Universidade Federal do Ceará – Campus de Quixadá
Disciplina: Segurança da Informação - 2017.1
Prof. Marcos Dantas Ortiz (mdo@ufc.br)
Nome: _____
Correção – 05/05

1) Liste e defina cada um dos serviços fundamentais de segurança.
2) Classifique os quatro tipos de ataques básicos à segurança e os relacione com serviços definidos na questão 1.
3) Cifre a mensagem a seguir usando cifra de César com K =7:
   a) A Cesar o que e de Cesar. Todos os caminhos levam a Roma.
4) Resolva a cifra monoalfabética a seguir.

   LXIPBT JD TKSTRXRKXLBO AKD KRXQXUBE BYDWBT KE BQIBSDRO LXIPBWRD

   Chave: *b-s-l-j-d-i-g-h-x-m-z-q-e-w-o-y-a-p-t-r-k-v-n-c-f-u*

   Comente a fragilidade desse sistema criptográfico, apesar do espaço de chaves ser da ordem 26!
5) Explique porque algoritmos de cifragem que geram repetição de padrões não são indicados para uso não-acadêmico. Use a questão 4 para justificar sua resposta, supondo que o atacante conhecia o assunto da mensagem.
6) Motive o uso da Confusão e da Difusão para evitar os problemas da questão 4. Como esses requisitos são implementados no DES?
7) Diferencie cifra de fluxo da cifra de bloco. Cite uma cifra de cada tipo.
8) Cifre “001101111” e decifre usando cifra de bloco

   Cifragem: C(i) = Ks(M(i) XOR (R(i))

   Decifragem: M(i) = Ks(C(i)) XOR R(i)

   R(1) = 001, R(2) = 111 e R(3) = 100

   Tabela de Mapeamento Ks ---------->

Entrada	Saída	Entrada	Saída
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

9) Comente o uso de números aleatórios na questão 8 (R1, R2 e R3). Por que é menos seguro usar apenas a tabela de mapeamento?
10) Repita o exercício da questão 8 utilizando a técnica de Encadeamento do Bloco de Cifra. Use R(1) como vetor de inicialização.
11) Explique porque o algoritmo *One Time Pad* é considerado uma cifra perfeita (inquebrável).
    a) Faça o ataque força bruta do texto cifrado: 1001
    b) Qual chave gerou esse texto cifrado?

12) Explique quais são as dificuldades relacionadas à distribuição de chaves para o uso de criptografia. Caracterize as soluções para criptografia simétrica e assimétrica.

13) 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.

14) 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.

15) Explique como funções Hash são usadas para fornecer integridade.
16) Descreva como o protocolo HMAC (Message Authentication Code) fornece autenticação.
17) No contexto de assinatura digital, explique os requisitos:
    a) Verificável.
    b) Não forjável
    c) Não repudiável.

18) Apresente de forma ilustrada como assinatura digital é implementada através de criptografia assimétrica e funções Hash .
19) 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?
20) 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!