

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) Relativamente à Base Computacional de Confiança (TCB) de um sistema informático:
- A. A TCB não tem defeitos de programação (bugs).
 - B. A TCB deve conter o conjunto mínimo de mecanismos que permitem implementar políticas de segurança.
 - C. A TCB deve englobar a maior parte do sistema.
 - D. A TCB identifica os utilizadores reconhecidos no sistema.
-
- 2) Qual é a diferença entre o AES-128 e o AES-256 ?
- A. Usam chaves de tamanho diferente, 128 e 256 bits, respetivamente.
 - B. Produzem resumos de tamanhos diferentes, 128 e 256 bits, respetivamente.
 - C. Usam tamanhos de bloco de cifra diferentes, 128 e 256 bits, respetivamente.
 - D. Necessitam de memória RAM em diferentes quantidades, 128 e 256 Mbyte, respetivamente.
-
- 3) Uma cifra simétrica contínua com chave baseada num gerador de números pseudo-aleatórios:
- A. É segura desde que os dados nunca repitam a mesma sequência binária.
 - B. É segura desde que o tamanho dos dados a cifrar seja muito menor do que o tamanho da sequência gerada pela chave.
 - C. É segura desde que os dados tenham um tamanho múltiplo do tamanho do bloco.
 - D. É insegura.
-
- 4) Considere um servidor de impressão (*Print server*) protegido por Kerberos. Ao receber um pedido de impressão de um documento, o servidor recebe também um ticket. O servidor deve então:
- A. Decifrar o ticket com a sua chave secreta de servidor.
 - B. Validar se o ticket está dentro do seu período de validade.
 - C. Validar que o número aleatório (*nonce*) contido no ticket nunca foi visto antes.
 - D. A e B
-
- 5) Ao ingressar no IST, um novo estudante recebe uma nova senha de utilizador para usar os serviços distribuídos do campus. Assumindo que o sistema de autenticação usa Kerberos, essa senha determina:
- A. A chave Kc
 - B. A chave Kc,s
 - C. A chave Ks
 - D. A chave Ktgs
-

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

- 7) O certificado digital de chave pública de Alice foi emitido pela autoridade de certificação Charlie e recebido pelo cliente Bob. A assinatura digital contida no certificado foi emitida por quem?
- A. Alice
 - B. Bob
 - C. Charlie
 - D. Nenhuma das anteriores.

- 8) A revogação de certificados digitais de chave pública:
- A. É eficaz porque usa o algoritmo RSA.
 - B. É eficaz porque a CA pode revogar instantaneamente o certificado e notificar todos os clientes.
 - C. Não é eficaz porque é necessário um cálculo complexo envolvendo a chave privada do utilizador.
 - D. Não é eficaz porque usa listas de distribuição (CRL) que podem demorar muito a ser divulgadas.

- 9) Considere a seguinte mensagem SOAP enviada para um Web Service:
- ```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" >
<S:Header /><S:Body><n2:sayHello
xmlns:n2="http://ws.org/"><arg0>friend</arg0></n2:sayHello></S:Body></S:Envelope>
```

O que deve adicionar para proteger apenas a autenticidade e integridade da mensagem?

- A. Cabeçalho com resumo dos cabeçalhos da mensagem cifrado com chave privada do emissor.
- B. Cabeçalho com resumo do corpo da mensagem cifrado com chave privada do emissor.
- C. Cabeçalho com cifra total do corpo com a chave privada do emissor.
- D. Cabeçalho com certificado digital do emissor.