FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

## Departamento de Informática

**Licenciatura em Engenharia Informática**
**Sistemas Distribuídos – 1ª chamada, 9 de Janeiro de 2009**
**1º Semestre, 2009/2010**

**NOTAS:** Leia com atenção cada questão antes de responder. A interpretação do enunciado de cada pergunta é um factor de avaliação do teste. **O exame é SEM consulta**. **A duração do exame é de 2h00 min**.
O enunciado contém **5** páginas que devem ser entregues com a resposta ao exame.

**NOME**: _____ **NÚMERO**.: _____

1) Explique o que é um sistema aberto e quais as suas vantagens (face a um sistema proprietário).

**Um sistema aberto é**

Vantagens:

2) Suponha que pretende criar um sistema de informação para a FCT, que mantém a informação dos utilizadores. A informação mantida inclui, além da informação pessoal típica destes sistemas (e.g. nome, tipo – estudante / professor / etc., gabinete, extensão telefónica, etc.), a informação da posição do utilizador. Para actualizar a sua posição, cada utilizador teria um dispositivo capaz de determinar a posição e comunicar com os servidores que se encontram na rede fixa. Suponha que este dispositivo comunica com os servidores periodicamente – por exemplo, de 20 em 20 segundos.

   a) Caso se pretenda fomentar a esclabilidade do sistema, qual a arquitectura que considera mais adequada para organizar o sistema? Justifique.

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

b) Considere que o sistema está organizado segundo uma arquitectura cliente/servidor replicado, na qual existe um conjunto de servidores que mantêm a informação completa do sistema. Suponha que o dispositivo do cliente actualiza a informação dos servidores usando um mecanismo de comunicação em grupo. Indique, justificadamente, qual a semântica mais fraca que esse mecanismo deve implementar (relativamente a fiabilidade e ordenação das mensagens) que permite fornecer um serviço de boa qualidade para os utilizadores.

c) Considere que o sistema está organizado segundo uma arquitectura cliente/servidor. Suponha que se quer criar uma aplicação a correr nas máquinas dos utilizadores que permita apresentar num mapa a localização de cada utilizador. Para tal, será necessário que o sistema disponibilize a informação da localização dos utilizadores. Discuta como poderia ser esta informação disponibilizada de forma a minimizar os recursos utilizados – computacionais e comunicação. **Nota**: na sua resposta indique qual o modelo para os clientes acederem à informação.

3) A codificação dos dados das mensagens usando um formato intermédio, potencialmente diferente do formato no emissor e no receptor, é a solução mais adoptada nos sistemas de invocação remota de procedimentos/métodos. Apresente vantagens deste método.

4) Assinale com **[V]erdadeiro** ou **[F]also** as seguintes afirmações (**nota: as respostas erradas descontam**):

   i. Um servidor implementado em Java RMI pode estar registado com nomes diferentes no mesmo servidor rmiregistry.

   ii. Em Java RMI, uma referência remota inclui informação da interface do servidor.

   iii. O WSDL inclui informação do formato e codificação das mensagens trocadas entre o cliente e o servidor

   iv. O REST utiliza, geralmente, como protocolo de transporte o HTTP (sobre TCP).

   v. No .NET remoting, a criação de uma referência para um servidor pode ser feita no cliente indicando a localização do servidor.

5) Considere o contexto de um sistema de difusão de ficheiros multimédia. Neste sistema, um servidor S difunde para um cliente C um ficheiro F com conteúdo *Cont* (de grandes dimensões). Para ajudar a garantir a segurança do sistema, existe um servidor de segurança (SS) que partilha com o servidor e com cada cliente uma chave simétrica (Kss para o servidor S, Ksc para o cliente 1, etc.).
Apresente um protocolo que permita difundir um ficheiro de S para C de forma segura, i.e., garantindo o secretismo das mensagens e do conteúdo do ficheiro e a autenticação dos parceiros de comunicação (i.e., C deve ter a certeza que recebeu o ficheiro de S e S deve ter a certeza que apenas C pode obter o conteúdo do ficheiro). Na sua solução, minimize a informação transmitida na rede e o poder computacional necessário para executar o protocolo. O protocolo deve ter, no máximo, 3 mensagens, efectuando a seguinte interacção: S->SS; SS->C; S->C (opcional). Explique como seriam garantidas as propriedades indicadas. Use as notações sintéticas de descrição de protocolos criptográficos que aprendeu nas aulas.

**NOTA**: Caso não consiga resolver o problema assumindo que os elementos do sistema apenas conhecem inicialmente as chaves indicadas, indique explicitamente as chaves adicionais que assume serem conhecidas para cada um dos elementos do sistema no início do protocolo.

**S -> SS:**

**O que garante o secretismo?**

---

**SS -> C:**

**O que garante o secretismo?**

---

**S -> C (opcional):**

**O que garante o secretismo?**

---

**Como é que C tem a certeza que recebeu o ficheiro de S?**

**Como é que S tem a certeza que apenas C pode obter o conteúdo do ficheiro?**

**Explique como é que se minimiza a capacidade computacional necessária?**

---

**Definição dos símbolos usados (complete, se necessário):**
F – nome do ficheiro a pedir; Cont – conteúdo do ficheiro
Kss – chave secreta partilha entre S e SS
Ksc – chave secreta partilha entre C e SS

6) O sistema PGP popularizou o método de distribuição de chaves designado por Web of Trust.
   a) Explique brevemente em que consiste este método.

   b) Discuta quais as possíveis motivações para a utilização deste método.

7) Considere um sistema de partilha de ficheiros multimédia semelhante ao implementado no trabalho prático, implementado usando uma arquitectura que mantém um servidor de grupo. O servidor de grupo deve manter informação sobre os clientes ligados ao sistema e respectivos ficheiros, permitindo: (a) informar o servidor que um cliente (o próprio) partilha um ficheiro; (b) listar os clientes do sistema; (c) para cada cliente, listar os ficheiros que partilha; (d) para cada ficheiro, listar os clientes que partilham esse ficheiro; (e) listar os ficheiros com uma dada tag.
   Indique como poderia implementar cada operação usando REST (indique a operação, URL e o que o servidor faria para executar a operação).

a.

b.

c.

d.

e.

8) Recentemente, a Google passou a disponibilizar um serviço que permite a uma máquina usar como servidor de DNS inicial o servidor da Google. Este servidor resolve todos os nomes localmente, recorrendo a uma cópia mantida nos servidores da Google com toda a informação que está nos vários servidores que constituem o sistema DNS.
Explique em que situações é que é expectável que o cliente consiga obter um resultado mais rápido usando o servidor da Google e em que situações é que é expectável o contrário.

**Mais rápido acedendo inicialmente ao servidor Google:**

**Mais rápido acedendo inicialmente a servidor local:**

9) Considere o sistema de caching do NFS. Para que este mecanismo de caching funcione correctamente é necessário que os relógios do cliente e do servidor se encontrem sincronizados (com um erro reduzido)?

**Sim, porque / Não, porque (risque o que não interessar)**

10) No protocolo NFS, todas as operações relativas a ficheiros devolvem, adicionalmente, os atributos do ficheiro. Explique porquê.