Com consulta de *cheat sheet* manuscrita. Duração: 2h00m.

Recomendação: As suas respostas devem estar bem estruturadas, ser completas e estar escritas de forma clara. Podemos avaliá-las **unicamente** tendo em conta o que foi escrito, e não o que pensa que podemos inferir.

Nota importante: Responda às questões 1 e 2 numa folha de exame e às questões 3, 4, 5 e 6 noutra folha de exame.

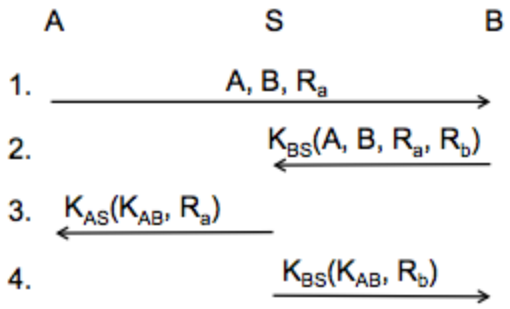
1. **[4 valores; 0.5 por questão]** Indique, para cada afirmação, se é **verdadeira** ou **falsa**, justificando brevemente a sua resposta.

    a. UDP é um protocolo de transporte, orientado à conexão, fiável.
    b. IP Multicast pode facilmente recorrer ao protocolo TCP para garantir fiabilidade.
    c. *Remote Procedure Calls* (RPCs) foram criados para tornar possível a comunicação remota entre dois processos comunicarem em sistemas identicos.
    d. O resolução de nomes DNS é delegada hierarquicamente pois, por exemplo, os nós da raz indicam quais servidores devem ser consultados para resolver os domínios ".com", e assim por diante, até que a consulta do cliente possa ser respondida.
    e. A fase de *Map* do *MapReduce* oferece uma forma de guardar e obter items de acordo com as suas chaves.
    f. Numa rede Peer-to-Peer centralizada, tal como o Naptser, apenas uma máquina precisa de ser visitada (*O(1)*) para localizar um ficheiro.
    g. TTL é um mecanismo utilizado para prevenir a propagação de *queries* em redes peer-to-peer baseadas em *flooding*.
    h. Em sistemas distribuídos de ficheiros NFS, é possível que alterações de um cliente não estejam visíveis para outro client que está a ler o ficheiro logo após a escrita no ficheiro.

2. **[6 valores; 1 por questão]** A seguinte figura ilustra um protocolo entre dois agentes A e B e um servidor S. A intenção do protocolo é que o servidor gere uma chave de sessão K_{AB} e garantir que A e B estão, seguramente, a comunicar entre eles.

    Cada um dos agentes partilha uma chave privada com o servidor S: a chave de A é K_{AS} e a de B é K_{BS}. Os valores Ra e Rb são *nonces* (number-used-once) gerados aleatoriamente. A notação $K(M_1,M_2,...,M_n)$ significa que a sequência de mensagens $M_1,M_2,...,M_n$ são encriptadas com a chave K.

Com consulta de *cheat sheet* manuscrita. Duração: 2h00m.



Assuma o seguinte:

- Inicialmente, somente A e S conhecem K_{AS}, bem como somente B e S conhecem K_{BS};
- O servidor S não é malicioso, mas poderá existir um impostor S' a tentar fazer-se passar por S;
- Poderá existir utilizadores maliciosos A' ou B' a tentar fazer-se de A ou B;
- Utilizadores maliciosos poderão interceptar qualquer tipo de tráfego, *replay* mensagens antigas, ou enviar mensagens novas;
- A encriptação é segura, e a encriptação da sequência não revela qualquer informação a encriptação dos elementos individuais. Por exemplo, conhecendo $K(M_1,M_2)$, não revela qualquer informação sobre $K(M_1)$ ou $K(M_2)$.

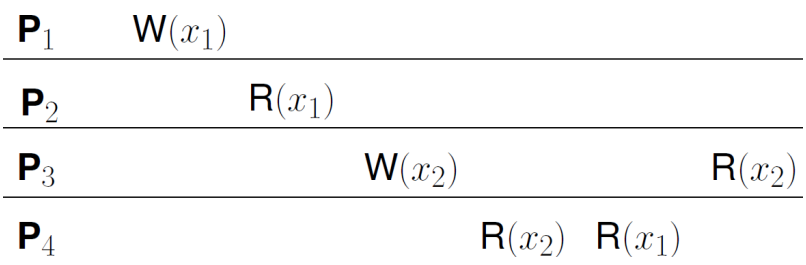
Indique, para cada afirmação, se é **verdadeira** ou **falsa**, justificando numa frase a sua resposta.

1. S tem a certeza de que a mensagem 2 acabou de ser gerada por B (ou seja, não é um *replay* de uma mensagem antiga)
2. A tem a certeza de que a mensagem 3 acabou de ser gerada por S (ou seja, não é um *replay* de uma mensagem antiga)
3. B tem a certeza de que a mensagem 4 acabou de ser gerada por S (ou seja, não é um *replay* de uma mensagem antiga)
4. Assim que o protocolo terminar, A terá a certeza de ter estabelecido uma sessão com B
5. Assim que o protocolo terminar, B terá a certeza de ter estabelecido uma sessão com A
6. Assim que o protocolo terminar, nenhum outro agente que não A,B, ou S poderá saber o valor de K_{AB}

Com consulta de *cheat sheet* manuscrita. Duração: 2h00m.

Nota importante: Responda às questões 1 e 2 numa folha de exame e às questões 3, 4, 5 e 6 noutra folha de exame.

3. **[2 valores]** Sobre sincronização de relógios.
   1. Embora seja possível sincronizar relógios usando uma única mensagem, muitos protocolos, p. ex. o NTP, usam duas mensagens, uma em cada direção. Explique porquê.
   2. Dê um exemplo do uso de relógios físicos sincronizados numa aplicação distribuída, e explique a vantagem desse uso no caso concreto da aplicação indicada. (**Nota:** Manter relógios físicos sincronizados não é uma aplicação.)
4. **[2.5 valores]** Considere o protocolo *"2 phase-commit"*.
   1. Descreva sucintamente este protocolo e explique para que serve.
   2. Assuma que numa execução deste protocolo todos os participantes estão no estado *READY* e que o coordenador falha sem que envie a sua decisão aos participantes. É possível que os participantes venham a decidir *COMMIT*? Justifique.
5. **[3 valores]** Sobre a replicação do tipo primário-apoio *(primary-backup)*.
   1. Explique a diferença entre implementações com e sem bloqueio.
   2. Dê uma vantagem e uma desvantagem de cada uma dessas implementações. Justifique.
   3. Pode este tipo de replicação tolerar falhas bizantinas? Justifique.
6. **[2.5 valores]** Sobre modêlos de consistência.
   1. A figura seguinte representa os acessos por 4 processos, P_1 a P_4, a um serviço de armazenamento de dados replicado.



      O eixo horizontal é o tempo. $W(x_1)$ e $W(x_2)$ denotam respetivamente a escrita dos valores x_1 e x_2 na variável x. $R(x_1)$ e $R(x_2)$ denotam a leitura da variável x com retorno dos valores x_1 e x_2, respetivamente.
      Este serviço garante consistência sequencial? Justifique.
   2. Considere um serviço replicado que implementa *read-your-writes* e *writes-follow-reads*. Este serviço garante consistência sequencial? Justifique.