	Departamento de Informática **Faculdade de Ciências e Tecnologia** **UNIVERSIDADE NOVA DE LISBOA**

Licenciatura em Engenharia Informática
Sistemas Distribuídos I – Época de recurso, 22 de Julho de 2006
2º Semestre, 2005/2006

Exame sem consulta com a duração de 2h30min – 15 minutos de tolerância

Aluno nº _____Nome: _____

1. Supondo que pretende implementar um sistema que forneça transparência relativamente às falhas, qual das seguintes arquitecturas é mais adequada para o efeito: cliente/servidor; cliente/servidor particionado; cliente/servidor replicado. Justifique a sua resposta.

Cliente/servidor, porque / **Cliente/servidor particionado,** porque / **Cliente/servidor replicado,** porque

2. Seria apropriado implementar um sistema de comunicação multi-ponto funcional (anycast) usando um sistema de message-queuing? Explique como ou porque não.

Sim, porque... / **Não,** porque...

3. Assinale com **[V]erdadeiro** ou **[F]also** as seguintes afirmações. **As respostas erradas descontam.**

   a) ___ A criptografia simétrica não permite proteger sistemas contra ataques do tipo negação da prestação de serviço (*denial of service*) ;

   b) ___ É possível utilizar assinaturas digitais recorrendo, apenas, a uma função de síntese segura;

   c) ___ Na criptografia assimétrica é uma mera convenção qual das chaves do par é a pública e qual é a privada que deverá ser mantida secreta;

   d) ___ A criptografia simétrica é a base para a protecção das aplicações contra a adulteração de mensagens (*message tampering*) ;

   e) ___ A criptografia simétrica é significativamente mais rápida que a criptografia assimétrica, porém produz codificações significativamente maiores;

f) ___ Tratar a questão do não repúdio de mensagens enviadas pelo próprio é um dos aliciantes da utilização de criptografia assimétrica;

g) ___ As assinaturas digitais usam, normalmente, criptografia assimétrica, cifrando e decifrando com a chave privada;

h) ___ No estabelecimento de um canal seguro autenticado, a autenticidade dos principais é comprovada pela validação dos certificados trocados, altura em que se verifica que estes não estão expirados e que foram assinados por uma autoridade de certificação legítima.

i) ___ A utilização de criptografia assimétrica, combinada com certificados de chave pública, permite trocas seguras de mensagens entre dois principais sem nunca ser necessária a participação de terceiros, nomeadamente a comunicação com a entidade de certificação que emitiu os certificados.

j) ___ A utilização de criptografia assimétrica, combinada com certificados de chave pública, permite trocas de mensagens entre dois principais com um nível de segurança elevado que dispensam a participação de terceiros

k) ___ Uma forma segura de optimizar a codificação de um certificado consiste em substituir o nome da entidade certificadora pela sua chave pública. Pode-se assim validar mais rapidamente o certificado pois continua-se a usar criptografia forte.

4. No decurso do desenvolvimento de um sistema de caching, as questões relativas à Segurança levaram ao enunciado de 3 requisitos fundamentais, referentes às garantias oferecidas por tal sistema relativamente ao conteúdo da cache mantido em disco. Concretamente, estes requisitos traduzem-se na promessa de **privacidade**, **integridade** e **autenticidade** dos conteúdos dispensados. Ou seja, a solução pretendida deve impedir que elementos estranhos e exteriores ao sistema possam inspeccionar o conteúdo da *cache* em disco, por exemplo, por acesso directo ao sistema de ficheiros. Também deverá evitar dispensar aos clientes qualquer informação que tenha sido adulterada, seja por corrupção deliberada da cache ou por acidente. E, finalmente, deverá haver um comprovativo que a informação armazenada em cache que é dispensada aos clientes foi guardada pela entidade competente e, por essa via, que ela será autêntica e corresponde à informação original.

   Critique, justificando, cada uma das propostas seguintes para conteúdo da cache quanto à sua eficácia em garantir os 3 requisitos descritos anteriormente. Considere que a cache em disco é gerida por um servidor ***S***, possuidor de um certificado de chave pública $Cert_S$, associado ao par de chaves assimétricas K_{Spub} e K_{Spriv} e, ainda, que U_i é o ***URN*** (*Universal Resource Name*) que identifica univocamente cada elemento de informação guardado na cache e V_i é o seu valor. ***F(i)*** e ***C(i)*** denotam, respectivamente, o nome do ficheiro e o formato do conteúdo em cache para o elemento de informação U_i. *hex(v)* denota a representação hexadecimal de *v.*

   Risque a resposta que não interessar. Justifique.

a) ***F(i)*** = *hex(U_i)*; ***C(i)***=$\{K_s\}_{\boldsymbol{KSpub}}$, $\{\boldsymbol{V_i}\}_{Ks}$, Hash(***$V_i$***)

Privacidade: Garante / Não garante***, porque:***

Integridade: Garante / Não garante***, porque:***

Autenticidade: Garante / Não garante***, porque:***

b) ***F(i)*** = *hex(U_i)* ; ***C(i)***=$\{K_s\}_{\boldsymbol{KSpriv}}$, $\{V_i$, Hash(V_i + ***F(i)***) $\}_{Ks}$

Privacidade: Garante / Não garante***, porque:***

Integridade: Garante / Não garante***, porque:***

Autenticidade: Garante / Não garante***, porque:***

c) ***F(i)*** = *hex(U_i)* ; ***C(i)***=$\{\{K_s\}_{\boldsymbol{KSpriv}}\}_{\boldsymbol{KSpub}}$, $\{V_i\}_{Ks}$, $\{$Hash(V_i + ***F(i)***$\}_{\boldsymbol{KSpriv}}$

Privacidade: Garante / Não garante***, porque:***

Integridade: Garante / Não garante***, porque:***

Autenticidade: Garante / Não garante***, porque:***

d) Porque razão nas alíneas ***b) e c)*** também se incluí ***F(i)*** na síntese (Hash(...)).

5. Suponha que se pretende modificar o sistema Java RMI para que o mesmo permita migrar os servidores (objectos remotos) entre diferentes máquinas, i.e., que permita que um servidor (objecto remoto) a correr numa máquina fosse transferido para outra máquina. Esta funcionalidade permitiria, por exemplo, transferir servidores entre máquinas com diferentes capacidade em função da carga dos serviços. Ignore os problemas da transferência do estado do serviço entre diferentes máquinas.
    a) Explique como poderia ser possível aos clientes continuarem a designar os servidores pelo mesmo URL. Na sua resposta, explique os passos a tomar no momento da migração e indique que modificações seriam necessárias efectuar ao RMI registry, se alguma.

    b) Considerando a composição de uma referência remota, explique o problema que se coloca aos clientes que já têm uma referência remota para o serviço aquando da migração do mesmo e apresente uma solução.

6. Seria possível implementar um sistema baseado no modelo produtor/subscritor (publish/subscribe) usando o sistema Java RMI? Explique como ou porque não.

Verdadeiro, porque... / **Falso**, porque...

Aluno nº _____Nome: _____

7. Suponha que se pretende implementar um sistema de invocação remota de métodos/procedimentos em que todos os tipos, incluindo os tipos básicos, são passados por referência, por oposição à aproximação comum em que apenas objectos remotos (servidores) são passados por referência.
    a) Indique, justificadamente, a influência desta aproximação no desempenho esperado do sistema.

O desempenho **será melhor** / **mantém-se** / **será pior** porque

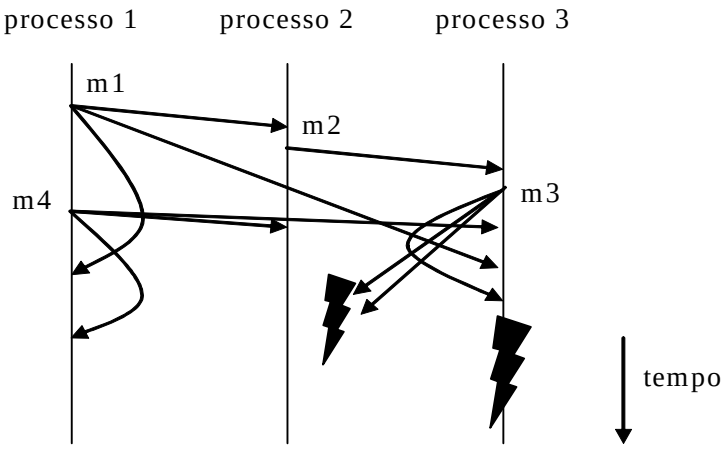
    b) Ignorando os problemas de implementação, indique uma vantagem e uma desvantagem desta aproximação face à solução actual.

8. No contexto do serviço de descoberta do sistema Jini, o qual inclui um conjunto de servidores de pesquisa (lookup services), responda às seguintes perguntas.
    a) Um servidor (que forneça um qualquer serviço na rede) regista-se periodicamente num (ou mais) servidores de pesquisa. Apresente duas razões para o registo ser efectuado periodicamente.

    b) Para fornecer um serviço semelhante numa rede local, seria possível dispensar a existência dos servidores de registo? Justifique a resposta, indicando em caso afirmativo uma aproximação alternativa e uma vantagem e uma desvantagem dessa solução; em caso negativo, explique o que torna os servidores de registo imprescindíveis.

SIM, porque... / **NÃO, porque...**

9. Considere o seguinte esquema temporal representando a propagação de mensagens num sistema composto por três processos. As setas indicam a propagação de mensagens entre os vários processos. O início de uma seta indica o envio de uma mensagem. O fim de uma seta representa a recepção de uma mensagem num processo. Suponha que o processo 3 falha antes de receber a mensagem m4 e que a mensagem m3 apenas é recebida pelo processo 3. Suponha ainda que os processos comunicam usando um sistema de *middleware* capaz de atrasar a entrega das mensagens recebidas para garantir a sua entrega por uma dada ordem.



a) Com base na informação anterior, indique se cada uma das seguintes afirmações é **[V]erdadeira** ou **[F]alsa**. **Nota: as respostas erradas descontam.**

i. É possível respeitar a ordem total entregando a mensagem m1 antes da mensagem m4 no processo 3.
ii. É possível respeitar a ordem total entregando a mensagem m4 antes da mensagem m1 no processo 3.
iii. Para garantir a ordem FIFO, é necessário entregar a mensagem m1 antes da mensagem m2 no processo 3.
iv. Para garantir a ordem causal é necessário entregar a mensagem m1 antes da mensagem m4 no processo 1.
v. É possível respeitar a ordem causal entregando a mensagem m2 no processo 3 antes da emissão da mensagem m3.
vi. Supondo que o sistema entrega a mensagem m3 apenas no processo 3, o sistema pode ser um sistema de comunicação fiável com *uniform agreement.*

10. Para confirmar, de forma atómica, a execução de um conjunto de operações submetidas anteriormente por um (ou mais) clientes, existem vários algoritmos, entre os quais o *one-phase commit* e o *two-phase commit*.
    a) Indique, de forma breve, o objectivo de cada uma das fases do algoritmo *two-phase commit*.

O objectivo da primeira fase é   O objectivo da segunda fase é

b) No protocolo two-phase commit, os participantes podem remover a informação que mantém sobre as transacções após chegarem ao estado confirmar/abortar. Explique porquê, indicando para cada mensagem que o coordenador pode enviar ao participante, qual deve ser a resposta do participante e a razão pela qual essa é a resposta correcta caso não tenha informação guardada sobre a transacção referida (use apenas os espaços necessários).

Mensagem recebida: Razão:	Resposta:
Mensagem recebida: Razão:	Resposta:
Mensagem recebida: Razão:	Resposta:
Mensagem recebida: Razão:	Resposta:

11. Suponha um ambiente de utilização semelhante ao do ambiente Linux nos laboratórios de alunos no DI, em que:
    - O servidor mantém as áreas pessoais dos alunos;
    - Os alunos acedem quase exclusivamente a ficheiros armazenados na sua área pessoal ou no computador local;
    - Os alunos podem fazer *login* em qualquer máquina dos laboratórios.

    a) Neste contexto, qual das seguintes estratégias de propagação das modificações parece mais apropriado para o cliente: *write-through* ou *delayed-write.* Justifique a sua resposta.

Write-through, porque... / Delayed-write, porque...

b) Suponha que se usava o mecanismo de cache do sistema Coda e que não existem falhas de comunicação nem nos servidores. Caso um utilizador efectuasse login em duas máquinas simultaneamente, isto poderia causar problemas de coerência dos dados? Justifique a resposta (am caso afirmativo dê um exemplo concreto e em caso negativo indique o mecanismo que garante a ausência de problemas).

SIM, porque... / NÃO, porque...