



Universidade Federal do Ceará (UFC)
Disciplina: Segurança da Informação
Prof. Marcos Dantas Ortiz
Lista teórica – Assimétrica - parte 2

- Campus Quixadá
- Período 2022:1
- mdo@ufc.br
- entrega – 09/05/22

- 1) Explique quais são as dificuldades relacionadas à distribuição de chaves para o uso de criptografia. Caracterize as soluções para criptografia simétrica e assimétrica.
- 2) Explique, através de um diagrama com troca de mensagens, o ataque *man-in-the-middle* (homem do meio) sobre autenticação com criptografia assimétrica. Qual a falha é explorada por este ataque? Ele também pode ocorrer quando utilizado criptografia simétrica? Justifique sua resposta.
- 3) Usando a troca de chaves Diffie-Hellman, encontre a chave de sessão que será usada por Bob e Alice.
 - Valores públicos combinados entre os dois: $q = 71$, $\alpha = 7$.
 - Chave secreta de Alice: 37.
 - Chave secreta de Bob: 63.
- 4) Explique como funções *Hash* são usadas para fornecer integridade.
- 5) Descreva como o protocolo HMAC (*Message Authentication Code*) fornece autenticação.
- 6) No contexto de assinatura digital, explique os requisitos:
 - a. Verificável.
 - b. Não forjável
 - c. Não repudiável.
- 7) Apresente de forma ilustrada como assinatura digital é implementada através de criptografia assimétrica e funções *Hash*.
- 8) De que modo um resumo de mensagem (código *hash*) criptografado por criptografia assimétrica proporciona uma assinatura digital melhor do que utilizar a própria mensagem criptografada com criptografia assimétrica?
- 9) Considere um sistema de comunicação (email, por exemplo) e descreva de forma ilustrada como é possível implementar nesse sistema:
 - a. sigilo;
 - b. integridade + autenticação de remetente;
 - c. sigilo + integridade + autenticação de remetente;
 - d. sigilo + integridade + autenticação de remetente e receptor;

Bom Trabalho!