Universidade Federal do Ceará (UFC) - Campus Quixadá
Disciplina: Segurança - Período 2023:1
Prof. Marcos Dantas Ortiz - mdo@ufc.br
Lista II - Cripto. Assimétrica e Hash - entrega 10/05/23

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) Refaça o ataque man-in-the-middle, mas agora para a troca de chaves Diffie-Hellman.

5) Explique como funções *Hash* são usadas para fornecer integridade.

6) Descreva como o protocolo HMAC (*Message Authentication Code*) fornece autenticação. Faça um diagrama com a troca de mensagens.

7) No contexto de assinatura digital, explique os requisitos:
   a. Verificável.
   b. Não forjável
   c. Não repudiável.

8) Apresente de forma ilustrada como assinatura digital é implementada através de criptografia assimétrica e funções *Hash* .

9) De que modo um resumo de mensagem (código *hash*) criptografado por criptografia assimétrica proporciona uma assinatura digital melhor do que utilizar a própria mensagem criptografa com criptografia assimétrica?

10) 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!