Sistemas Distribuídos, 2014/2015
1º MINI Teste – 8 de Maio de 2015

Todas as perguntas têm a mesma cotação. Escolha apenas uma resposta em cada alínea.
Cada resposta de escolha múltipla errada desconta 1/3 da sua cotação.
No caso de encontrar mais do que uma resposta certa, escolha a que faz a afirmação mais forte.

Número: _____ Nome:_____

1) O DES é um dos primeiros algoritmos de cifra normalizados.
   a. A chave inicial era de 128 bits, desdobrada em chaves de 48 bits para cada etapa.
   b. Usa um algoritmo para cifrar e outro diferente para decifrar, ambos aplicando funções de permutação e substituição a cada bloco.
   c. O triple DES é a versão actualmente mais usada, com uma chave de 168 bits, o que o torna atualmente praticamente seguro.
   d. Apenas pode ser realizado em *hardware*.

2) Assuma que a Alice e o Bob queriam dialogar de forma segura usando cifra simétrica, para tal o segundo gerava uma chave secreta. A distribuição da chave secreta para a Alice teria de ser feita assegurando quais requisitos?
   a. Apenas confidencialidade da chave secreta.
   b. Apenas autenticidade e Integridade da chave secreta
   c. Autenticidade, Integridade e Confidencialidade da chave secreta.
   d. Nenhum dos anteriores.

3) Comparando o protocolo Kerberos analisado nas teóricas e o Needham-Schroeder, qual das seguintes é verdadeira?
   a) No Kerberos, o Saut conhece as chaves secretas dos utilizadores; no Needham-Schroeder, o Saut não conhece qualquer segredo dos utilizadores.
   b) O Kerberos baseia-se exclusivamente em cifra assimétrica, enquanto que o Needham-Schroeder é em simétrica.
   c) O objetivo do Kerberos é entregar a chave de longa duração do cliente ao serviço, enquanto que o Needham-Schroeder distribui uma chave de sessão.
   d) O Kerberos assume relógios sincronizados, enquanto que o Needham-Schroeder não.

4) Usando Kerberos, um cliente obteve um ticket para sessão com o serviço S. O cliente C pretende agora enviar um pedido confidencial a S. Para tal, a mensagem de invocação deve incluir:
   a) {pedido}Kcs
   b) {pedido}Ks
   c) {pedido}Kc
   d) {pedido}Ksaut

5) Considere no sistema de replicação passiva do tipo primary-backup, a situação em que o primário teve uma falta de paragem mas o servidor secundário ainda não a detectou
   a) Pode dizer-se que houve uma falta mas o sistema não falhou
   b) O sistema falhou porque não há nenhum servidor disponível durante o tempo de substituição
   c) A situação não é possível porque o secundário responde sempre ao cliente
   d) O FE do cliente detecta que o primário falhou e produz uma excepção interrompendo a chamada remota

6) Considere o protocolo de primary backup. O que pode ser uma falta arbitrária (ou bizantina)?
   a) O primário actualiza o estado e não envia a mensagem ao secundário.
   b) O tempo de propagação do I´m alive excede o valor de P.
   c) O cliente contacta o secundário e este executa a operação pedida.
   d) Todas as acima.

7) Usando o protocolo Quorum Consensus, um sistema com 3 réplicas, quóruns de maioria, pesos uniformes, tem o seguinte estado nas réplicas: R1 <val=8, <seq=4, pid=1>>, R2 <val=6, <seq=2, pid=1>>, R2 <val=10, <seq=3, pid=2>>,
   Neste instante, um cliente inicia um pedido de leitura. Que valor(es) pode a leitura devolver?
   a) Devolve garantidamente 8.
   b) Devolve garantidamente 6.
   c) Pode devolver 8 ou 10, dependendo das respostas recebidas.
   d) Pode devolver 6, 8 ou 10, dependendo das respostas recebidas.

8) Considere um protocolo de quórum a operar sobre um sistema assíncrono. Assuma que se usam quóruns de maioria. Qual a frase ERRADA?
   a) Com o grau de replicação 2*f+1 o protocolo tolera faltas bizantinas.
   b) O protocolo é correcto mesmo se a rede atrasar indefinidamente as mensagens.
   c) Quanto todas as escritas invocadas terminaram, nem todas as réplicas estão necessariamente consistentes, uma maioria tem o estado correcto.
   d) O grau de replicação considerando f faltas de paragem é de 2*f+1 replicas.