Sistemas Distribuídos, 2014/2015
2º MINI Teste – 29 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) A Alice pretende assinar um documento que vai ser guardado na *nuvem* e precisa de garantir os seguintes requisitos: integridade, autenticação e não repúdio. Indique a solução apropriada:
   a) Usa um MAC para assinar.
   b) Usa uma função de resumo e depois cifra o resultado com cifra assimétrica com a sua chave privada.
   c) Usa uma função de resumo e depois cifra o resultado com cifra simétrica com uma chave que mantém secreta.
   d) Usa uma função de resumo e depois cifra o resultado com cifra assimétrica com a sua chave pública.

   [ ]

2) O Bob recebeu um certificado com a chave pública da Alice emitido pela CA "TrueCA", cuja chave pública não era conhecida do Bob. Por essa razão, o Bob obteve a chave pública da "TrueCA" por canal inseguro a partir de uma fonte não certificada. Qual dos ataques seguintes é possível?
   a) *Man-in-the middle* em que um atacante substitui a chave pública no certificado pela chave pública do atacante.
   b) *Replay attack* em que um atacante tenta reutilizar o certificado depois do seu prazo de validade expirar.
   c) Ataque *man-in-the middle* ao momento em que a chave pública da TrueCA é entregue ao Bob.
   d) Nenhuma das anteriores.

   [ ]

3) Compare a distribuição de chaves entre cifra simétrica e assimétrica:
   a) É mais fácil distribuir uma chave simétrica que uma chave pública pois não precisamos de garantir integridade nem autenticidade para distribuir a primeira.
   b) É mais fácil distribuir uma chave simétrica que uma chave pública pois não precisamos de garantir confidencialidade para distribuir a primeira.
   c) É mais fácil distribuir uma chave pública que uma chave simétrica pois não precisamos de garantir integridade nem autenticidade para distribuir a primeira.
   d) É mais fácil distribuir uma chave pública que uma chave simétrica pois não precisamos de garantir confidencialidade para distribuir a primeira.

   [ ]

4) O 2-phase commit baseia-se no uso de *timeouts*.
   a) Consequentemente, o protocolo só pode ser usado em sistemas síncronos.
   b) Consequentemente, o protocolo exige relógios sincronizados.
   c) Apesar de usar *timeouts*, o protocolo pode ser usado em sistemas assíncronos.
   d) Nenhuma das anteriores.

   [ ]

5) Em 2-phase commit, o participante votou "sim".
   a) Pode confirmar imediatamente a sua transação local.
   b) Tem de esperar pela decisão do coordenador.
   c) Um participante nunca vota "sim".
   d) Espera um *timeout* e depois confirma a transação local.

   [ ]

6) No 2PC, qual das seguintes situações não pode levar um participante a votar NÃO?
   a) Conflito entre acessos da transação em causa com acessos de outra transação concorrente.
   b) Falha de algum componente do participante, e.g. falha temporária no acesso à BD local, quando o participante está ainda no estado Inicial.
   c) Participante já ter decidido abortar unilateralmente, devido a atraso na receção da mensagem PREPARAR.
   d) Todas as anteriores.

7) Nomes de grande amplitude referencial gerados aleatoriamente:
   a) Permitem assegurar unicidade referencial mais facilmente em redes de grande escala.
   b) O seu espaço de nomes é várias vezes maior que a dimensão do espaço de objectos referenciados.
   c) São números aleatórios de grande dimensão e não necessitam de ser definidos por uma autoridade
   d) Todas as anteriores.

8) Porque é que os nomes puros são mais difíceis de usar?
   a) Porque não são hierárquicos
   b) Porque não tendo informação de localização não permite orientar o algoritmo de resolução
   c) Porque são mais difíceis de criar
   a) Porque são normalmente binários e não podem ser usados em XML