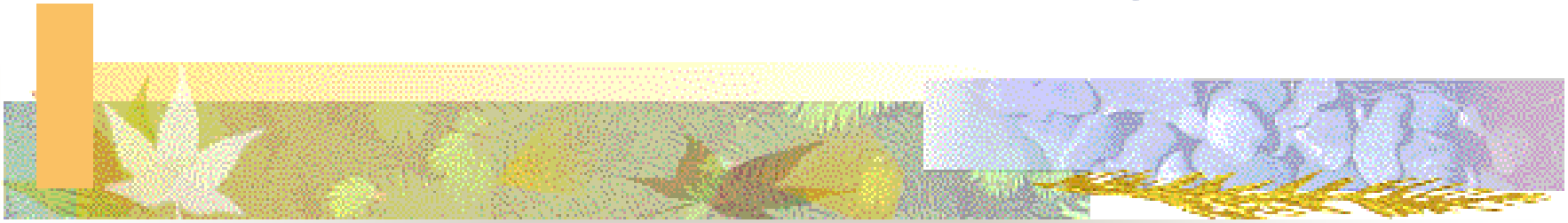
Introdução à Criptografia



Profa. Yeda

Aula 03 – Trabalho DES

TRABALHO DES

- GRUPOS: individual ou em dupla

- PRAZOS
  - ENTREGA: 17/10
  - APRESENTAÇÃO: para o professor em 17/10

DES

- Implementar, preferencialmente em linguagem C, o algoritmo DES para **cifragem**.
- Utilizar bibliotecas comerciais de criptografia para **decifrar** e validar seu código.
- **ATENÇÃO**: trabalhar diretamente com os bits. Não transformar byte em vetor de bits, conforme orientação em sala.
  - Perderá 2,0 pontos se transformar.

DES

- Requisitos
  - Receber 1 bloco de texto claro da entrada padrão no formato:
    - 8 caracteres de texto, ou 8 dígitos decimais equivalente ao ASCII do texto (0 a 255), ou 16 dígitos hexadecimais (escolher).
  - Apresentar em dígitos hexadecimais maiúsculos na saída padrão o resultado criptográfico:
    - Parcial, após permutação inicial, e após cada round.
    - Na apresentação dos round incluir a chave de round.
    - Final, o resultado criptográfico.