UNIVERSIDADE FEDERAL DO MARANHÃO	
Disciplina: Introdução à Criptografia	**Data:** 01/07/2025
Professor(a): [redacted]	
Discente: [redacted]	**Matrícula:**
Curso: Ciência da Computação	**Semestre:**
2ª avaliação	

Orientações gerais:

1- Sua avaliação consta de 7 questões, somando 14 pontos.

2- Escolham 5 das 7 questões para resolver.

1. (2 pontos) Por que a segurança dos algoritmos de criptografia não é comprometida pelo fato de seu funcionamento ser de conhecimento público?

2. (2 pontos) Quais são as vantagens do uso de sistemas criptográficos de curvas elípticas?

3. (2 pontos) Alice deseja enviar uma mensagem secreta para Bob através da criptografia quântica. Para isso segue o protocolo:

   1. Preparação da Chave: Alice inicia o processo criando uma chave secreta, que é uma sequência de bits representada por fótons. Ela utiliza um polarizador linear para polarizar cada fóton em um de quatro estados: horizontal, vertical, diagonal para direita ou diagonal para esquerda.
   2. Envio da Chave: Alice envia os fótons polarizados para Bob através de um canal de comunicação quântico.
   3. Verificação da Chave: Alice e Bob comparam as configurações dos divisores de feixe que utilizaram. Os fótons que foram direcionados para o divisor de feixe incorreto são descartados. A sequência restante de fótons, com polarização correta, representa a chave secreta compartilhada entre Alice e Bob.

   Um intruso presente no canal quântico, que tem as mesmas ferramentas de BOB deixará rastros segundo as leis da física quântica. Explique como Alice e Bob podem utilizar esses rastros para detectar a presença do intruso bisbilhotando a comunicação?

4. (2 pontos) Calcule a inversa de 7 módulo 31.

5. (2 pontos) Em criptografia de chave pública:

   a) O sigilo é obtido através da codificação com a chave privada do remetente e decifragem com a chave pública do destinatário.

   b) O sigilo é obtido através da codificação com a chave pública do destinatário e decifragem com a chave privada do destinatário.

   c) O sigilo é obtido através da codificação com a chave privada do destinatário e decifragem com a chave privada do remetente.

   d) Para assinar digitalmente uma mensagem codifica-se a mesma com a chave pública do remetente e esta é decifrada com a chave privada do destinatário.

   e) Para assinar digitalmente uma mensagem codifica-se a mesma com a chave pública do destinatário e esta é decifrada com a chave privada do destinatário.

6. (2 pontos) Considere os seguintes grupos:

- **Grupo 1** Conjunto de todos os números inteiros $\mathbb{Z}$, com a operação de adição $+$. Elementos: $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$; Operação: $+$; Identidade: Número inteiro 0 (identidade aditiva); Inverso: Para qualquer número inteiro, o inverso é -a.
- **Grupo 2** Conjunto de todos os números pares $2\mathbb{Z}$, com a operação de adição $+$. Elementos: $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$; Operação: Adição $+$; Identidade: Número inteiro 0 (identidade aditiva); Inverso: Para qualquer número par, o inverso é -a.

Marque a alternativa que identifique a função f que é um isomorfismo entre o Grupo 1 e o Grupo 2.

a) $f(x) = x + 1$

b) $f(x) = 2x$

c) $f(x) = x^2$

d) $f(x) = |x|$

e) $f(x) = \frac{x}{2}$

Isto é, a função f que mapeia um grupo para outro, preservando a identidade, a operação e a bijetividade (ou seja a função f tem inversa). Por exemplo: $f(a + b + c) = f(a) + f(b) + f(c)$, em que $a, b, c, (a + b + c)$ são elementos do Grupo 1 e $f(a), f(b), f(c), f(a + b + c)$ são elementos do Grupo 2.

7. (2 pontos) Claude Shannon demonstrou que cifras (algoritmos criptográficos) verdadeiramente indecifráveis existem e, de fato, já eram conhecidas há mais de 30 anos. Elas foram inventadas em 1918 por Gilbert Vernam, engenheiro da American Telephone and Telegraph, e pelo Major Joseph Mauborgne do Corpo de Transmissões do Exército dos Estados Unidos. Esses sistemas são chamados de "blocos de uso único (one-time pads)"ou "cifras de Vernam". Explique como o método de Vernam funciona.