Questão 3
(Gestão contributiva de chaves em sistemas de comunicação em grupo)

a) De acordo com o estudo e leituras que realizou para realização do trabalho 3, quais são as propriedades fundamentais e os critérios fundamentais de comparação utilizados para o estudo comparativo de diversas aproximações da literatura para análise de sistemas de gestão descentralizada e contributiva de chaves ?

b) Que vantagens ou desvantagens existem entre um esquema do tipo Diffie Hellman do tipo Distributed Logical Key Hierarchy e um esquema do tipo Group Diffie Hellman (do tipo distribuição em anel, tomando como exemplo uma variante do tipo GDH-1) para se implementarem esquemas contributivos de gestão e distribuição de chaves ?

c) Se se considerar um ambiente do tipo Internet, um protocolo contributivo com as características do tipo TGDH pode exibir propriedades interessantes para suportar a re-junções de partições após falhas que provocam partições de grupos. Tente resumir de forma o mais rigorosa possível como é que num protocolo deste tipo se desencadeia uma junção após uma partição que tenha sido provocada por uma falha de ligações entre membros de grupos e em que moldes essa junção pode ser vantajosa face a outras aproximações que conheça.