

## LETI/LEIC 2016/17, Repescagem do 2º Teste de Sistemas Distribuídos 4 de julho de 2017

Responda no enunciado, usando apenas o espaço fornecido. Identifique todas as folhas.  
Uma resposta errada numa escolha múltipla com N opções desconta  $1/(N-1)$  do valor da pergunta.  
Duração da prova: 1h30m

### Grupo I [8 valores]

- 1) Considere que quer criar um canal seguro entre a Alice e o Bob com cifra híbrida. O envio de uma mensagem M neste canal é feito de acordo com o esquema abaixo.

$$\{K_1\}_{K_2} \quad \{M\}_{K_3} \quad \{\text{Hash}(M)\}_{K_4}$$

em que  $K_1, K_2, K_3$  e  $K_4$  são genéricos.

- a) [0,5] Para o sistema ser eficaz, qual deverá ser o tipo de cifra aplicado à mensagem M? Justifique.


- b) [0,9] Escolha para a cifra de M um protocolo de cifra e uma dimensão de chave que cumpra os seguintes requisitos:

- Eficaz no tempo de cifra/ decifra
- Praticamente seguro para a tecnologia atual
- Dificulta deteção de blocos no texto cifrado

Protocolo:

Sugestão de Chave:

Modo de cifra:

- c) [0,8] Das chaves genéricas referenciadas por  $K_1$  a  $K_4$ , indique quais são iguais e justifique.


- d) Que componente do protocolo garante cada propriedade seguinte?

Copie a parte relevante do esquema de 1) para o retângulo:

- i. [0,6] Autenticação.

Justifique.


ii. [0,6] Confidencialidade.   
Justifique.


e) [0,6] A função de Hash:

- i. Garante a ofuscação do conteúdo da mensagem.
- ii. Reduz a dimensão da mensagem tornando mais rápida a cifra.
- iii. Reduz a dimensão da mensagem para otimizar a transmissão.
- iv. Garante só por si a integridade.

f) [0,6] Que elemento deveria adicionar para robustecer o protocolo eliminando um possível ataque de *man-in-the-middle* no envio desta mensagem?

- i. Um certificado da chave  $K_4$
- ii. Um certificado da chave  $K_2$
- iii. Um certificado da chave  $K_3$
- iv. Todas as chaves deveriam ter certificados

2) No Kerberos v5, considere a seguinte interação entre um cliente C e um servidor S:

$$Aut_{c,s} \quad Ticket_{c,s} \quad \{Pedido\} \quad K_{c,s}, n_3$$

a) [0,6] Quais as chaves de cifra usadas em Aut e Ticket?

Identifique na forma habitual  $K_x$  ou  $K_{x,y}$  indicando sempre o X e o Y concretos.

Aut  Ticket

b) [0,6] Quem conhece essas chaves? Justifique claramente.


c) [0,8] Explique deterministicamente porque razão o servidor S acredita que está a interagir com o cliente C.


d) O servidor Kerberos foi alvo de um *replay attack* na mensagem apresentada em 2).

i) [0,4] Em que consiste um *replay attack*? Seja claro na sua explicação.

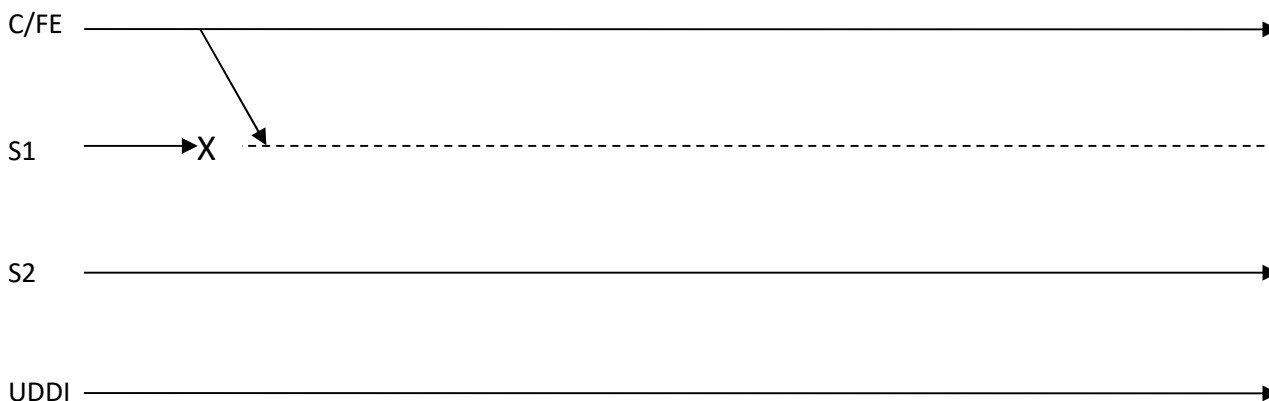

ii) [0,5] Que elemento do protocolo é suposto impedir *replay attack*? Justifique.


iii) [0,5] Como poderia então o ataque concretizar-se, tendo em atenção a resposta dada em ii) ?


### Grupo II [7 valores]

1) Considere um sistema replicado usando o protocolo "*primary backup*" tal como foi estudado na disciplina. Assuma que a localização do servidor primário é mantida por um servidor UDDI.

a) [0,5] Complete a seguinte execução de um pedido de um cliente ao sistema replicado:



b) [0,7] Este sistema sempre recorreu a TCP/IP para a comunicação entre as suas componentes. Um dia mudou-se a implementação para usar UDP/IP. Apesar de ligeira melhoria no desempenho, observou-se que o servidor secundário passou a ter valores incoerentes com o primário. Proponha uma explicação para este caso.


c) De que forma é que os seguintes parâmetros afetam a disponibilidade do sistema?  
[Escolha múltipla: sublinhe a resposta correta]

i) [0,4] Tempo de resposta do servidor UDDI:

Maior valor aumenta a disponibilidade / Maior valor reduz a disponibilidade / Não tem impacto

ii) [0,4] Tempo máximo de propagação de mensagens na rede (tmax):

Maior valor aumenta a disponibilidade / Maior valor reduz a disponibilidade / Não tem impacto

iii) [0,4] Período de provas de vida (P):

Maior valor aumenta a disponibilidade / Maior valor reduz a disponibilidade / Não tem impacto

iv) [0,4] Fiabilidade do servidor primário:

Maior valor aumenta a disponibilidade / Maior valor reduz a disponibilidade / Não tem impacto

d) Neste sistema, uma mensagem de atualização enviada do primário para o secundário foi corrompida por um *router* danificado, tendo o secundário aceite a mensagem e atualizado a sua réplica com os dados inválidos. Nesta situação:

i) [0,5] Identifique a falta.

ii) [0,6] Identifique o erro e indique em que momento o erro passou de latente para efetivo.


iii) [0,5] Esta situação imprevista pode levar o sistema a manifestar uma falha bizantina?  
Justifique explicitando o que é uma falha bizantina.


2) Considere agora um sistema *quorum consensus* com 3 réplicas. Num dado momento, o estado das réplicas é o seguinte:

R1: valor = 10; tag = [seq-no=3; client-id=1]

R2: valor = 10; tag = [seq-no=3; client-id=1]

R3: valor = 0; tag = [seq-no=2; client-id=3]

a) [0,5] Se um cliente efetuar uma leitura enquanto o sistema se mantém neste estado, que valor será lido? Justifique.


b) No estado acima, a réplica 1 recebe uma mensagem “write(valor = 0; tag = [seq-no=2; client-id=3])”.

i) [0,6] Que sequência de acontecimentos levou a esta situação?


ii) [0,5] Qual é o estado da réplica após receber esta mensagem?


### Grupo III [3 valores]

A norma X/Open **XA** é uma especificação para transações distribuídas que descreve a interface disponibilizada pelos gestores de recurso local e que são invocadas pelo gestor da transação global. O XA usa o protocolo 2PC para assegurar que todos os participantes fazem COMMIT ou que todos fazem ROLLBACK.

A norma XA define as seguintes funções que podem ser chamadas remotamente:

Rotina do gestor de recurso (Participante)	Descrição da função
<code>xa_start</code>	Inicia uma nova transação local e associa-a ao identificador de transação distribuída (XID) fornecido como argumento ou associa o processo a uma transação em curso.
<code>xa_prepare</code>	Prepara a transação local associada ao XID fornecido como argumento.
<code>xa_rollback</code>	Cancela a transação local associada ao XID fornecido como argumento.
<code>xa_commit</code>	Confirma a transação local associada ao XID fornecido como argumento.
<code>xa_recover</code>	Obtém uma lista de transações locais já preparadas ou canceladas localmente.

1) [0,3] A que propriedade ACID se refere a afirmação sublinhada no texto?

--

2) [0,4] Tendo em conta a informação apresentada na tabela, a norma XA impõe o uso de controlo de concorrência pessimista ou otimista para garantir a propriedade de Isolamento? Ou deixa à escolha da implementação? Justifique.


- 3) Considere agora uma **aplicação interbancária** para realizar **transferências** entre bancos diferentes. Cada banco que participa no sistema disponibiliza uma implementação da interface remota XA definida na tabela. Existe um servidor que coordena transações distribuídas neste sistema.

O sistema está a ser usado para transferir EUR 100 de uma conta do banco A para uma conta no banco B.

- a) [0,5] Chegados à fase da votação, que invocações de rotinas XA deve o coordenador fazer ao banco A e B?

--

- b) [0,5] Qual a condição para o coordenador vir a optar por uma decisão COMMIT?


- c) [0,6] Considere agora que o banco B já respondeu a `xa_prepare()` e que o coordenador recebeu a resposta, mas que B entrou em falta temporária e não responde a novos pedidos. Indique as duas situações que podem resultar da resposta a `xa_prepare()`.

1
2

- d) [0,7] Escolha uma das duas situações anteriores e complete o estado do *log* do participante banco B no momento de iniciar a recuperação da falta temporária.

Situação: 1 / 2 (assinalar a situação escolhida)

*Log*: (preencha da esquerda para a direita, linha a linha, usando apenas as entradas necessárias)

Join DTx 12521 Estado: inicial			

## Grupo IV [3 valores]

Cada *smartphone* de uma conhecida marca com nome de fruta tem um *Unique Device Identifier* (UDID), que é uma sequência de 40 letras e números específicos ao dispositivo. É um número de série, que é atribuído de forma única mas não sequencial. O UDID é atribuído ao dispositivo na fábrica.

Exemplo de UDID: 2b2f0cc704d137be2e1730235f5664094b831186

1) Classifique o UDID quanto a:

a) [0,4] Âmbito global/local. Justifique.


b) [0,4] Homogeneidade. Justifique.


c) [0,4] Pureza. Justifique.


2) Numa versão mais recente do sistema operativo móvel, e para proteger a privacidade dos utilizadores, as aplicações móveis passaram a ser impedidas de aceder ao UDID. Em alternativa têm acesso ao IDFV: *IDentifier for (App) Vendor*. Estes identificadores são criados e geridos apenas pelo sistema operativo do *smartphone*.

Exemplo de IDFV: 599F9C0092DC4B5C94647971F01F8370

O valor de IDFV é o mesmo para aplicações do mesmo fornecedor de aplicações a correr no mesmo dispositivo. O identificador muda caso as aplicações do fornecedor sejam todas desinstaladas.

a) [0,3] Assinale as propriedades (uma ou mais) que mudam no IDFV comparando com o UDID:

<input type="checkbox"/>	Âmbito
<input type="checkbox"/>	Homogeneidade
<input type="checkbox"/>	Pureza

b) [0,5] Considere agora que o fornecedor de aplicações quer fazer uma *push notification*, isto é, pretende enviar uma mensagem para uma aplicação a correr no *smartphone*.

Pode usar um dos dois identificadores referidos (UDID ou IDFV) para endereçar o *smartphone*? Justifique.

Sim / Não

3) Assuma agora que o fornecedor da aplicação quer disponibilizar informação num servidor com o nome DNS **update.maca.pt**.

a) [0,5] Como seria resolvido este nome a partir de uma máquina ligada à Internet noutra domínio? Assuma que é a primeira vez que se acede e que as eventuais *caches* estão vazias. Descreva o processo, passo a passo, até se descobrir o endereço IP do servidor.


b) [0,2] O processo anterior é recursivo ou iterativo? Justifique.

Recursivo / Iterativo

c) [0,3] Das duas abordagens anteriores, qual é a que favorece mais o preenchimento das *caches* DNS? Justifique.

Recursivo / Iterativo