Sistemas Distribuídos, 2016/17 - 1º MINI Teste

Todas as perguntas têm a mesma cotação. Escolha apenas uma resposta em cada alínea.
Cada resposta de escolha múltipla errada desconta 1/4 da sua cotação.
No caso de encontrar mais do que uma resposta certa, escolha a que faz a afirmação mais forte.

Número: _____ Nome:_____

1) Considere o nome (PROGRAM, VERSION) que identifica uma interface remota em SUN RPC. Qual a autoridade associada?
   A) O servidor RPCBIND da máquina onde o servidor RPC está alojado.
   B) A autoridade do domínio DNS ao qual pertence o servidor RPC.
   C) O run-time library do SUN RPC.
   D) O gestor da rede local.

2) Numa dada máquina, existe um servidor SUN RPC identificado pelo par (1898, 1) e um objeto remoto Java RMI identificado por "rmi://rmi.tecnico.pt/objsd". Compare ambos os nomes:
   A) Ambos são globais.
   B) Ambos são relativos.
   C) O primeiro é global, o segundo é relativo.
   D) O primeiro é relativo, o segundo é global.

3) Nomes hierárquicos:
   A) Permitem assegurar unicidade referencial mais facilmente em redes de grande escala.
   B) São necessariamente homogéneos.
   C) São necessariamente de âmbito global.
   D) Todas as anteriores.

4) Considere um documento em formato TXT com dimensão 2Kbyte. Este documento foi cifrado com o algoritmo AES de 128 bits em modo CBC.
   A) Um atacante pode trocar blocos cifrados de posição dentro do documento cifrado.
   B) Um atacante pode remover blocos arbitrários sem deteção.
   C) Para decifrar o documento é necessário um valor designado por IV.
   D) A e B

5) Qual a principal desvantagem da cifra simétrica que torna atrativa a cifra híbrida?
   A) Mau desempenho da cifra simétrica.
   B) Dificuldade de distribuição de chaves públicas.
   C) Dificuldade de distribuição de chaves secretas.
   D) Chaves de grande dimensão.

6) Com a cifra assimétrica RSA é possível:
   A) Cifrar com a chave pública, decifrar com a chave privada.
   B) Cifrar com a chave privada, decifrar com a chave pública.
   C) Combinar com função de resumo para construir assinaturas digitais.
   D) Todas as anteriores.

7) Um certificado digital de chave pública confiável deve conter, pelo menos:
   A) A chave pública da entidade.
   B) A chave pública e o nome da entidade certificada.
   C) O par de chaves da entidade certificada.
   D) A chave pública, o nome da entidade certificada e a assinatura de uma autoridade de certificação.

8) Considere uma entidade A cujo par de chaves de cifra assimétrica foi criado pela entidade certificadora CA. Verificou-se que a entidade não é confiável e lhe deveria ser inibido o uso do certificado.
   A) A CA invalida o certificado e deixa de responder a pedidos do certificado de A
   B) A CA muda a sua chave pública para que o certificado deixe de ser válido
   C) O certificado da entidade A deve ser acrescentado à blacklist (lista negra) da CA
   D) A CA informa os detentores de certificados que já não são válidos

9) Considere um problema de distribuição de chave num sistema que usa cifra simétrica
   A) O problema só pode ser resolvido usando cifra híbrida
   B) O Kerberos é um sistema de autenticação com cifra simétrica, mas obriga a usar cifra híbrida para partilhar a chave
   C) Mesmo com cifra híbrida tem de existir um modo de transmissão da chave simétrica off-line para o sistema ser seguro
   D) O Kerberos permite de forma segura partilhar uma chave simétrica entre entidades previamente registadas

10) $\{X\}_Y$ $\{M\}_Z$

Suponha que a Alice (A) quer enviar uma mensagem M ao Bob (B) de forma confidencial, num sistema de cifra híbrida. Escolha as chaves que deveriam ser usadas na expressão acima, de entre as diversas opções:

   A) $X= K_{A,B}$; $Y= K_{PB}$; $Z= K_{A,B}$
   B) $X= K_{A,B}$; $Y= K_{PB}$; $Z= K_{PB}$
   C) $X= K_{A,B}$; $Y= K_{PA}$; $Z= K_{A,B}$
   D) $X= K_{PB}$; $Y= K_{PA}$; $Z= K_{A,B}$

1	2	3	4	5	6	7	8	9	10	**Total**
2	2	2	2	2	2	2	2	2	2	**20**