ACH2076 – Segurança da Informação

Exercício Programa

Valdinei Freire

valdinei.freire@usp.br

http://www.each.usp.br/valdinei

Escola de Artes, Ciências e Humanidades - USP

2025

Resumo

Conteúdo do Relatório:

1. Introdução
2. Teoria
3. Métodos Propostos
4. Resultados

Regras

- Grupo de 4 pessoas no máximo (comunicar Grupo ao professor para receber dados)
- Máximo de 6 páginas
- Deve-se seguir o formato de texto colocado no eDisciplinas
- Deve ser entregue Impresso até o dia 02/06/2025
- Arquivo Zip com resultados e códigos seguindo estrutura a ser disponibilizadas

Problema

- Textos abertos serão selecionados como trechos de um:
  - texto público e **disponível** no eDisciplinas
  - texto **não disponível** no eDisciplinas

- Cada grupo receberá textos (120 letras) para serem decriptografados e descoberta as chaves utilizadas com as seguintes cifras:
  1. Cifra Monoalfabética
  2. Cifra de Hill (2x2, 3x3, 4x4, 5x5)
  3. Cifra de Vigènere (20, 30, 40, 60)

- Espera-se soluções com duas restrições:
  - utilização do texto público para força bruta
  - utilização do conhecimento da língua (português) para construção de modelo de linguagem