Respostas corretas

Departamento de Matemática **Faculdade de Ciências e Tecnologia — UNL**

Criptografia **05/06/2019** **Teste**

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 A máquina Enigma foi criada e usada

- [a] na antiga Grécia.
- [b] no período que engloba a segunda Guerra Mundial.
- [c] no período que engloba a primeira Guerra Mundial.
- [d] na segunda metade do século XX .

Questão 2 A máquina Enigma

- [a] usa a técnica de substituição, mas não de transposição.
- [b] não usa substituição nem transposição.
- [c] usa a técnica de transposição, mas não de substituição.
- [d] usa ambas as técnicas — substituição e transposição.

Questão 3 No DES cada S-box transforma

- [a] 8 bits em 4 bits.
- [b] 6 bits em 4 bits.
- [c] 4 bits em 6 bits.
- [d] 4 bits em 8 bits.

Questão 4 Para aplicar o Fast Powering Algorithm ao cálculo de $g^a \pmod{\mathrm{n}}$ precisamos conhecer a expansão binária de:

- [a] g.
- [b] n.
- [c] nenhuma das restantes opções.
- [d] a.

Questão 5 O problema do logaritmo discreto, formulado com base na equação $g^x \equiv h \pmod{\mathrm{p}}$, consiste em:

- [a] Conhecendo x, h, p determinar g.
- [b] Conhecendo g, h, p determinar x.
- [c] Conhecendo g, x, p determinar h.
- [d] Conhecendo g, x, h determinar p.

Questão 6 O teorema de Euler permite afirmar que, sendo p e q primos distintos,

$$a^{(p-1)\cdot(q-1)} \equiv 1 \pmod{\mathrm{p} \cdot \mathrm{q}}$$

qualquer que seja o a satisfazendo:

- [a] $\mathrm{mdc}\,(\mathrm{a}, \mathrm{p} \cdot \mathrm{q}) = 1$.
- [b] $\mathrm{mdc}\,(\mathrm{a}, (\mathrm{p}-1)\cdot(\mathrm{q}-1)) = 1$.
- [c] $\mathrm{mdc}\,(\mathrm{a}, \mathrm{p}) = 1$.
- [d] $\mathrm{mdc}\,(\mathrm{a}, \mathrm{p}-1) = 1$.

Note que mdc abrevia *máximo divisor comum.*

Questão 7
Enuncie e demonstre o teorema de Fermat.

Questão 8
Descreva detalhadamente o protocolo de Diffie-Hellman, explicando pontos fortes e vulnerabilidades.

Questão 9
Descreva detalhadamente o RSA, explicando em que problema é que assenta, pontos fortes e vulnerabilidades.