

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

2023

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 07/07/2023
- ▶ 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
- ▶ Cada grupo receberá textos para serem decriptografados e descoberta as chaves utilizadas com as seguintes cifras:
 1. Cifra Monoalfabética
 2. Cifra de Hill
 3. Cifra de Vigenere
 4. Cifra de Vigenere com o tamanho do texto (dois textos fechados serão disponibilizados)
- ▶ Espera-se soluções com duas restrições:
 - ▶ utilização do texto público para força bruta
 - ▶ utilização do texto público para construção de modelo de linguagem