SIO-Criptografia assimétrica

**1. Para enviar uma mensagem confidencial a um destinatário, usando criptografia assimétrica, deve:**

a) cifrar a mensagem usando a sua (remetente/ originador) chave pública

b) cifrar a mensagem usando a sua (remetente/ originador) chave privada

c) cifrar a mensagem usando uma síntese da sua (remetente/ originador) chave pública

d) cifrar a mensagem usando uma cifra híbrida com a chave simétrica aleatória e a chave pública do destinatário

**2.Uma cifra híbrida consiste em:**

(a) Um mecanismo para aumento da performance no uso prático de chaves assimétricas

(b) Cifrar um texto com uma chave assimétrica aleatória, que é cifrada com a chave pública do destinatário

(c) Utilizar uma qualquer combinação de algoritmos de cifra

(d) Realizar uma cifra com controlo de integridade

**3. Uma cifra híbrida consiste em:**

(a) Utilizar cifra com decifra

(b) Utilizar uma combinação de cifras por blocos e contínuas

(c)Cifrar um texto com uma chave simétrica aleatória, que é cifrada com a chave pública do destinatário

(d) Utilizar uma qualquer combinação de algoritmos de cifra

SIO-Assinaturas digitais

**1.Um dos objectivos das assinaturas digitais é o não-repúdio, que consiste em:**

a) Garantir que uma mensagem, no documento, não sofreu qualquer alteração

b) Impedir o acesso não autorizado ao conteúdo das mensagens/documentos

c) Forçar o uso de smartcards na geração de assinaturas

d) Impedir que uma entidade que produziu uma mensagem/documento assinada(o) o

possa negar

**2.Para se verificar uma assinatura digital de um documento é preciso:**

a) A chave privada do assinante

b) O certificado de chave pública do verificador

c) O certificado de chave privada do assinante

d) O certificado de chave publica do assinante

**3. A assinatura digital de um documento:**

a) garante que é possível detetar qualquer adulteração do mesmo após a sua assinatura

b) deixa de ser válida quando o par de chaves do assinante expira

c) impede que o documento possa ser compreendido por quem não estiver autorizado

d) pode, em certos casos, ser realizada com chave simétrica

**4. Uma assinatura digital de uma mensagem:**

(a) Permite que terceiros verifiquem a identidade de quem a envia numa rede

(b) Impede que o recetor aceite uma mensagem adulterada depois de assinada

(c) Garante a identidade de quem a envia numa rede

(d) Garante a identidade de quem a recebe

**5. Um dos objectivos das assinaturas digitais é o não- repúdio, que consiste em:**

(a) Impedir a negação da criação de uma assinatura digital

(b) Impedir o acesso não autorizado ao conteúdo das mensagens/documentos

(c) Forçar o uso de smartcards na geração de assinaturas

(d) Impedir que uma entidade negue a autoria de um documento de texto

**6. Para se verificar uma assinatura digital de um documento precise**

(a) A chave pública do verificador

(b) A identidade do assinante

(c)A chave pública do assinante

(d) O certificado de chave pública do verificador

**7.Uma assinatura digital de uma mensangem usando RSA:**

(a) Não tem qualquer vantagem em relação a uma autenticação com um MAC

(b) Permite que terceiros verifiquem a identidade de quem a envia

(c) Garante a identidade de quem a envia

(d) Garante a identidade de quem a cria

SIO-Derivação de chaves

**1. Ao utilizar o mecanismo PBKDF2, que informação pode ser publica?**

(a) O tamanho dos blocos

(b) O Pseudo Random Generator

(c) O número de blocos

(d) O tipo de operações

**2. Ao utilizar o mecanismo PBKDF2, que informação deve ser privada?**

(a) A dimensão do resultado

(b) A senha

(c)O Pseudo Random Generator

(d)O tamanho dos blocos

SIO-Gestão de chaves assimétricas

**1.Uma Entidade Certificador raíz é confiável porque:**

a) Confiamos na correção da sua chave pública

b) Ninguem certifica o seu certificado

c) Tem um certificado autoassinado

d) Certifica muitas outras Entidades Certificadoras

**2.Tendo em conta o período de validade de um certificado, qual destas afirmações é falsa?**

a) Serve para limitar, no tempo, o uso da correspondente chave privada

b) Impede que a chave privada possa ser usada fora desse periodo

c) Não pode ser usado para validar assinaturas feitas fora desse periodo

d) Pode ser encurtado caso seja revogado

**3. Tendo em conta o uso de CRL qual destas é falsa?**

a) as listas delta completam as listas base

b) quando uma lista base é emitida, importa obrigatoriamente a lista delta imediatamente anterior

c) as CRL indicam a data de revogação dos certificados revogados

d) as CRLS delta incluem certificados expirados, mas as CRL base não.

**4. Em qual dos seguintes casos é possível um utente realizar uma verificação incompleta, mas válida, de uma cadeia de certificação?**

a) a data do certificado é válida

b) o certificado não está listado na CRL

c) não é de todo possível

d) existe uma Entidade Certificadora (CA) intermédia confiável no caminho da certificação

**5. Tendo em conta o uso de CRL (Certificate Revocation List), qual destas afirmações é verdadeira?**

(a) As CRL indicam a identidade dos sujeitos afetos aos certificados revogados

(b) A localização da CRL de uma Entidade Certificadora faz parte de todos os certificados que ela revogar

(c) As CRL delta incluem certificados expirados, mas as CRL base não

(d) Quando uma lista base é emitida, importa obrigatoriamente a lista delta imediatamente anterior

**6. Em qual dos seguintes casos é possível um utente realizar uma verificação incompleta, mas válida, de uma cadeia de certificação?**

(a) Existe confiança na Entidade Certificadora (CA) raiz do caminho de certificação

(b) A validação via OCSP (Online Certificate Status Protocol) devolve indicação de que o certificado é válido

(c) Não é de todo possível

(d) O certificado de uma Entidade Certificadora (CA) intermédia foi revogado após a data do certificado por ela assinado

**7. Tendo em conta o uso de CRL (Certificate Revocation List), qual destas afirmações é verdadeira?**

(a)As CRL delta constituem uma validação de integridade das CRL base

(b) As CRL base devem ser obtidas em conjunto com as CRL delta

(c) As CRL delta devem ser consultadas a cada acesso remoto

(d) Quando uma lista base é emitida, importa obrigatoriamente a lista delta imediatamente anterior

**8. Em qual dos seguintes casos é possível um utente realizar uma verificação incompleta, mas válida, de uma cadeia de certificação?**

(a) Existe uma Entidade Certificadora (CA) intermédia confiável no caminho de certificação

(b) Não é de todo possível

(c)O certificado de todas as Entidade Certificadoras (CA) intermédias ainda não expirou

(d) A data do certificado é válida

SIO-Autenticação

**1. Relativamente à autenticação com desafio e resposta:**

a. Não permite uma fácil implementação do protocolo de autenticação mútua.

b. Não pode ser utilizada em combinação com smart-cards.

c. Pode ser utilizada em autenticações unidirecionais.

d. É fundamental que os desafios apresentados a uma mesma credencial nunca se repitam.

**2. Relativamente à autenticação por apresentação de senha direta memorizável:**

a. O sal serve para aumentar a dimensão das senhas.

b. É vulnerável a ataques por dicionário.

c. Os utentes memorizam senhas complexas com facilidade.

d. Se o administrador definir a necessidade de senhas de 256 bits aleatórias, o processo torna-se seguro.

**3. Relativamente à autenticação biométrica de utentes:**

a. Facilita a transferência de credenciais entre utentes.

b. É um método de autenticação ideal quando se tem muitos utentes.

c. É um método de autenticação universal (não exclui pessoas).

d. Pode dar origem a falsos negativos, mas estes não são perigosos

**4. Relativamente à autenticação usando TLS (Transport Layer Security):**

a. Não protege a integridade da informação.

b. Está bem adaptada para a autenticação de servidores dos quais nada se conhece (exceto o endereço IP, ou nome DNS).

c. O cliente pode escolher livremente quais as credenciais que usa na sua autenticação.

d. É vulnerável a ataques por dicionário.

**5. Relativamente à autenticação no SSH (Secure Shell):**

a. Usa sempre segredos partilhados entre utentes e servidor.

b. Usa sempre pares de chaves assimétricas não certificadas para autenticar o servidor.

c. Está bem adaptada para a autenticação de servidores dos quais nada se conhece (exceto o endereço IP, ou nome DNS).

d. É da responsabilidade do servidor SSH forçar a utilização de segredos complexos

**6. Relativamente à autenticação usando TLS (Transport Layer Security):**

a. Não protege a integridade da informação.

b. Serve para garantir a negociação de uma chave de sessão entre os interlocutores corretos.

c. O cliente pode escolher livremente quais as credenciais que usa na sua autenticação.

d. A autenticação dos clientes é uma opção dos mesmos.

**7. Relativamente à autenticação de utentes com desafio resposta e pares de chaves assimétricas:**

a. Quem se autentica deve cifrar a resposta com a chave pública do autenticador.

b. Quem se autentica deve apresentar a sua chave privada.

c. A utilização de certificados de chave pública pode fornecer os mecanismos de identificação de quem se autentica.

d. A validação das credenciais obriga à pré-partilha da chave pública do autenticador.

SIO-Armazenamento

**1. Qual dos seguintes sistemas tem o menor desperdício de espaço de armazenamento?**

a. RAID 1.

b. RAID 0+1

c. RAID 6.

d. RAID 5.

**2. Num sistema RAID 6 com N discos, qual a situação limite, após o qual existirá perda de informação?**

a. Avaria de 2 discos (qualquer)

b. Avaria de todos os N discos.

c. Avaria de 5 discos.

d. Avaria de 4 discos

**3. Num sistema RAID 1 com N discos, qual a situação limite, após o qual existirá perda de informação?**

a. Avaria de N-1 discos.

b. Avaria de apenas um disco (qualquer).

c. Avaria de 3 discos.

d. Avaria de 2 discos.

**4. Num sistema RAID 0 com N discos, qual a situação limite, após o qual existirá perda de informação?**

a. A avaria de qualquer disco implica sempre a perda de informação.

b. Avaria de todos os N discos.

c. Avaria de ambos os discos com as somas de controlo (paridade).

d. Avaria de N-1 discos.

**5. Em relação às cópias de segurança ao nível do sistema de ficheiros, que afirmação é correta?**

a. Permitem utilizar mecanismos de duplicação de blocos.

b. Garantem integridade do estado de cada ficheiro.

c. Não garantem integridade do estado global dos ficheiros.

d. Não garantem integridade do estado de cada ficheiro.

**6. Relativamente ao método dos backups incrementais do sistema de ficheiros, qual das afirmações é verdadeira?**

a. A adição de novos dados é feita considerando o último backup completo.

b. A longo prazo, o carácter incremental deste método irá resultar na utilização de mais espaço do que backups completos.

c. A recuperação de dados é mais complexa que em outros métodos.

d. Permite salvaguardar versões incrementais e globalmente consistentes de bases de dados.

**7. Num sistema RAID 4 com N discos, qual a situação limite, após o qual existirá perda de informação?**

a. Avaria de todos os N discos.

b. Avaria do disco que contém as somas de controlo e um outro qualquer.

c. Avaria de qualquer disco, excepto o que contém as somas de controlo (paridade).

d. Avaria de 1 disco (qualquer).

**8. Qual dos seguintes sistemas tem o menor desperdício de espaço de armazenamento?**

a. RAID 6

b. RAID 0

c. RAID 1

d. RAID 0+1

**9. Qual é o principal problema com os dispositivos de armazenamento?**

A. Acesso mecânico lento

B. Falta de espaço

C. Falha dos dispositivos

D. Ataques informáticos

**10. Quais são as principais soluções para minimizar a perda de dados?**

A. Cópias de segurança e armazenamento redundante

B. Armazenamento em nuvem

C. Encryption

D. Todas as opções acima

**11. Qual é o tipo de backup que permite recuperar arquivos para versões anteriores?**

A. Backup completo

B. Backup incremental

C. Backup diferencial

D. Todos os tipos de backup

**12. Qual é o tipo de backup que é mais eficiente em termos de espaço?**

A. Backup completo

B. Backup incremental

C. Backup diferencial

D. Todos os tipos de backup

**13. Quais são os benefícios da compressão em backups?**

A. Redução do espaço usado

B. Cópias seletivas da informação

C. Deduplicação

D. Todas as opções acima

**14. Qual é a função principal dos backups?**

A. Armazenar dados em um disco adicional

B. Realizar, manter e recuperar cópias de informação

C. Aumentar a velocidade de acesso aos dados

D. Proteger os dados contra incêndios e roubos

**15. Qual é a diferença entre backup completo e incremental?**

A. O backup completo é uma imagem completa dos dados enquanto o

incremental é apenas as diferenças desde o último backup

B. O backup completo é uma imagem completa dos dados enquanto o

incremental é apenas as diferenças desde o último backup completo

C. O backup completo é uma imagem completa dos dados enquanto o

incremental é apenas as diferenças desde o último backup incremental

D. Não há diferença entre backup completo e incremental

**15. Qual é a vantagem de usar algoritmos de compressão sem perdas nos backups?**

A. Aumenta a velocidade de acesso aos dados

B. Reduz o espaço de armazenamento necessário para os backups

C. Permite recuperação mais rápida dos dados

D. Permite cópias seletivas da informação.

**16. O que é a deduplicação no contexto de backups?**

A. Armazenar apenas cópias totais dos dados

B. Armazenar apenas cópias diferenciais dos dados

C. Armazenar apenas ficheiros/blocos únicos

D. Armazenar apenas cópias seletivas da informação

**17. Qual é o objetivo de se usar níveis de backup?**

A. Aumentar a velocidade de acesso aos dados

B. Permitir recuperação mais rápida dos dados

C. Organizar e priorizar a recuperação dos dados

D. Armazenar apenas cópias seletivas da informação

**18. Em que consiste a realização de backups locais?**

A. Armazenar cópias de segurança dos dados em dispositivos de

armazenamento no mesmo local do sistema original

B. Armazenar cópias de segurança dos dados em dispositivos de

armazenamento remotos através da nuvem

C. Armazenar cópias de segurança dos dados em dispositivos de

armazenamento off-site

D. Armazenar cópias de segurança dos dados em dispositivos de

armazenamento externos conectados ao sistema original

**19. O que é o RAID e como ele pode ser usado para aumentar a segurança de armazenamento de dados?**

A. RAID (Redundant Array of Inexpensive Disks) é um conjunto de técnicas que

permitem armazenar os dados em múltiplos discos de forma a reduzir o risco de perda

de dados.

B. RAID (Redundant Array of Inexpensive Disks) é um conjunto de técnicas que

permitem armazenar os dados em múltiplos discos de forma a aumentar a velocidade

de acesso aos dados.

C. RAID (Redundant Array of Independent Disks) é um conjunto de técnicas que

permitem armazenar os dados em múltiplos discos de forma a aumentar a capacidade

de armazenamento.

D. RAID (Redundant Array of Independent Disks) é um conjunto de técnicas que

permitem armazenar os dados em múltiplos discos de forma a aumentar a segurança

de armazenamento de dados.

**20. Em que consiste a técnica RAID 0?**

A. Striping para acelerar o acesso à informação em disco

B. Armazenamento de dados em N-1 discos

C. Duplicação da informação (mirroring)

D. Armazenamento de paridade num disco

**21. Qual é a desvantagem de usar o RAID 0?**

A. Aumenta a velocidade de acesso aos dados

B. Aumento da probabilidade de perda de informação

C. Redução do número de dispositivos

D. Aumento do desperdício da capacidade de armazenamento

**22. Em que consiste a técnica RAID 1?**

A. Striping para acelerar o acesso à informação em disco

B. Armazenamento de dados em N-1 discos

C. Duplicação da informação (mirroring)

D. Armazenamento de paridade num disco

**23. Qual é a desvantagem de usar o RAID 1?**

A. Aumento da probabilidade de perda de informação

B. Aumento do número de dispositivos

C. Redução do número de dispositivos

D. Desperdício da capacidade de armazenamento

**18. Em que consiste a técnica RAID 0+1?**

A. Um nível RAID 0 de volumes em RAID 1

B. Armazenamento de dados em N-1 discos

C. Striping para acelerar o acesso à informação em disco

D. Armazenamento de paridade num disco

SIO-Segurança 802.11 internet e redes

**1. A segunda fase do 802.1X destina-se a:**

a. Autenticar mutuamente o Suplicante e o Servidor de Autenticação.

b. Autenticar apenas o Servidor de Autenticação.

c. Autenticar mutuamente o Autenticador e o Servidor de Autenticação.

d. Autenticar apenas o Suplicante.

**2. A proteção de tráfego Wi-Fi no meio sem fios com WEP permite qual das seguintes funcionalidades?**

a. Controlo de integridade do cabeçalho e da carga útil com CBC-MAC e

AES.

b. Controlo de integridade do cabeçalho e da carga útil com Michael.

c. Cifra da carga útil com o algoritmo RC4.

d. Cifra de carga útil com o algoritmo AES.

**4. A autenticação WPA no acesso a um terminal móvel à rede:**

a. Depende sempre de um serviço central de autenticação.

b. Mantém a autenticação SKA do WEP mas evita a sua insegurança.

c. Segue os princípios do padrão 802.1X.

d. Elimina apenas o modo OSA do WEP.

**5. O EAP (Extensible Authentication Protocol):**

a. É um protocolo de autenticação baseado em chaves assimétricas.

b. É usado no 802.1X para autenticar um Suplicante perante um Autenticador.

c. É um protocolo que permite entender outros protocolos de autenticação.

d. É usado no 802.1X para autenticar um Suplicante perante um Servidor de Autenticação.

**6. A proteção do tráfego Wi-Fi por meio sem fios com TKIP permite qual das seguintes funcionalidades?**

a. Controlo de integridade do cabeçalho e da carga útil com Michael.

b. Controlo de integridade do cabeçalho e da carga útil com CRC-32.

c. Controlo de integridade do cabeçalho e da carga útil com CBC-MAC e AES.

d. Controlo de integridade da carga útil com CBC-MAC e AES.

**7. A autenticação do WPA no acesso a um terminal móvel à rede:**

a. Depende sempre de um serviço central de autenticação.

b. Mantém a autenticação SKA do WEP mas evita a sua insegurança.

c. Usa sempre EAP.

d. Realiza sempre uma distribuição de chaves ao Suplicante e ao Autenticador.

**8. A proteção do tráfego Wi-Fi no meio sem fios com WEP permite qual das seguintes funcionalidades:**

a. Controlo de integridade da carga útil com CBC-MAC e AES.

b. Controlo de integridade do cabeçalho e da carga útil com CBC-MAC e

AES.

c. Controlo de integridade da carga útil com Michael.

d. Controlo de integridade da carga útil com CRC-32.

**9. A autenticação do WPA no acesso de um terminal móvel à rede:**

a. Usa sempre EAP

b. Permite a utilização de SKA para sistemas mais antigos.

c. Elimina apenas o modo OSA do WEP.

d. Permite o modelo SOHO para redes de pequenas dimensão.

**10. A fase four-way Handshake do 802.1X destina-se:**

a. Autenticar mutuamente o Suplicante e o Servidor de Autenticação.

b. Distribuir chaves criptográficas entre o Suplicante e o Servidor de Autenticação.

c. Distribuir chaves criptográficas entre o Autenticador e o Servidor de Autenticação.

d. Autenticar mutuamente o Suplicante e o Autenticador.