Sistemas Distribuídos, 2018/19
3º MINI Teste

- Todas as perguntas têm a mesma cotação. Cada pergunta tem apenas uma resposta completamente certa.
- Na sua resposta pode selecionar uma ou mais alíneas. Preencha-as por ordem crescente, com vírgulas.
- Para cada pergunta, a nota é calculada pelas alíneas que escolheu na sua resposta, da seguinte forma: a alínea correta conta com a cotação completa; cada alínea incorreta desconta 1/3 da cotação da pergunta.
- Exemplo: numa dada pergunta, escolheu as alíneas "A, D". Se a alínea certa for a A, então a nota final será 2/3 da cotação (cotação completa pela alínea certa menos 1/3 pela alínea incorreta).

Número: _____ Nome: _____

1) Considere os conceitos de política e mecanismo de segurança:
   A. Os mecanismos de segurança fazem sentido em sistemas centralizados, as políticas de segurança em sistemas distribuídos.
   B. As políticas de segurança servem apenas para documentar os mecanismos de segurança.
   C. Os mecanismos de segurança definem a política de segurança.
   D. As políticas de segurança podem ser asseguradas por uma utilização adequada de mecanismos de segurança.

   [ ]

2) Qual é a diferença entre o SHA-256 e o SHA-512 ?
   A. Necessitam de memória RAM em diferentes quantidades, 256 e 512 Mbyte, respetivamente.
   B. Produzem resumos de tamanhos diferentes, 256 e 512 bits, respetivamente.
   C. Usam chaves de tamanho diferente, 256 e 512 bits, respetivamente.
   D. Usam tamanhos de bloco de cifra diferentes, 256 e 512 bits, respetivamente.

   [ ]

3) Assuma que a rede de serviços do IST usa o Kerberos como sistema de autenticação. Quando um departamento decide instalar uma nova fotocopiadora na rede, para que esta possa ser devidamente usada pelos utilizadores registados no sistema Kerberos, é necessário definir uma nova chave. Qual é essa chave?
   A. A chave Ktgs
   B. A chave Kc,s
   C. A chave Ks
   D. A chave Kc

   [ ]

4) Um servidor de ficheiros protegido por Kerberos (versão simplificada apresentada nas aulas teóricas) recebe um pedido juntamente com um *ticket*. O *ticket* permite ao servidor:
   A. Verificar que a sua hora atual está sincronizada com o Saut.
   B. Receber chave de sessão gerada pelo Saut
   C. Receber chave de sessão gerada pelo cliente.
   D. A e B.

   [ ]

5) 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.

   [ ]

6) Considere a cifra de blocos AES-128. O modo CBC permite:
   A. Esconder os padrões dos blocos cifrados.
   B. Aumentar a velocidade de cifra.
   C. Tornar mais difícil o ataque força-bruta à chave.
   D. Ter blocos de tamanho variável.

7) O Bob recebeu uma mensagem M da Alice, à qual vinha anexada uma assinatura digital de chave pública. Para validar a assinatura, o Bob deve:
   A. Decifrar M com a chave privada do Bob, gerar o resumo do resultado e ver se é igual à assinatura digital.
   B. Decifrar a assinatura digital usando a chave pública da Alice, gerar o resumo de M, e comparar se ambos os resultados são iguais.
   C. Gerar o resumo de M e ver se é igual à assinatura digital.
   D. Gerar o resumo de M, cifrá-lo com a chave pública da Alice e ver se é igual à assinatura digital.

8) A chave privada de um *web site* foi roubada! O que fazer?
   A. É necessário comunicar à CA o sucedido para que ela possam informar diretamente todos os clientes do *site*.
   B. É necessário comunicar à Apple, Google e Microsoft para que possam atualizar os seus sistemas operativos.
   C. É necessário comunicar a todos os clientes do site por e-mail.
   D. É necessário comunicar à CA o sucedido para que ela possam revogar o certificado e o adicionem à CRL.

9) Para que um utilizador Artur possa usar a chave contida num certificado digital de chave pública, qual das seguintes condições é verdadeira?
   A. O certificado foi descarregado por Artur a partir de um site web acessível por HTTPS.
   B. Emitido com o campo “To:” preenchido com “Artur”
   C. Emitido por uma autoridade de certificação de quem Artur conhece/consegue obter a chave privada.
   D. Emitido por uma autoridade de certificação de quem Artur conhece/consegue obter a chave pública.

D B C B D A B D D