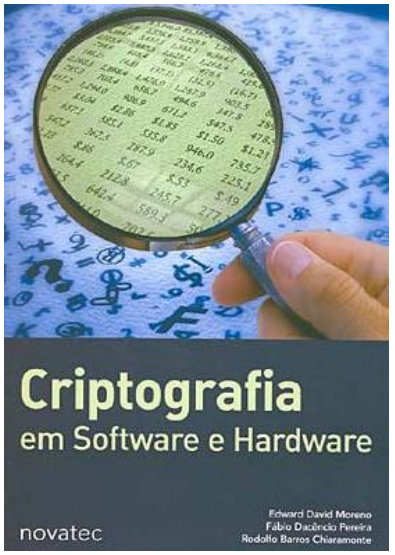
Escopo

- 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

Bibliografia







Criptografia II – Carga Horária

- **11 vídeo aulas (03h39m03s / 00h19m55s)**
  - Criptografia Simétrica
    - Modos de operação: ECB, CBC, CFB, OFB, CTR
    - Vetores de Inicialização
  - Primeira Bateria de Questões de Aprendizagem
  - Certificação Digital
    - Conceitos
    - Tipos de Certificado
    - CRLs
    - Protocolos envolvidos
    - Componentes da PKI
  - Segunda Bateria de Questões de Aprendizagem
  - Terceira Bateria de Questões de Aprendizagem

ITnerante

Criptografia Intermediária

Modos de Operação Dos Sistemas Criptográficos Simétricos

ITnerante

Modos de Operação
Considerações iniciais

- “Criptografar o mesmo texto simples sob a mesma chave sempre produz a mesma saída”
- Solução: Vetor de Inicialização e/ou encadeamento de criptografias

Modos de Operação
Considerações iniciais

Modos de Operação
ECB – Eletronic Code Book

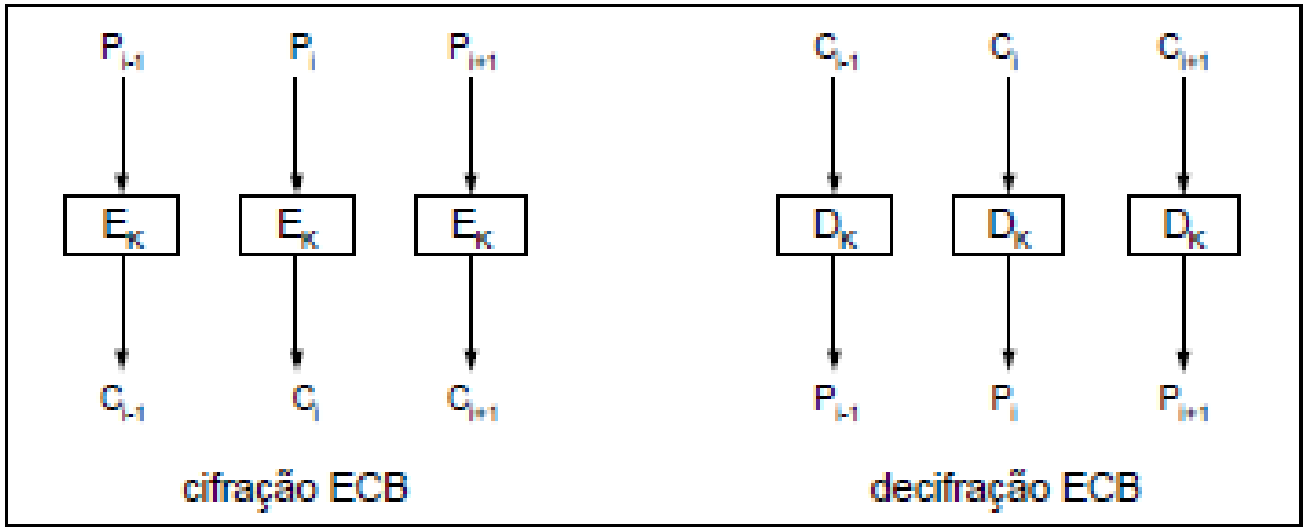
- Cada bloco é cifrado isoladamente
- ÚNICO MODO sem Vetor de Inicialização
- ÚNICO MODO Vulnerável ao ataque de Block replay
- Mensagem clara é fracionada em blocos de tamanho fixo
- Fornece paralelismo (velocidade) na cifragem e decifragem
- Mensagem cifrada é obtida pela concatenação dos blocos cifrados
- Ideal para cifrar arquivos aleatórios
- Ideal para pequenas quantidades de dados, como uma chave criptográfica
- Não acrescenta nada à confidencialidade proporcionada pela cifra
  - Não existe a figura do Vetor de inicialização
- Blocos em claro iguais geram blocos criptografados iguais

Modos de Operação
ECB – Eletronic Code Book

Figura em Claro

Figura Cifrada Utilizando ECB

Modos de Operação
ECB – Eletronic Code Book



Modos de Operação
ECB – Eletronic Code Book

- Erro em um bit no bloco cifrado afeta 1 bloco do texto claro decifrado
- Remoção ou adição de 1 bit no texto cifrado afeta o bloco presente e todos os subsequentes

Modos de Operação
CBC – Cipher Block Chaining

- Cada um dos blocos cifrados depende de TODOS os blocos anteriores
- A cada bloco de texto simples é aplicada uma função XOR junto com o bloco cifrado anterior (antes do texto ser criptografado)
- Cada bloco cifrado fica dependente de todos os blocos de texto simples processados até este momento
- Para que cada mensagem seja única, mesmo de um mesmo texto original, um vetor de inicialização único deve ser utilizado no primeiro bloco, preferencialmente gerado aleatoriamente.

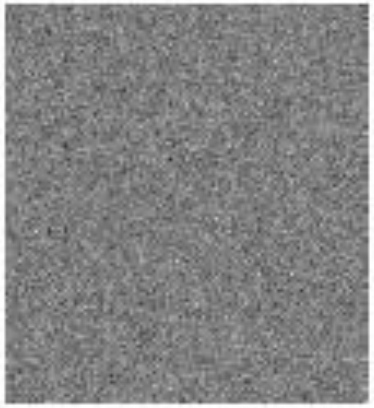
Modos de Operação
CBC – Cipher Block Chaining

- Remove padrões do texto em claro.
- Ideal para grandes massas de dados. Off-line
- Reutilizar um IV transmite alguma informação sobre o primeiro bloco do texto simples e sobre qualquer prefixo comum compartilhado pelas duas mensagens
- Desvantagens
  - criptografia é sequencial (não pode ser paralelizada)
  - Descriptografia pode ser paralelizada
    - dois blocos adjacentes do texto cifrado
  - Mensagem deve ser alinhada de acordo com um múltiplo do tamanho do bloco de cifra

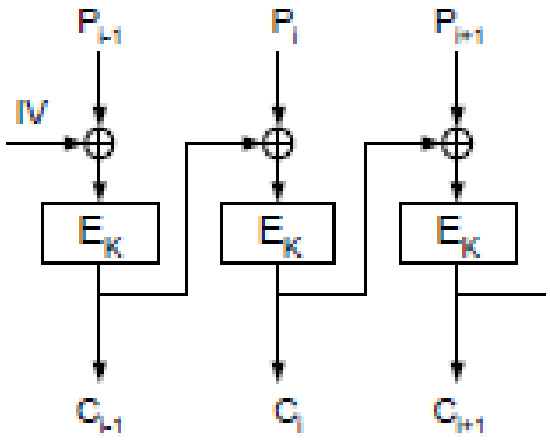
Modos de Operação
CBC – Cipher Block Chaining

Figura em Claro

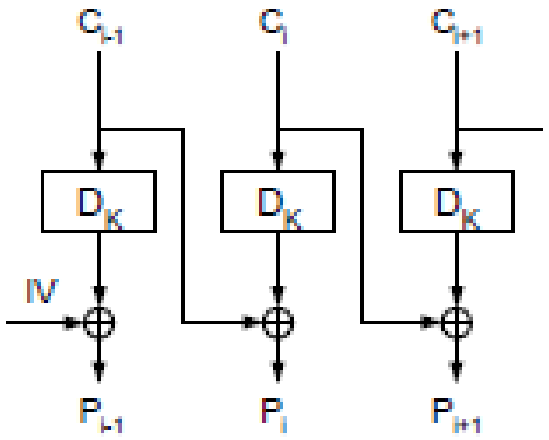
Figura Cifrada Utilizando CBC



Modos de Operação
CBC – Cipher Block Chaining



cifração CBC



decifração CBC

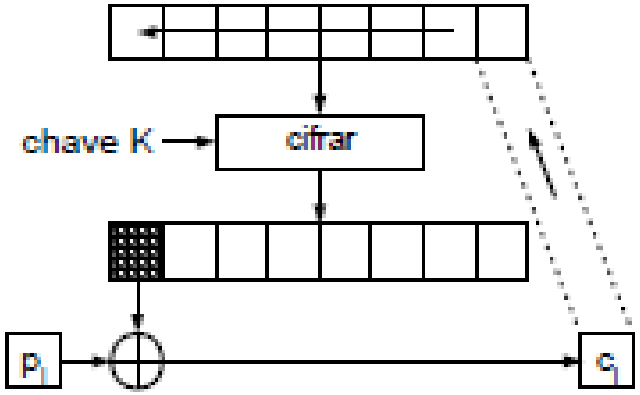
Modos de Operação
CBC – Cipher Block Chaining

- Erro em um bit no bloco cifrado afeta o bloco atual e 1 bit do bloco seguinte do texto claro decifrado
- Remoção ou adição de 1 bit no texto cifrado afeta o bloco atual e todos os seguintes

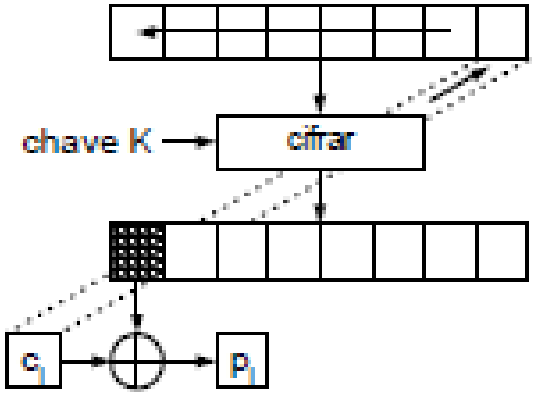
Modos de Operação
Cipher Feedback Block(CFB)

- A mensagem não precisa ser complementada
  - Padding
- Transmissão de uso geral orientada a fluxo
- Difere do OFB apenas porque o texto cifrado (depois da etapa XOR) realimenta o método ao invés da saída da cifra de bloco (antes da etapa XOR)
- NÃO PODE ser usado como um gerador de números pseudo-aleatórios
- Reutilizar um IV transmite alguma informação sobre o primeiro bloco do texto simples e sobre qualquer prefixo comum compartilhado pelas duas mensagens

Modos de Operação
Cipher Feedback Block(CFB)



cifração CFB



decifração CFB

Modos de Operação
Cipher Feedback Block(CFB)

- Erro em um bit no bloco cifrado gera 1 bit trocado no byte atual + 1 bloco no texto claro decifrado
- 1 bit do texto cifrado é removido ou adicionado – o erro se propaga em todos os blocos decifrados a partir deste erro (inclusive)
- CFB - Único que se recupera de problema de sincronismo, desde que seja a ALTERAÇÃO DE UM BYTE inteiro
  - 8 bytes seguintes com erro, depois se recupera

Modos de Operação
Output Feedback Block (OFB)

- Igual ao CFB, só que o byte realimentado não é o cifrado, mas sim usado na cifração
- Permite uso de códigos de correção de blocos
- Os erros de bit na transmissão não se propagam
- Mais vulnerável a um ataque por modificação de fluxo de mensagem do que o CFB
- Ideal para transmissão orientada a fluxo por canal de ruído (ex. comunicação por satélite)
- O OFB do DES pode ser usado para geração de chaves, bem como criptografia de fluxo

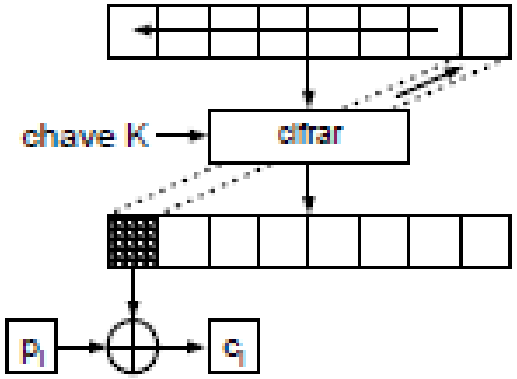
Modos de Operação
Output Feedback Block (OFB)

- O fluxo de bits pode então servir para fazer uma operação XOR com o texto claro a fim de produzir o texto cifrado, transformando efetivamente a cifra de bloco numa cifra de fluxo
- O modo output feedback gera o próximo bloco de fluxo de chave cifrando o bloco de fluxo de chave anterior:
- Reutilizar um IV destrói completamente a segurança
- Transforma uma cifra de bloco num GNPA
  - O texto cifrado realimenta a cifra de bloco e este processo é repetido para produzir um fluxo de bits pseudorrandômicos

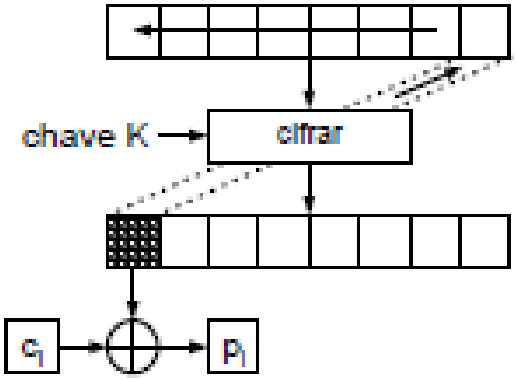
Modos de Operação
Output Feedback Block (OFB)

- O fluxo de bits é totalmente determinado pelo algoritmo, pela chave, por um vetor de inicialização e pelo número de bits que realimentam a cifra em cada etapa
- difere do OFB apenas porque saída da cifra de bloco(antes da etapa XOR) realimenta o método ao invés do texto cifrado (depois da etapa XOR)
- Pré-processamento
  - A execução do algoritmo criptográfico básico não depende da entrada do texto claro ou do texto cifrado
  - O pré-processamento pode ser utilizado para preparar a saída das caixas de criptografia que alimentam as funções XOR

Modos de Operação
Output Feedback Block (OFB)



cifração OFB



decifração OFB

Modos de Operação
Output Feedback Block (OFB)

- Erro de 1 bit no texto cifrado – gera 1 bit errado no texto claro decifrado
- 1 bit do texto cifrado é removido ou adicionado – o erro se propaga em todos os blocos decifrados a partir deste erro (inclusive)

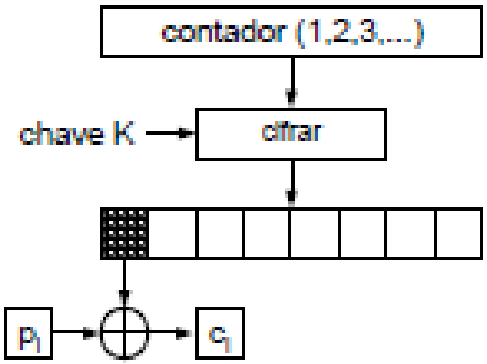
Modos de Operação
Modo counter (CTR)

- Sinônimos
  - Integer Counter Mode - ICM
  - Segmented Integer Counter - SIC
- Pré-processamento
  - A execução do algoritmo criptográfico básico não depende da entrada do texto claro ou do texto cifrado
  - O pré-processamento pode ser utilizado para preparar a saída das caixas de criptografia que alimentam as funções XOR
- Acesso aleatório
  - Diferente dos modos encadeados, no modo counter é possível o processamento aleatório de blocos
- Útil para requisitos de alta velocidade

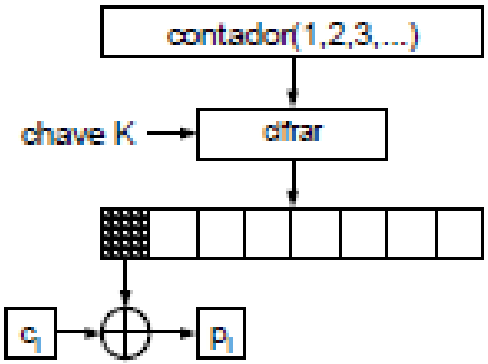
Modos de Operação
Modo counter (CTR)

- Transforma a cifra de bloco em uma de fluxo
- vetor de inicialização é acrescido de uma unidade a cada bloco
  - Nonce
- Reutilizar um IV destrói completamente a segurança
- Vantagem em relação ao OFB
  - Pode-se cifrar ou decifrar Pi sem ter que gerar toda a seqüência para cifração dos Pj (onde j<i) anteriores

Modos de Operação
Modo counter (CTR)



cifração Counter Mode



decifração Counter Mode

Modos de Operação
Modo counter (CTR)

- Erro de 1 bit no texto cifrado – gera 1 bit errado no texto claro decifrado
- 1 bit do texto cifrado é removido ou adicionado – erro em todos os blocos decifrados a partir deste erro

Modos de Operação
Considerações finais

- Nenhum modo proporciona qualquer proteção de integridade
  - É possível a modificação do fluxo de dados
- Aprimora ou adapta o algoritmo para uma aplicação específica
- O modo de operação é quem gera o Padding, não o algoritmo
  - ECB
  - CBC

Modos de Operação
Considerações finais

- Vetor de Inicialização
  - O Vetor de Inicialização ou Initialization Vector, em inglês, é uma espécie de 'bloco falso' que inicializa o processo para o primeiro bloco verdadeiro
  - Ele que dá uma aleatoriedade ao processo, fazendo com que mesmo texto que seja encriptado várias vezes, o código encriptado resultante seja diferente
  - Serve para que mensagens que começam iguais não gerem os mesmos textos cifrados
  - O VI não precisa ser secreto, mas é importante que o mesmo VI não seja reutilizado com a mesma chave
  - A criptografia no envio é importante para garantir integridade

Modos de Operação
Considerações finais

- Vetor de Inicialização
  - Nos modos CBC e CFB, a reutilização de VIs deixa vazar algumas informações
  - Nos modos OFB e CTR, VIs repetidos destroem totalmente a segurança
  - Já no modo CFB, o VI precisa ser gerado randomicamente e ser mantido em segredo até que o primeiro bloco de texto claro esteja pronto para ser cifrado
  - ECB não requer VI
    - Todos os outros modos o requerem
  - Não há adição de qualquer segurança extra
    - O algoritmo de criptografia é quem fornece a segurança

Modos de Operação
Considerações finais

- Block Replay
  - ECB não é imune
  - Todos os outros são
- Gerar cifra em Fluxo
  - Não precisam de padding
- Somente os modos ECB e CBC necessitam do algoritmo de decriptografia, os demais necessitam somente do algoritmo de criptografia
  - Melhor desempenho

Bateria de Questões de Aprendizagem 1

Criptografia

Modos de Operação Dos Sistemas Criptográficos Simétricos

ITnerante

FINEP – CESGRANRIO 2011 – Analista Suporte

1. Um algoritmo de cifra de bloco é um elemento básico para fornecer segurança aos dados que devem ser criptografados. O NIST publicou na Special Publications 80.0-38.A, uma lista com modos de operação de cifra de bloco que são usados com qualquer cifra de bloco simétrica, incluindo DES triplo e AES. Os modos de operação publicados são:

A. ECB (Electronic Code Book), CBC (Cipher Block Chaining), CFB (Cipher feedback), OFB (Output Feedback), CTR (Counter)

B. ECB (Electronic Code Book), CBC (Cipher Block Chaining), OFB (Output Feedback), CTR (Counter), RC (Random Chaining)

C. ECB (Electronic Code Book), CBC (Cipher Block Chaining), CFB (Cipher feedback), RC (Random Chaining), ACTR (Advanced Counter)

D. CBC (Cipher Block Chaining), CFB (Cipher feedback), OFB (Output Feedback), RC (Random Chaining), ACTR (Advanced Counter)

E. CBC (Cipher Block Chaining), CFB (Cipher feedback), OFB (Output Feedback), CTR (Counter), RC (Random Chaining)

INMETRO – CESPE 2010 – pesquisador TMQ – Desenvolvimento de Sistemas

2. No que se refere à criptografia, assinale a opção correta.

A. Nos sistemas simétricos, os modos de operação ECB e CBC são seguros.

B. O esforço computacional necessário para cifração e decifração é idêntico para sistemas simétricos e assimétricos.

C. Confidencialidade e integridade são obtidas apenas nos sistemas assimétricos.

D. Autenticidade e não repúdio são obtidos nos sistemas simétricos.

E. Nos sistemas assimétricos, cada usuário utiliza duas chaves: uma que deve ser mantida secreta e a outra que é pública.

INMETRO – CESPE 2009 – Analista Executivo em metrologia e Qualidade - redes

3. A respeito dos sistemas criptográficos, julgue os itens que se seguem.

[61] O modo ECB é mais seguro que o CBC, mas é menos eficiente que o CTR.

[62] Os sistemas assimétricos normalmente demandam mais recursos computacionais para cifração e decifração quando comparados aos sistemas simétricos.

[63] A segurança do criptossistema RSA tem como base a dificuldade em se fatorar grandes números em seus fatores primos.

[64] A criptografia simétrica oferece sigilo, integridade, autenticidade e irretratabilidade.

[65] O criptosistema Diffie-Hellman é normalmente usado para cifração e decifração, além do estabelecimento de chaves.

SUSEP – ESAF 2006 – Analista Técnico - TI

4. Técnicas criptográficas são essenciais à segurança da informação, nas organizações. A respeito de tal contexto, é correto afirmar que

A. no modo CBC (*Cipher Block Chaining) do DES (Data Encryption Standard), se houver um erro em um bloco do criptograma transmitido, apenas aquele bloco da mensagem original será afetado, ou seja, o erro não se propaga aos demais blocos.*

B. para A enviar uma mensagem M confidencial para B, uma possibilidade é encriptar M com uma chave secreta ECB-DES (*Encoding Code Book - Data Encryption Standard) e encriptar a chave secreta com a chave pública RSA (Rivest-Shamir-Adleman) de B, garantindo melhor performance ao processo.*

C. o DES [*Data Encryption Standard] é um algoritmo simétrico com chaves de tamanho 64 bits, baseando-se em operações XOR (OU-exclusivo) e S-boxes (caixas-S) variáveis.*

D. o RSA (*Rivest-Shamir-Adleman) é um algoritmo de criptografia simétrica que limita o tamanho das chaves em 1024 por questões de desempenho, já que se baseia em operações com números primos de grande magnitude.*

E. para um grupo de N usuários, haveria 1 chave pública e N chaves privadas para provar uma comunicação confidencial para quaisquer usuários, i e j, ao considerar a criptografia assimétrica.

SEFAZ-AM – NCE 2005 – Analista de TI

5. Com relação à criptografia, é INCORRETO afirmar que:

A. criptografia simétrica usa a mesma chave para codificar e decodificar uma mensagem;
B. RSA é um algoritmo de criptografia assimétrico;
C. o algoritmo DES possui os modos de operação ECB, CBC e CFB;
D. o protocolo SSL exige que ambos servidor e cliente tenham certificados digitais;
E. MD5 e SHA-1 são funções de resumo de mensagens (hash).

SEFAZ-AM – NCE 2005 – Analista de TI

6. Acerca de criptografia, uma das técnicas fundamentais para a segurança da informação, de protocolos criptográficos e de sistemas de criptografia e aplicações, julgue os itens subsequentes.

- O modo de operação cipher block chain (CBC) pode ser aplicado à maioria dos algoritmos de criptografia. Na sua utilização como algoritmo data encryption standard (DES), o modo CBC impede que um atacante substitua um bloco cifrado sem ser descoberto. Entretanto, o modo CBC do DES apresenta o inconveniente de permitir que um erro em um bloco cifrado afete a decifração de todos os demais blocos.
- Um protocolo de assinatura digital deve apresentar como propriedades básicas a impossibilidade de fabricação de assinaturas por terceiros e a garantia da autenticidade de determinada assinatura. Além disso, deve garantir que uma transação com assinatura digital seja inalterável e não possa ser reutilizada em outra ocasião.
- Um dos fatores que complicam o emprego de sistemas de criptografia simétricos com chave privada única é a necessidade de distribuir e armazenar chaves (N * (N-1))/2 , caso haja um canal criptográfico próprio para cada par de usuários em um conjunto de N usuários.

Gabarito

1. A
2. E
3. E, C, C, E, E
4. B
5. D
6. E, C, C

Criptografia Intermediária

Certificação Digital

ITnerante

PKC - Public Key Certificate

- Conjunto de dados à prova de falsificação
- Missão do PKC: Associar uma entidade a uma chave pública
- São assinados digitalmente por uma CA/AC
  - Terceiros confiáveis confirmam a identidade
- Armazenados em diretórios públicos

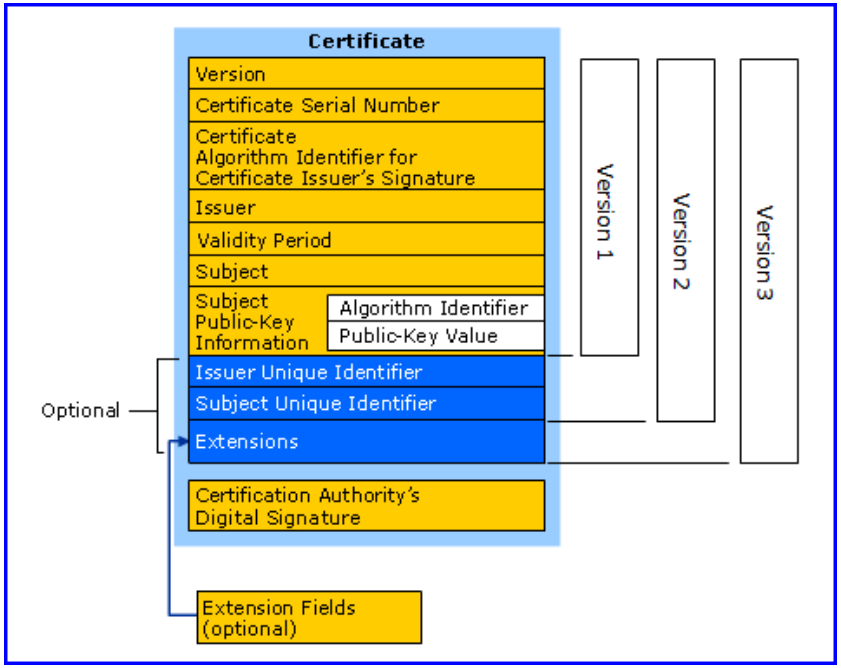
PKC - Public Key Certificate

- Garante, por força da legislação atual, validade jurídica aos atos praticados com o seu uso
- Documento eletrônico que por meio de procedimentos lógicos e matemáticos assegura a integridade das informações e a autoria das transações

PKC - Public Key Certificate

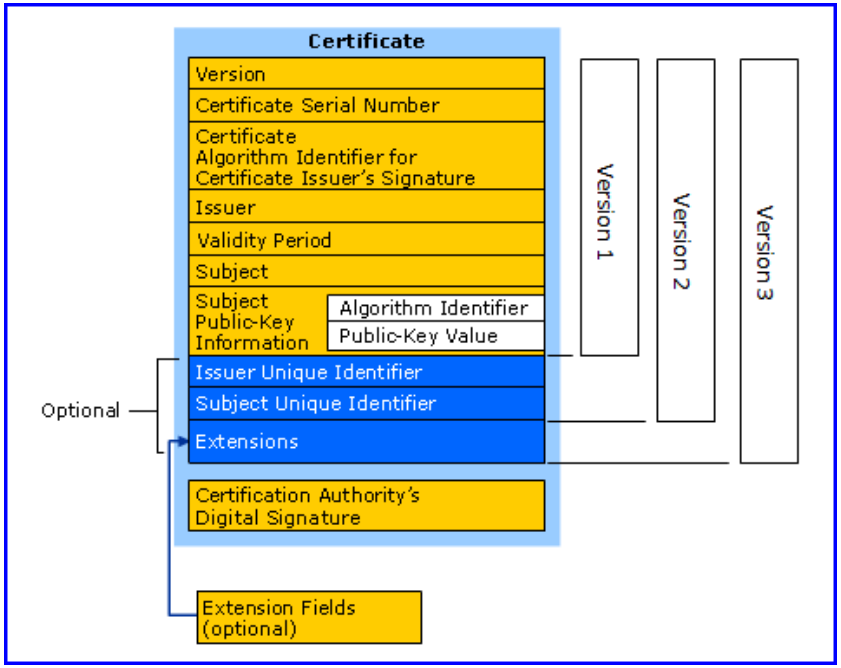
- Existem vários padrões.
  - PGP - patenteado
  - IPSEC
  - Mais reconhecido X.509.v3

PKC - Public Key Certificate
Padrão X.509.v3



- Versão
- Número Serial (gerado pela CA)
- Identificador do algoritmo de assinatura
- Nome do emissor (DN)
- Validade (Não antes/Não depois)
- Nome do sujeito (DN)
- Informações sobre a chave pública do sujeito

PKC - Public Key Certificate
Padrão X.509.v3



- Formato de certificado mais amplamente aceito
- Transmissões sempre através de conexões seguras (SSL, por exemplo)
- Não dita nenhum algoritmo de hash
- Recomenda o RSA
- Passo a Passo

1. Escolher uma AC
2. Solicitar a emissão à AC/AR
3. Validação presencial na AR
4. Será notificado sobre os procedimentos para baixar o certificado

www2.bancobrasil.com.br.crt

Tipos de Certificado

- Série A (A1, A2, A3 e A4)
  - Reúne os certificados de assinatura digital, utilizados na confirmação de identidade na Web, em e-mail, em redes privadas virtuais (VPN) e em documentos eletrônicos com verificação da integridade de suas informações
- Série S (S1, S2, S3 e S4)
  - Reúne os certificados de sigilo, que são utilizados na codificação de documentos, de bases de dados, de mensagens e de outras informações eletrônicas sigilosas

Tipos de Certificado
Considerações importantes

- Os oito tipos são diferenciados pelo uso, pelo nível de segurança e pela validade
  - A1 e S1: As chaves privadas ficam armazenadas no próprio computador do usuário
  - A2, A3, A4, S2, S3 e S4: As chaves privadas e as informações referentes ao seu certificado ficam armazenadas em um hardware criptográfico
    - cartão inteligente (smart card)
    - cartão de memória (token USB ou pen drive)

Tipos de Certificados Digitais

Certificado	Tam Chave (bits)	Geração Chave	Mídia Armazenamento	Validade (Anos)
A1 / S1	1024	Soft	Rep protegido por senha	1
A2 / S2	1024	Soft	Smart / Token – Sem capacidade de geração de chave	2
A3 / S3	1024	Hard	Smart / Token – Com capacidade de geração de chave	3
A4 / S4	2048	Hard	Smart / Token – Com capacidade de geração de chave	3

Tipos de Certificado Considerações importantes

- A1 e A3 são os mais usados
  - A1 - de menor nível de segurança, é gerado e armazenado no computador do usuário. Os dados são protegidos por uma senha de acesso. Somente com essa senha é possível acessar, mover e copiar a chave privada a ele associada,
  - A3 - de nível de segurança médio a alto, é gerado e armazenado em um hardware criptográfico, que pode ser um cartão inteligente ou um token. Apenas o detentor da senha de acesso pode utilizar a chave privada, e as informações não podem ser copiadas ou reproduzidas

Ger. de múltiplos pares de chaves

- Assinatura-digital
  - Backup durante toda vida útil para garantir a decriptografia
  - Não há necessidade de backup da chave privada após a vida útil
    - Deve ser seguramente destruída
  - Em caso de perda, um novo par é gerado sem problemas
  - Usuários finais geram as chaves para oferecer não repúdio

Ger. de múltiplos pares de chaves

- Criptografia
  - Backup durante toda vida útil para garantir a decriptografia
  - Há necessidade de backup da chave privada após a vida útil (decriptografia dos dados legados)
  - Backup da chave pública
    - RSA - Chave pública não requer arquivamento ou backup
    - DH - Há necessidade de armazenamento da chave pública para recuperação posterior de dados
- Sistema central fornece as chaves da criptografia

ITnerante

Aplicações Recentes

- e-CPF
- e-CNPJ
- Passaporte Eletrônico
- RIC
- e-NF
- Etc...

PKC - Public Key Certificate Revogações

- Lista de Certificados Revogados- LCR / CRL
- Causas
  - Mudança de info no certificado
  - Dano com a chave privada
  - Comprometimento da chave privada da AC ou Usuário
  - Vício de origem

PKC - Public Key Certificate Revogações

- Certificados revogados na lista de revogação de certificados – CRL. Está na versão 2
- Lista torna-se grande com o tempo
  - Solução CRLs Delta - lista apenas alterações incrementais a partir da precedente
  - CRLs Indiretas - fornecida para a parte verificadora por terceiros que não emitiram o certificado
  - Um certificado pode também ser apenas suspenso sem a necessidade de revogação (Férias)

PKC - Public Key Certificate Revogações

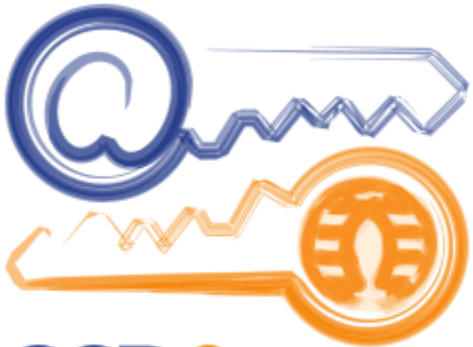
- Problema com as CRLs – Gap temporal entre as publicações
- Solução - OCSP - Online Certificate Status Protocol
  - Protocolo usado para conferência on-line de revogação
  - Dribla o gap de tempo entre as publicações DE CRLS
- Tipos de status: Bom, revogado, desconhecido + intervalo de validade + opcionalmente a razão da revogação
- As respostas emitidas por este serviço são individuais e assinadas digitalmente
  - O outro método é a LCR
- Computador - respondedor de OCSP

PKC - Public Key Certificate
Considerações importantes

- Protocolos
  - De gerenciamento - CMP
  - Protocolo on-line do status do certificado – OCSP
- Renovação de certificado
  - Renova-se o prazo de uso da mesma chave
  - Troca-se o certificado

PKI - Componentes

1. Autoridade Certificadora (CA – AC)
2. Autoridade de Registro
3. Repositório de Certificado
4. Servidor de Recuperação de Chave
5. Usuário Final



ITnerante

PKI - Componentes

- Autoridade Certificadora (CA – AC)
  - Entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais
  - Desempenha como função essencial a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado
  - Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada).

ITnerante

PKI - Componentes

- Autoridade Certificadora (CA – AC)
  - Cabe também à AC emitir listas de certificados revogados - LCR e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação - DPC
  - Emite, gerencia e revoga certificados para SEUS usuários finais
  - Fornece sua chave pública aos usuários finais e aos verificadores
  - Categorias
    - Públicas
    - Privadas
  - Algumas ACs suportam dois pares de chaves
  - Registro: Momento no qual o usuário final e a CA estabelecem a confiança
  - Certificados de AC Raiz são "auto-assinados"

ITnerante

PKI - Componentes

- Autoridade de Registro (RA - AR)
  - Intermediária entre a CA e o usuário final
  - Recebimento, validação, encaminhamento de solicitações de forma presencial
  - Autoridade delegada pela CA
  - Usuário final e CA estabelecem a confiança

PKI - Componentes

- Repositório de Certificado
  - Único ponto para administração e distribuição de certificados
  - Não existe padrão para os diretórios (X.500)
  - A mais conhecida alternativa é o LDAP
    - Simplificação do X.500, usado para acessar os diretórios sobre TCP/IP
  - As CRLs também se encontram aqui

PKI - Componentes

- Servidor de recuperação de chave
  - Perda da chave privada
    - CA revoga o PKC correspondente
    - Novo par de chaves é gerado
    - Novo PKC criado
  - Backup das chaves privadas no momento da criação para posterior recuperação

PKI - Componentes

- Usuário final
  - Pode gerar as chaves ou pedir à CA que o faça
  - Chave pública fica com a CA
  - Chave privada com a entidade

ICP - Brasil

- Modelo Hierárquico: Uma AC não pode certificar outra que não seja imediatamente inferior (hierarquia)
- AC Raiz no Brasil é o ITI
  - É a primeira autoridade da cadeia de certificação
  - Executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil
  - emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras DE NÍVEL IMEDIATAMENTE SUBSEQUENTE AO SEU
  - encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil
  - Somente a AC Raiz pode realizar certificação cruzada com AC raízes noutros países

Modelos de confiança

- Hierarquia de certificados
  - CA delega autoridade para uma ou mais autoridades subsidiárias que também podem delegar...
  - Nem todas as partes devem confiar automaticamente em todas autoridades certificadoras
  - A única autoridade cuja confiança deve ser estabelecida é a CA raiz

Modelos de confiança

- Caminho de certificação
  - Inicia a busca a partir do nó mais confiável
- Certificação cruzada
  - Permite a interação entre domínios independentes de PKI de CAs e usuários finais
  - Cada CA deve operar de maneira independente
  - Caminho de confiança não hierárquico
  - Depois que duas CAs estabelecem um caminho de confiança, as partes verificadoras são capazes de confiar em usuários finais do outro domínio
  - Entre o Brasil e o exterior, somente via AC Raiz

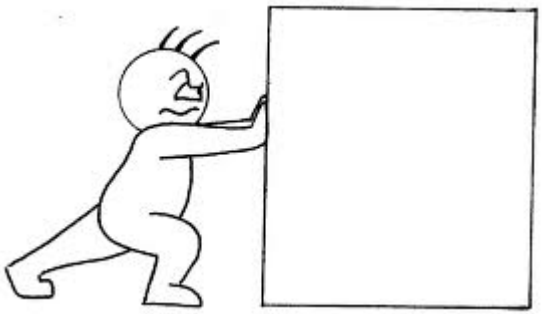
Modelos de confiança

- Cadeia de Certificados X.509
  - Método mais comum

  1. verifica-se se o certificado está assinado com a chave privada do próximo certificado na cadeia
  2. Verificar se cada certificado está revogado ou expirado
  3. Certificado esteja em conformidade com um conjunto de critérios

Modelos de confiança

- Cadeia de Certificados X.509
  - Modelos
    - Push - Emissor envia a cadeia inteira de certificados de uma só vez
    - Pull - Envia apenas o certificado do remetente e deixa para o destinatário extrair o certificado da CA



Bateria de questões de aprendizagem 2

Criptografia Intermediária

Certificação Digital

ITnerante

MPE AP – FCC 2012 – Analista Ministerial - TI

1. São elementos da Public Key Infrastructure: End-Entities, Certification Authority, Certificate Repository e

A. Public Defender (PD).
B. Registration Authority (RA).
C. Certificate Revocation Authority (CRA).
D. Users Validation Authority (UVA).
E. Private Only Registration Authority (PRA).

CGU – ESAF 2012 AFC - TI

2. Infraestrutura de Chave Pública é o conjunto de hardware, software, pessoas, políticas e procedimentos necessários para

A. instanciar, transmitir, apagar, publicar e revogar certificados digitais.
B. montar, validar perante a Polícia Federal, distribuir e apagar certificados digitais.
C. criar, gerenciar, armazenar, distribuir e revogar certificados digitais.
D. criar, instanciar, armazenar, restaurar e publicar certificados digitais.
E. montar, gerenciar, armazenar, restaurar e publicar certificados digitais.

CHESF – CESGFRANRIO 2012 – Analista de Sistemas

3. A autoridade Certificadora Raiz da ICP-Brasil é o

A. Instituto Brasileiro de Segurança da Informação
B. Instituto Nacional de Tecnologia da Informação
C. Instituto Nacional de Pesos e Medidas
D. Instituto Nacional de Metrologia, Normalização e Qualidade Industrial
E. Gabinete de Segurança Institucional

SUSEP – ESAF 2006 – Analista Técnico - TI

4. A1 e S1 são tipos de certificados digitais com tamanho da chave criptográfica de ??? bits e com validade de ???.

As lacunas I e II são preenchidas correta e respectivamente por:

A. 2048; dois anos.
B. 1024; seis meses.
C. 4096; cinco anos.
D. 2048; três anos.
E. 1024; um ano.

PETROBRAS – CESGRANRIO 2012 – Analista de Sistemas Júnior Infraestrutura

5. O certificado digital visa a garantir a associação de uma chave pública a uma pessoa, entidade ou host. Para isso, a Autoridade Certificadora (AC) que emite o certificado digital deve

A. apenas gerar sua assinatura digital para o certificado emitido.

B. apenas fazer a criptografia assimétrica do certificado emitido.

C. apenas fazer a criptografia simétrica do certificado emitido.

D. gerar sua assinatura digital para o certificado emitido e fazer a criptografia assimétrica desse certificado.

E. gerar sua assinatura digital para o certificado emitido e fazer a criptografia simétrica desse certificado.

PETROBRÁS – CESGRANRIO 2012 – Engenheiro de Telecomunicações Júnior

6. A Public Key Infrastructure (PKY) tem uma série de funções executadas por componentes específicos da infraestrutura. Uma dessas funções é descrita como um tipo de certificação necessária, empregada quando um certificado de uma Certificate Authority (CA) é enviado a outra CA, de modo que uma entidade de um domínio administrativo possa comunicar-se de forma segura com uma entidade de outro domínio. Essa interoperabilidade entre certificados é importante em um ambiente corporativo, no qual os usuários acessam recursos de diferentes organizações.

Essa função é denominada certificação

A. universal
B. referencial
C. integralizada
D. globalizada
E. cruzada

7. Ao gerar o par de chaves criptográficas para o certificado digital, a Autoridade de Registro

A. armazena a chave pública.
B. armazena a chave privada.
C. armazena as chaves pública e privada.
D. armazena a chave privada e a senha de acesso à chave.
E. armazena as chaves pública e privada e a senha de acesso à chave privada.

INFRAERO – FCC 2011 – Analista Superior III – Segurança da Informação

8. Sobre Certificação Digital, analise:

I. As transações feitas com a identidade digital têm validade jurídica garantida pela Medida Provisória 2.200.

II. A validade do certificado digital pode variar de 1 a 3 anos. Após o vencimento, é necessário fazer a renovação novamente com a Autoridade de Registros.

III. Smart card, token ou computador pessoal são algumas das opções de armazenamento do certificado digital.

IV. O certificado digital Tipo A1 oferece maior segurança e praticidade, pois, é gerado e armazenado em um hardware, ou seja, em um smart card ou token.

Está correto o que consta em

A. I, II, III e IV.

B. I, II e III, apenas.

C. I e II, apenas.

D. II, III e IV, apenas.

E. I e IV, apenas.

UFPA – CEPS-UFPA 2011 – Analista de TI - Suporte

9. Assinale a alternativa que contém informações presentes em um certificado digital X.509.

A. Número serial, emissor, validade, informações da chave pública, versão.
B. Valor da assinatura, validade, informações da chave pública e privada, emissor.
C. Validade, número serial, chave privada, emissor, informações da chave pública.
D. Informações da chave privada, validade, algoritmo de assinatura, valor da assinatura.
E. Emissor, algoritmo de assinatura, valor da assinatura, informações da chave privada, validade

TRT 19 – FCC 2011 – Técnico Judiciário - TI

10. Sobre a chave pública do titular do documento de um certificado digital pode-se afirmar:

A. Uma mensagem assinada digitalmente é criptografada com a chave pública do emissor antes de ser enviada.
B. Somente quem recebe uma mensagem assinada deve conhecer.
C. É utilizada apenas na criptografia simétrica, no processo de certificação digital.
D. Somente seu dono deve conhecer.
E. Quando o destinatário recebe um documento assinado digitalmente, ele utiliza a chave pública do emissor para decifrá-la.

Gabarito

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

Bateria de questões de aprendizagem 3

Criptografia Intermediária

Certificação Digital

ITnerante

TRT 19 – FCC 2011 – Técnico Judiciário - TI

1. Na estrutura I, a II , é composta por entidades vinculadas operacionalmente a uma determinada III. Sua função é identificar e cadastrar os usuários, em postos de atendimento a que os mesmos possam comparecer e, a partir daí, encaminhar as solicitações de certificados digitais para uma IV. As lacunas I, II, III e IV são completadas correta e respectivamente por

A. da Casa Civil da Presidência da República, Autoridade de Registro, Autoridade Certificadora Raiz, Autoridade Certificadora.

B. ICP Brasil, Autoridade de Registro, Autoridade Certificadora, Autoridade Certificadora.

C. ICP Brasil, Autoridade Certificadora, Autoridade de Registro, Autoridade de Registro.

D. da Casa Civil da Presidência da República, Autoridade Certificadora Raiz, Autoridade Certificadora, Autoridade de Registro.

E. de criptografia, Autoridade de Registro, Autoridade Certificadora Raiz, Autoridade Certificadora.

UFSC– UFSC 2011 – Analista de TI

2. Assinale a alternativa CORRETA a respeito do emprego de certificação digital, levando em conta as normas legais brasileiras.

A. De modo a assegurar o sigilo na comunicação, o remetente de uma mensagem de correio eletrônico deve ser identificado através de um certificado digital.

B. A autenticidade de um servidor Web seguro pode ser verificada por meio da validação do certificado digital fornecido pelo servidor.

C. Um certificado digital contém a chave privada da Autoridade Certificadora (AC) que o emitiu.

D. Um certificado digital contém a chave privada do sujeito detentor do certificado.

E. Um certificado digital emitido por uma Autoridade Certificadora (AC) reconhecida só deixará de ser válido quando for atingida a sua data de expiração.

FINEP – CESGRANRIO 2011 – Analista de Suporte

3. Um certificado de chave pública (certificado digital) é um conjunto de dados à prova de falsificação e que atesta a associação de uma chave pública a um usuário final. Essa associação é garantida pela Autoridade Certificadora (AC) que emite o certificado digital após a confirmação da identidade do usuário. Com relação ao certificado emitido por uma AC, sua integridade e autenticidade são conferidas APENAS de posse da

A. assinatura digital presente no certificado
B. assinatura digital presente no certificado e da chave pública da AC
C. assinatura digital presente no certificado e da chave privada da AC
D. assinatura digital presente no certificado e das chaves pública e privada da AC
E. assinatura digital presente no certificado e do certificado e chave privada da AC

CORREIOS – CESPE 2011 – Analista de Correios – Suporte de Sistemas

4. Com relação a certificação digital e infraestrutura de chaves públicas, julgue os itens que se seguem

[101] O protocolo LDAP (lightweight directory access protocol) não possui utilidade em uma infraestrutura de chave pública.

[102] A Infraestrutura de Chave Pública Brasil (ICP-Brasil) emite certificados, autentica-os e possui uma autoridade certificadora que faz manutenção dos certificados durante o ciclo de vida destes, apesar de não ser uma entidade reconhecida pela legislação brasileira.

[103] Para se garantir o tráfego seguro e criptografado na autenticação entre o usuário e um servidor que disponibiliza determinado serviço na Internet, pode-se utilizar certificado digital, que é validado por uma autoridade certificadora e utiliza o protocolo HTTPS

CORREIOS – CESPE 2011 – Analista de Correios – Desenvolvimento de Sistemas

5. Julgue os itens seguintes, a respeito de certificação digital e assinatura digital

[108] Para conferir a autenticidade de um certificado digital, é necessário utilizar o certificado digital da autoridade certificadora que o emitiu. Esse certificado pode ser emitido por outra autoridade certificadora ou pode ser autoassinado.

[109] Para assinar digitalmente um documento eletrônico, um usuário deve utilizar a chave que consta no seu certificado digital.

TRT 1 – FCC 2011 – Analista Judiciário – TI

6. Considere:

I. A Infraestrutura de Chaves Públicas (ICP) pode ser formada por órgão, ou iniciativa pública ou privada, com competência para definir os padrões técnicos e práticos para suportar um sistema criptográfico com base em certificados digitais.

II. A AC Raiz da ICP-Brasil, representada pelo ITI, é a responsável por fazer o credenciamento e auditoria de toda a cadeia hierárquica de confiança e delega às ACs a responsabilidade pela fiscalização e supervisão das ARs.

III. Nos níveis de hierarquia que formam a cadeia de confiança de uma ICP, apenas o segundo nível, sempre representado por uma AC, está habilitado para gerar um certificado digital.

IV. A obtenção de um certificado digital pode ser feita por qualquer pessoa jurídica ou física, bastando apresentar fisicamente a documentação necessária a uma AR, que passará esses dados para a AC à qual é subordinada.

É correto o que consta APENAS em

A. I e II.

B. I e IV.

C. II e III.

D. II, III e IV.

E. III e IV.

7. São itens associados à certificação digital, EXCETO:

A. privacidade.
B. chave pública.
C. chave privada.
D. criptografia assimétrica .
E. criptografia simétrica.

8. Sustentando a certificação digital existe toda uma cadeia que envolve políticas de uso, procedimentos, mecanismos de segurança e entidades que seguem diretrizes e normas técnicas determinadas por uma entidade ou comitê gestor. Essa cadeia chama-se

A. Autoridade Certificadora Suprema (AC-Raiz).
B. Comitê Gestor de Chave Pública (PKMC).
C. Autoridade Certificadora (AC).
D. Autoridade de Registro (AR).
E. Infraestrutura de Chave Pública (PKI).

TRT 24 – FCC 2011 – Analista Judiciário – TI

9. Consiste em uma chave pública mais um ID de usuário do proprietário da chave, com o bloco inteiro assinado por um terceiro que tenha credibilidade. A definição é de

A. assinatura digital e o terceiro referido corresponde ao signatário recebedor da mensagem.

B. criptografia assimétrica e o terceiro referido corresponde ao signatário recebedor da mensagem.

C. criptografia simétrica e o proprietário referido corresponde a uma autoridade certificadora.

D. certificado de chave pública e o terceiro referido corresponde a uma autoridade certificadora.

E. assinatura de chave pública e o proprietário referido corresponde a uma autoridade certificadora.

10. Assinale a opção correta.

A. A criptografia verifica se uma entidade é quem diz ser.
B. A autoridade certificadora (CA) cria um certificado que vincula a chave pública da entidade à entidade verificada.
C. A componente certificadora (CC) verifica se uma entidade é parte de outra entidade.
D. A autoridade autenticadora (AA) desvincula a chave pública da entidade da chave primária da entidade verificada.
E. A autoridade certificadora (CA) cria uma chave privada que substitui a chave pública da entidade.

Gabarito

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