Universidade Tecnológica Federal do Paraná (UTFPR)
Departamento Acadêmico de Informática (DAINF)

Introdução à Criptografia

Professor: Rodrigo Minetto

Lista de exercícios (escolha 3 para entregar)

---

1) Dada a curva $y^2 = x^3 + 2x + 3$ sobre $\mathbb{F}_5$, liste todos os pontos da curva.

---

2) Verifique se o ponto $(0, 2)$ pertence à curva $y^2 = x^3 + x + 1$ sobre $\mathbb{F}_7$.

---

3) Explique o que é o ponto no infinito $\mathcal{O}$ em uma curva elíptica.

---

4) O que significa dizer que um ponto tem ordem n na curva?

---

5) Calcule $3G$ na curva $y^2 = x^3 + 2x + 2$ sobre $\mathbb{F}_{17}$ para $G = (5, 1)$.

---

6) Descreva passo a passo o algoritmo ECIES usando:

- Curva $y^2 = x^3 + 2x + 2$ sobre $\mathbb{F}_{17}$
- $G = (5, 1)$, $k_B = 7$ (chave privada de Bob), $k = 3$ (aleatório de Alice)

---

7) Detalhe o uso do algoritmo de curvas elípticas em alguma aplicação da internet.