## SEGURANÇA INFORMÁTICA E DAS COMUNICAÇÕES

## CAPÍTULO 1. FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO

### Exercícios Práticos 2 – Capitulo 1

Esta ficha tem como o objectivo de consolidar todos os conceitos apreendidos nas aulas Teóricas.

1. Marque a alternativa abaixo que indica, correctamente, o nome do algoritmo simétrico de criptografia de fluxo de tamanho de chave variável com operações orientadas a *bytes*. O algoritmo é baseado no uso de uma permutação aleatória. Neste algoritmo uma chave de tamanho variável de 1 a 256 *bytes* (8 a 2043 *bits*) é usada para inicializar um vector de estado S de 256 *bytes*, com elementos S[0], S[1], ... , S[255]. Em todos os momentos, S contém uma permutação de todos os números de 8 *bits* de 0 a 255. Para a encriptação e a decriptação, um *byte* K é gerado a partir de S selecionando uma das 255 entradas de uma forma sistemática. À medida que cada valor de K é gerado, as entradas em S são mais uma vez permutadas.

   Selecione a afirmação correcta:

   A) RSA.

   B) RC4**.**

   C) 3DES.

   D) IDEA.

   E) Nenhuma está correcta.

2. Tendo em conta o algoritmo RSA, com os parâmetros p = 29, q = 37 e com a chave secreta Ks = 457. Encontre a chave pública Kp?

   a) A chave é Kp = 660

   b) A chave é Kp =13

   c) A chave é Kp = 713

   d) A chave é Kp = 203

3. Para aprimorar a segurança na transferência de documentos da Defesa Nacional, decidiu-se implantar o sistema de assinatura digital dos documentos. Para essa implementação, o Técnico foi incumbido de escolher um hash criptográfico. De entre as opções, o Técnico escolheu o (…)

   Esta correcta a afirmação:

   A) RSA

   B) 3DES

   C) RC4

   D) MD5

4. Escolha uma das opções e justifique que, o método de autenticação dos algoritmos de criptografia de chave pública que opera um conjunto com uma função resumo, também conhecida como função de hash, é chamado de assinatura digital. Um algoritmo usado para gerar o resumo (hash) de uma mensagem é o…
   a) DES
   b) AES
   c) RSA
   d) SHA
   e) MD5

5. Quais são e qual é o objectivo dos comandos executados no AES com Nb=4

6. Pode-se resumir o RSA em três partes: Geração das Chaves, Codificação das Chaves e Decodificação das Chaves. Explique de forma detalhada, o processo de Geração das Chaves.

7. Como é constituído o algoritmo Simétrico RC4?

8. Descreva o mecanismo criptográfico que usa o algoritmo RSA.

9. O procedimento de descriptografia do algoritmo RC2, toma como entrada quatro palavras de texto cifrado: R [0] R [1] R [2] R [3], que formam um bloco de dados criptografados. Cada bloco de dados será descriptografado usando as mesmas 64 palavras da chave secreta expandida: K [0] K [1] ... K [63].
   a) Quais são as etapas de descriptografia que são realizadas em cada bloco de texto cifrado?
   b) Em que consiste as operações de R-Mixing, realizadas em quatro palavras do bloco de dados criptografado?

**Bom Trabalho!**