Lista 1 - Segurança da informação

1. Em um cenário de troca de informações sensíveis entre empresas, garantir a confidencialidade e a integridade dos dados é essencial para evitar vazamentos e acessos não autorizados. Seja a seguinte mensagem em um texto claro:
   “A aula será nas quintas”.
   Crie um algoritmo de criptografia usando as seguintes abordagens:
   A. Use a criptografia dos espiões (Cifra de Cézar) em que a cada letra do alfabeto é adicionada um valor (chave) aleatória para criar uma saída criptografada. Apresente um resumo da lógica e o código.
   B. Crie um algoritmo usando matrizes para criptografar a mensagem. Apresente um resumo da lógica e o código.
   C. Usando os códigos disponibilizados no Moodle, faça o processo de criptografia e descriptografia usando os algoritmos Hill Cipher e RSA. Apresente os resultados.

Instruções:

- Para os itens A e B devem ser criados também os algoritmos em Python ou outra linguagem de sua preferência.
- A mensagem deve ser criptografada usando a chave e depois descriptografada novamente.
- Apresente tanto o texto cifrado após a criptografia, quanto o texto claro após a descriptografia.
- Regra da Cifra de Cézar: Para cada letra do texto, somamos um número fixo (n) ao seu valor na ordem do alfabeto.
- Regra de criptografia com matrizes:
  - Transformar a mensagem em números. (por exemplo: A = 0, B = 1, ..., Z = 25)
  - Dividir a mensagem em blocos.
  - Cada bloco é um vetor coluna (o tamanho depende da matriz que você escolheu, tipo 2×2, 3×3...).
  - Escolher uma matriz chave K, que seja invertível (determinante diferente de 0).
  - Multiplicar a matriz chave K pelo vetor da mensagem.
  - O resultado é a mensagem criptografada.
  - Para descriptografar, você usa a inversa da matriz K