Prova 1: Segurança da Informação

Prof. Márcio Moretto Ribeiro

22 de outubro de 2025

Exercício 1: Calcule o tamanho do universo de chaves (isto é, o número de chaves possíveis) para:

1. a cifra de deslocamento;
2. a cifra de substituição;
3. a cifra de Vigenère, considerando que a chave é escolhida aleatoriamente e tem comprimento l.

Quais dessas cifras são seguras contra ataques de força bruta? Justifique sua resposta.

Exercício 2: Explique, utilizando um diagrama se desejar, o funcionamento do sistema *One-Time Pad*. Em que condições ele atinge sigilo perfeito? E o que acontece se uma mesma chave for reutilizada em duas mensagens diferentes?

Exercício 3: Compare uma cifra de fluxo moderna com o OTP. Indique uma vantagem prática e uma limitação de segurança do ponto de vista teórico.

Exercício 4: Descreva, com auxílio de um diagrama, o modo de operação **Ctr** (Contador) aplicado a uma cifra de bloco. Por que ele é considerado seguro contra ataques de texto escolhido?

Exercício 5: Alice e Bob compartilham uma chave secreta e usam uma cifra simétrica para criptografar mensagens. Eles desejam garantir não apenas a confidencialidade, mas também que a mensagem recebida não tenha sido modificada por um atacante.

1. Por que criptografar a mensagem não é suficiente para garantir integridade?

2. Cite uma forma correta de garantir integridade junto com a criptografia.