

- Justifique todas as respostas.
-

1 [12v]- Indique, para cada afirmação, se é **verdadeira** ou **falsa**, justificando. Cada alínea desta pergunta tem a mesma cotação (1 valor). Respostas erradas não descontam. Por outro lado, respostas certas sem justificação também não contam. (Responda a esta pergunta no enunciado.)

1.1- UDP é mais apropriado do que TCP para qualquer aplicação multimédia.

1.2- Algoritmos epidémicos para difusão (*broadcast*) podem ser facilmente modificados para suportar multicast duma forma eficiente.

1.3- Uma biblioteca de RPC que suporte a semântica **at-most-once** não pode ser usada em aplicações cliente-servidor com operações idempotentes.

Nome:

1.4- Um servidor **concorrente** tem que ser implementado necessariamente com o recurso a múltiplos processos ou a múltiplos *threads*.

1.5- A partir da versão 1.1 do protocolo HTTP, a qual suporta a reutilização de conexões TCP, não se justifica o uso de *cookies* como *transport-layer independent handles* em serviços Web, exceto pelo desejo de rastrear os acessos dos seus utilizadores.

1.6- Leases com tempos de expiração relativos podem ser facilmente implementados em sistemas assíncronos.

Nome: _____

1.7- Sejam e_1 e e_2 dois eventos, e $LS(e)$ e $VS(e)$ a *Lamport timestamp* e a *vector timestamp* do evento e , respectivamente. Então: $LS(e_1) < LS(e_2) \Rightarrow VS(e_1) < VS(e_2)$

1.8- Qualquer algoritmo distribuído de exclusão mútua pode substituir um algoritmo distribuído de eleição de **leader**.

1.9- No protocolo **two-phase commit**, a falha de qualquer participante pode adiar a tomada de decisão até esse participante recuperar.

Nome: _____

1.10- View synchronous communication garante apenas que todos os processos que comunicam estão de acordo em relação aos participantes na vista.

1.11- Um serviço replicado que assegura que o resultado duma execução é equivalente a uma execução desse serviço sem replicação em que todas as operações de qualquer cliente são aplicadas diz-se **sequential consistent**.

1.12- Se a **cloud** fosse um sistema síncrono, o **CAP theorem** não seria verdadeiro.

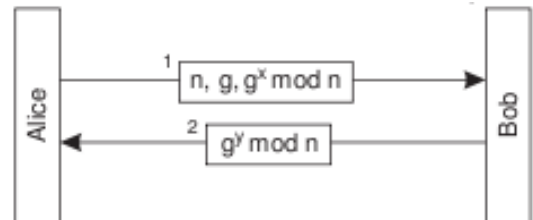
2 [2v]- Sobre serviços de nomes.

2.1- Em geral, em termos da sua estrutura, os nomes podem ser de um de dois tipos . Descreva-os. Para cada um deles apresente uma razão que poderá justificar a sua adopção (em vez do outro).

2.2- Considere uma implementação de Chord com chaves de 5 bits. Assuma que os nós com os identificadores 1, 9, 18, 20, 21 e 28 são os únicos nós activos e que as suas **finger tables** convergiram para o seu valor final nesta configuração. Ilustre a resolução da chave de valor 11 por esse sistema partindo do nó 20. Explique.

3 [3v] - Sobre segurança.

3.1- Considere o protocolo representado na figura ao lado. Diga para que serve e explique como as mensagens representadas contribuem para esse fim. Note que para isso poderá ter que descrever o significado de cada um dos símbolos representados.



3.2- Admita que uma aplicação necessita de todas as propriedades tipicamente associadas a um canal de comunicação seguro. O protocolo da alínea anterior é suficiente? Em caso negativo, descreva o que deverá ser acrescentado. Em caso positivo, justifique.

3.3- Admita que nesta aplicação se pretende usar JSSE com o protocolo representado na figura. Quais, se alguma, das seguintes *cipher-suites* satisfazem os requisitos?

SSL_RSA_WITH_RC4_128_MD5

TLS_DH_anon_WITH_AES_256_CBC_SHA256

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

TLS_KRB5_WITH_RC4_128_MD5

Justifique.

4 [2v]- Sobre **state machine replication (SMR)** e Paxos.

4.1- Explique a implementação de SMR usando **Paxos** proposta por Lamport.

4.2- Na ausência de falhas esta implementação é ótima. Explique porquê.

5 [1v]- Durante o semestre tentamos apresentar os conceitos fundamentais de sistemas distribuídos e alguns aspetos importantes para a implementação de aplicações distribuídas. Para contribuir para uma melhoria da UC, faça uma proposta para melhorar algum ponto fraco que tenha identificado.

Nota: A avaliação da resposta será feita estritamente do ponto de vista da sua qualidade formal, i.e. identificação do ponto fraco e descrição da proposta, independentemente de concordarmos ou não com a sua resposta.