

**SEGURANÇA INFORMÁTICA E DAS COMUNICAÇÕES****TRABALHO DE INVESTIGAÇÃO**

Turma: LEIT41 / LEIT42 / LECC41

[50 Pontos]

Data da Distribuição: Semana 02

1º Semestre

Prazo de Entrega: Semana 03

**GENERALIDADES**

Este trabalho prático tem por finalidade refinar os conceitos analisados nas aulas teóricas/práticas e ainda abstrair o estudante.

**REGRAS E ESTRUTURA**

O trabalho deve ser apresentado nos seguintes moldes:

- a) Deve ter capa, onde estará indicado: **Nome da Instituição; Curso; Disciplina; Título do trabalho (em destaque) e a lista dos elementos integrantes no grupo (Nome) e data da conclusão.**
- b) Deve ser feito no computador com tamanho da letra recomendada de 12.
- c) O número de páginas **não** deve ultrapassar 10, incluindo a capa.
- d) Deve conter fontes bibliográficas, onde uma das obras deve ter sido editada.
- e) O Grupo deve ser constituído por 4 (Quatro) ou 5 (Cinco) Estudantes, no mínimo ou máximo.
- f) O trabalho será apresentado por qualquer estudante, membro do grupo a ser escolhido aleatoriamente.

**PRAZO DE ENTREGA**

O trabalho deverá ser entregue na semana indicada no cabeçalho do enunciado, na aula teórica da semana 3, sendo que o chefe de turma deverá recolher os trabalhos entregar ao Docente no início da aula do mesmo dia.

**TEMA**

Os temas a abordar por grupo são os algoritmos: DES e 3DES, IDEA, RC2 e RC4, AES, DSA, RSA e *Diffie-Hellman*.

**NOTA:** Ter em conta as características e as técnicas matemáticas de criptografia do recurso.

O Docente

-----  
(Emírcio Zeca Vieira)

*“Mentes poderosas têm objectivos, as demais têm desejos.”*