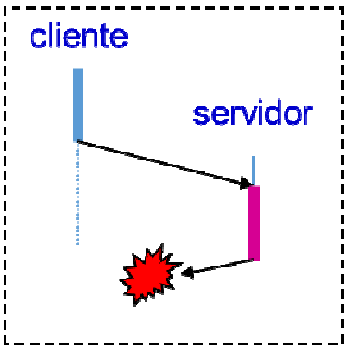
LEIC/LETI – 2013/14, 1º Exame de Sistemas Distribuídos, 17 de Junho de 2014

Responda no enunciado, apenas no espaço fornecido. Identifique todas as folhas. Duração: 2h30m

Grupo I [3,4v]

1) Um pressuposto no exercício visto nas teóricas foi a utilização de UDP como protocolo de transporte.
   a) [0,3] Assuma um RPC que usa UDP e a semântica Talvez. Identifique 3 faltas que podem ocorrer e que podem provocar o mau funcionamento deste RPC.

   b) [0,4] Que faria apenas ***do lado do cliente*** para procurar tolerar essas faltas? Seja objectivo na sua resposta.



   c) [0,4] Explique se a sua solução resolve totalmente o caso ilustrado na figura acima e porquê.

2) Considere este extracto do ficheiro *ttt-clnt.c* que deve ter examinado nas aulas práticas e que ilustra a chamada remota à função *play*.

```
int *play_1(play_args *argp, CLIENT *clnt)
{
        static int clnt_res;

        memset((char *)&clnt_res, 0, sizeof(clnt_res));
        if (clnt_call (clnt, PLAY,
                (xdrproc_t) xdr_play_args, (caddr_t) argp,
                (xdrproc_t) xdr_int, (caddr_t) &clnt_res,
                TIMEOUT) != RPC_SUCCESS) {
                return (NULL);
        }
        return (&clnt_res);
}
```

a) Neste excerto de programa estão representados vários dos elementos de uma arquitectura de RPC.
   i) [0,2] Como designa genericamente a função *play_1* apresentada acima?

   ii) [0,3] "Um dos objectivos da função *play_1* é o marshalling dos parâmetros." Copie do programa um excerto que ilustre a afirmação anterior. Justifique.

b) Neste excerto aparece a função clnt_call.
   i) [0,2] Para que serve?

   ii) [0,4] Com base neste exemplo, justifique a razão de existirem funções geradas pelo compilador da IDL e funções de uma biblioteca de run-time do RPC.

c) Na função aparece um parâmetro CLIENT *clnt .
   i) [0,4] Para que serve?

   ii) [0,4] Onde foi obtido o valor deste parâmetro?

   iii) [0,4] Explique objectivamente a vantagem da existência deste parâmetro, dando um exemplo concreto.

Grupo II [2,5v]

Considere a seguinte interface Java de uma pilha:

```
public interface Pilha {

     void push(Elemento);

     Elemento pop();
  }
```

1. [0,5v] Faça as transformações necessárias no código acima para tornar esta interface remota.

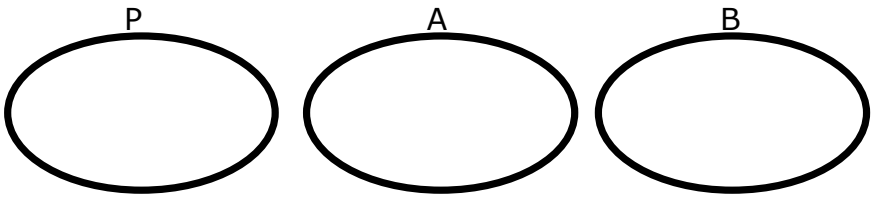
2. [0,6v] Considere que a classe PilhaServant implementa a interface remota Pilha. Crie um programa que cria um objeto remoto dessa classe e o regista no RMI com o nome "pilha-sd-exame".
   Simplificação: omita do seu programa a definição do SecurityManager.

```
public static void main(String args[]){









 while (true) ; //ciclo infinito para não terminar
}
```

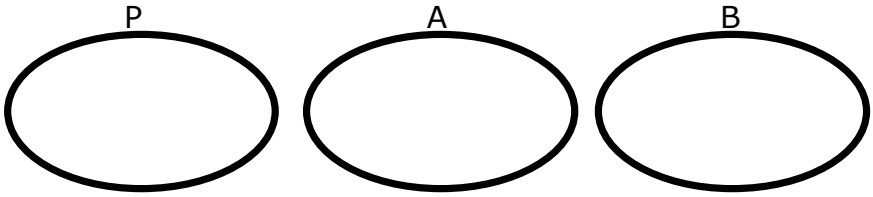
3. [0,6v] Construa agora um programa cliente que: cria uma instância de MeuElemento (classe que implementa a interface Elemento) e a coloca no topo da pilha "pilha-sd-exame" (invocando o método push) que foi instanciada na alínea anterior. Assuma que o objeto remoto da alínea anterior foi criado na máquina a correr em "sd.tecnico.ulisboa" (no porto habitual).
   Mais uma vez, omita do seu programa a definição do SecurityManager.

```
public static void main(String args[]){









}
```

4. Assuma que: i) o objeto remoto pilha foi instanciado na máquina virtual P; ii) as máquinas virtuais A e B criaram novos objetos e adicionaram-nos à pilha remota de P.
   Apresente as instâncias (θ) existentes neste sistema e as referências entre elas (↪), para os dois casos seguintes. Junto a cada instância que apresentar, indique o nome da respetiva interface.
   a. [0,4v] Caso em que a interface Elemento é *Remote*.



   b. [0,4v] Caso em que a interface Elemento não é *Remote*. Justifique.



Grupo III [3,2v]

1. Quanto ao WSDL:
   a) [0,4] A que secções corresponde a assinatura (no sentido usado nas linguagens OO) do serviço? Justifique.

   b) No RMI e RPC é um servidor de nomes que permite conhecer a localização do servidor. No WSDL esta localização faz parte do contrato.
      i) [0,3] Em que secção?

      ii) [0,4] Apresente uma razão que justifique a sua inclusão no contrato.

      iii) [0,4] Apesar de presente no contrato, pode justificar-se utilizar um Serviço de Nomes. Apresente uma razão.

   c) [0,4] Explique qual é a real mais-valia do WSDL mesmo quando a abordagem de desenvolvimento dos WS é *implementation-first*?

d) [0,4] Suponha que pretende colocar informação no header de um pacote soap relativa por exemplo à chave usada para cifrar o conteúdo do body. Em que secção do WSDL se define esta informação? Justifique.

2. Considere o excerto de um programa de um cliente que pretende usar um Web service. Explique-o de acordo com as alíneas seguintes:

```
HelloWorld_Impl proxy = new HelloWorld_Impl();
HelloWorldSoap soapProxy = proxy.getHelloWorldSoap();
```

a) [0,3] Como é que o cliente sabe o nome da classe?

b) [0,3] Como é que a classe pode ter sido gerada?

c) [0,3] Pode deduzir deste excerto se o Web Service foi desenvolvido em implementation first ou contract-first? Justifique.

Grupo IV [4v]

Considere um portal de reserva de viagens que permite aos utilizadores comprarem viagens, agindo de intermediário entre turistas e operadoras de viagens.

Quando um cliente - a correr em nome de um dado utilizador, *U* - pede ao portal (*P*) para comprar uma determinada viagem, *P* responde com a seguinte mensagem:

$$P\text{->}U: \underbrace{\{senha\}_{Kx}\ ,\ detalhes\ da\ reserva}_{M},\ \{resumo(M)\}_{Ky}$$

A mensagem acima transporta uma senha secreta que, no início da viagem, o utilizador deverá comunicar à empresa que oferece a viagem para provar que fez a compra, logo tem direito à viagem.

Na mensagem acima, considere que:

- "{}" significa cifragem assimétrica.
- Tanto o portal *P* como cada utilizador *U* dispõem de um par de chaves assimétricas: $K_{pub(P)}$, $K_{priv(P)}$, $K_{pub(U)}$, $K_{priv(U)}$, respetivamente. As chaves públicas foram previamente partilhadas entre os interlocutores de forma segura.

1. Quanto à componente $\{senha\}_{Kx}$:
   a. [0,4v] De entre as chaves $K_{pub(P)}$, $K_{priv(P)}$, $K_{pub(U)}$, $K_{priv(U)}$, a qual corresponde Kx?

   b. [0,4v] Escutando a mensagem que passou pela rede, observou-se o seguinte extrato: `TWFuIGlzIGRpc3RpbmdlaXN...`
   É este o resultado retornado diretamente pela função de cifra? Justifique.

2. A componente $\{resumo(senha)\}_{Ky}$ corresponde a uma assinatura digital de chave pública.
   a. [0,4v] De entre as chaves $K_{pub(P)}$, $K_{priv(P)}$, $K_{pub(U)}$, $K_{priv(U)}$, a qual corresponde Ky?

   b. [0,5v] Apresente o pseudo-código do algoritmo que U executa para validar a assinatura que recebe.

   c. [0,7v] Indique um ataque que seria possível caso a mensagem não levasse uma assinatura digital. Seja claro nos passos que o atacante segue para executar o ataque e no benefício que o atacante obteria do ataque. (Nota: não se aceitam ataques que apenas visam o vandalismo.)

3. O cliente de U conheceu a chave pública de P num certificado digital de chave pública que obteve numa pesquisa na Web, a partir de um site de origem duvidosa.
   a. [0,6v] U tem forma de confirmar que a chave pública contida no certificado é legítima? Se sim, indique os passos que U segue para chegar a essa confirmação. Se não, indique uma alternativa correta.

   b. [0,5v] Considere que o certificado que U recebeu foi emitido pela CA_2, que por sua vez é uma sub-CA da CA raiz CA_1. A não conhece CA_2 mas tem instalado o certificado de chave pública de CA_1. Como deve U proceder?

4. [0,5v] Quanto à abordagem seguida para autorizar o acesso às viagens neste sistema, como a classifica: lista de controlo de acessos ou capacidades? Justifique.

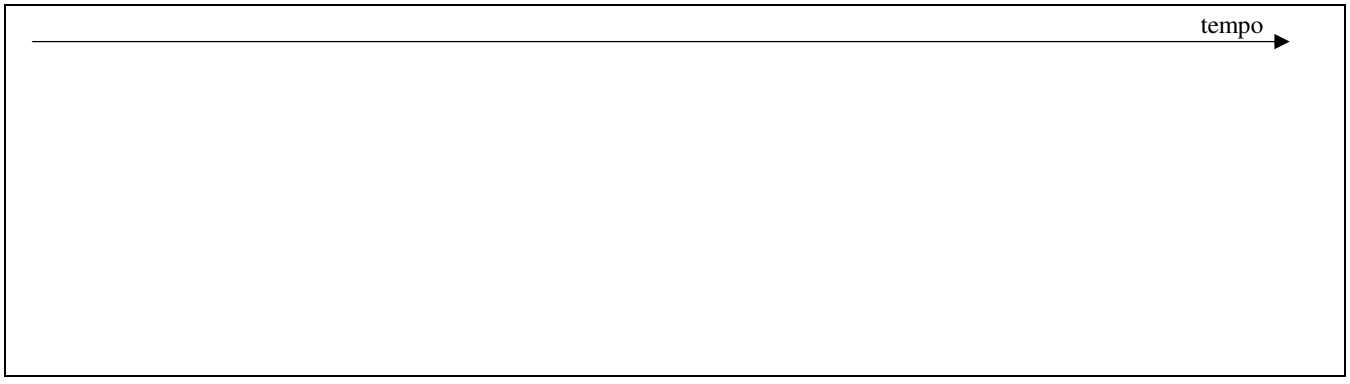
Grupo V [2,5v]

1. Considere uma invocação de um cliente a um serviço em RPC (em qualquer das tecnologias que aprendeu). Considere o pressuposto que pretende tolerar faltas silenciosas do servidor (também designadas por faltas de paragem – crash).
   a) [0,4v] Explique o que caracteriza uma falta silenciosa.

   b) [0,6v] Que implicação tem assumir que as faltas dos servidores são silenciosas (e não outro tipo de faltas) no grau de replicação? Justifique com um exemplo.

2. O protocolo de primary backup, que aprendeu nas aulas teóricas, com dois servidores tolera uma falta silenciosa de um servidor.
   a) Um dos pressupostos é que o sistema é síncrono, o que implica que todas as mensagens e processamento são executados dentro de um período máximo de tempo.
      i) [0,5v] Dê um exemplo de uma situação em que o sistema falha se eliminar este pressuposto.

      ii) O protocolo de quórum (*quorum consensus*, ensinado nas aulas) tolera o funcionamento assíncrono do sistema.
         (1) [0,5v] Explique com um exemplo.



(2) [0,5v] Como compara o grau de replicação deste protocolo com o primary backup?

Grupo VI [2,4v]

Excerto do IDL

```
program BANCOPROG {
  version BANCOVERS {
    ……;
  } = 1;
} = 0x20000005;
```

Excerto do programa de ligação ao servidor

```
void main (int argc, char *argv[]){
  CLIENT *cl;
  int a, *result;
  char* server;
  server = argv[1];
  cl = clnt_create(server, BANCOPROG, BANCOVERS, "tcp");
  if(cl == NULL) {
      clnt_pcreateerror(server);
      exit(1);
  }
  ……
}
```

1. O excerto de programa acima implica a utilização de um serviço de nomes.
   a) [0,4v] Explique qual a função deste serviço de nomes no Sun-RPC.

   b) Considerando o nome do serviço (BANCOPROG, BANCOVERS):
      i) [0,4v]Como o classifica quanto ao âmbito? Justifique.

      ii) [0,4v] Do ponto de vista das propriedades dos nomes, indique **duas** diferenças relevantes entre este nome e o URL que é utilizado na invocação dos Web Services.

2. Considere a frase: "a disponibilidade do serviço de nomes pode determinar a disponibilidade de um serviço".
   a) [0,4v] Com o conhecimento que tem da invocação de serviços em Web Services, apresente um exemplo uma forma de utilização dos Web Services em que a frase tem sentido.

b) [0,4v] Que técnica(s) conhece para mitigar o problema da disponibilidade dos serviços de nomes? Explique como o DNS a(s) utiliza.

3. [0,4v] Uma preocupação nas soluções de tolerância a faltas é que não invalidem propriedades de soluções centralizadas. Uma dessas propriedades é a serialização das operações. Acha que a arquitetura que referiu do DNS garante esta propriedade? Justifique.

Grupo VII [2v]

Considere o seguinte programa transacional, que efetua um conjunto de reservas de viagens sobre diferentes operadores. Assuma que o protocolo de terminação atómica é o 2-phase commit (2PC).

```
1 Boolean reservarViagens(List<Reserva> reservas) {
2  tx = openTransaction();
3  for each (Reserva r in reservas) {
4    Endpoint e = r.obterOperador();
5    if (e.reservarViagem(r, tx) == false) {
6      abortTransaction(tx);
7      return false;
8    }
9  }
10 closeTransaction(tx);
}
```

1. [0,4v] Indique uma razão que levou o programador a incluir as linhas 3-9 numa transação.

2. [0,4v] Indique que linhas correspondem a invocações sobre o coordenador do 2PC.

3. [0,6v] A transação distribuída pode abortar caso o programa chegue à linha 6. Há outras situações em que a transação distribuída aborte? Se não, justifique. Se sim, indique uma dessas situações em detalhe.

4. [0,6v] Assuma que o método é chamado com reservas no argumento, geridas pelos servidores A, B e C, respetivamente. Apresente num diagrama as mensagens que são trocadas quando a linha 10 se executa. Assuma um cenário em que o servidor A está em falha silenciosa durante o seu exemplo todo; todos os outros servidores estão corretos.