

**DURAÇÃO DO TESTE: 1 HORA**

0	0	0	0	0
1	1	1	1	1
2	2	2	2	2
3	3	3	3	3
4	4	4	4	4
5	5	5	5	5
6	6	6	6	6
7	7	7	7	7
8	8	8	8	8
9	9	9	9	9

← Marque o seu número de aluno preenchendo completamente os quadrados respectivos da grelha ao lado (■) e escreva o nome completo, o número e o curso abaixo.

Nome: .....

.....

Número: ..... Curso: .....

Para cada questão 1-6 existe uma e apenas uma resposta certa. Marque a resposta certa preenchendo completamente o quadrado respectivo (■) com caneta azul ou preta. Cada resposta certa vale 0,5 valores. Cada resposta errada desconta 0,2 valores. Marcações múltiplas anulam a questão.

Das questões 7, 8 e 9 escolha uma sobre um tema diferente do seminário que apresentou e responda apenas a essa. Vale 1 valor.

**Questão 1** As duas técnicas base da criptografia de chave simétrica são:

- |  |   |
|--|---|
| <input type="checkbox"/> a) transposição e permutação.   | <input type="checkbox"/> c) permutação e substituição.    |
| <input type="checkbox"/> b) transposição e substituição. | <input type="checkbox"/> d) nenhuma das restantes opções. |

**Questão 2** O ADFGVX

- ☐ a) é um protocolo de chave simétrica, que usa as duas técnicas base.
- ☐ b) é um protocolo de chave assimétrica, não vulnerável ao man-in-the-middle.
- ☐ c) é um protocolo de chave simétrica, que usa apenas uma das técnicas base.
- ☐ d) é um protocolo de chave assimétrica, vulnerável ao man-in-the-middle.

**Questão 3** Qual das seguintes afirmações é FALSA. Ao codificar uma mensagem a máquina Enigma

- ☐ a) pode codificar a mesma letra por letras diferentes.
- ☐ b) pode codificar uma letra por ela própria.
- ☐ c) nenhuma das restantes opções.
- ☐ d) pode codificar letras diferentes pela mesma letra.



**Questão 4** Os princípios de Kerckhoff são princípios que todos os sistemas criptográficos devem satisfazer. Um dos princípios de Kerckhoff diz que a segurança de um sistema criptográfico deve depender:

- ☐ a) só da complexidade do algoritmo de encriptação.
- ☐ b) do segredo da chave e do segredo do algoritmo.
- ☐ c) do segredo do algoritmo, não do segredo da chave.
- ☐ d) só do segredo da chave, não do segredo do algoritmo.

**Questão 5** O funcionamento do RSA é baseado no seguinte:

- ☐ a) multiplicação é fácil e exponenciação é difícil.
- ☐ b) multiplicação é fácil e factorização é difícil.
- ☐ c) no problema do logaritmo discreto.
- ☐ d) multiplicação é fácil e divisão é difícil.

**Questão 6** No protocolo de troca de chaves de Diffie-Hellman, Alice e Bob usam números secretos  $a$  e  $b$  para calcular números  $A$  e  $B$  que são depois trocados entre eles.

- ☐ a)  $A$  é calculado por  $g^a \pmod{p}$ ,  $B$  por  $g^b \pmod{p}$  e a chave comum secreta é  $g^{a.b} \pmod{p}$ .
- ☐ b)  $A$  é calculado por  $g^a \pmod{p}$ ,  $B$  por  $g^b \pmod{p}$  e a chave comum secreta é  $A.B \pmod{p}$ .
- ☐ c)  $A$  é calculado por  $a^g \pmod{p}$ ,  $B$  por  $b^g \pmod{p}$  e a chave comum secreta é  $(a.b)^g \pmod{p}$ .
- ☐ d)  $A$  é calculado por  $a^g \pmod{p}$ ,  $B$  por  $b^g \pmod{p}$  e a chave comum secreta é  $A.B \pmod{p}$ .

**Questão 7**

Descreva detalhadamente o DES, explicando pontos fortes e vulnerabilidades.

**Questão 8**

Enuncie e demonstre o teorema de Euler.

**Questão 9**

Explique o que é uma assinatura digital e explique detalhadamente o uso do RSA para assinaturas digitais.