

### Atividade B - Perguntas 70 a 76

Aluno: Rafael B. Castilhos Matrícula: 20205642

70) A fase laranja realiza a identificação das partes, fazendo uso da sincronização da requisição para autenticação (SYN), a mensagem que deverá ser entendida e processada (ACK) e por fim a parte do número ( $n^x$ ), que pode ser formulada com um Hash da hora, identificador de destino e origem e um número sequencial. A fase verde é responsável pela troca de chaves assimétricas. A fase amarela formula o contrato de chaves simétricas, utilizando o método de Diffie-Hellman. Por fim a fase azul realiza a criptografia das informações.

71) AES, RSA, SHA256 e Diffie-Hellman.

72) Raspberry Pi 3 - Model B, notebook i7 8 core com 8GB Ram e VM na GCP Engine com 1 core e 8GB Ram (Skylake CPU).

73) É evidente que nas tabelas de resultados, o tempo em milissegundos para as etapas dos procedimentos possui uma expressão diferente entre Fog e Cloud no quesito Network, isso devido ao fato do fog estar mais próximo fisicamente do Raspberry, assim não necessitando passar por diferentes países e consequentemente modems e switches.

74) Devido a menor capacidade de processamento do Raspberry o tempo em milissegundos ficou mais elevado em todas as passagens comparado ao fog e cloud. Também foi possível concluir que a cloud possui as melhores médias de tempo.

75) AITSPA detecta se o protocolo é seguro contra o ataque do homem do meio, e conforme a figura b, todo



os testes passaram com sucesso na verificação.

76) As atividades relacionadas ao desenvolvimento de protocolos iniciam-se na especificação técnicas e formais. Com isso, a validação e verificação são atividades importantes. Tendo isso completo, parte-se para implementação

