Bài tập

Bài 1 (Hệ mã Affine)

1. Hệ mã Affine có khoá $k = (a, b)$ với $a, b \in \mathbb{Z}_{26}$. Hàm mã hoá biến đổi thông điệp x thành bản mã y như sau:

   $$y = a \cdot x + b \mod 26$$

   Hàm giải mã là gì?
2. Hãy cài đặt hàm mã hoá và giải mã bằng C/C++ hoặc một ngôn ngữ lập trình khác.

Bài 2

Nghịch đảo của 5 trong $\mathbb{Z}_{11}$, $\mathbb{Z}_{12}$, và $\mathbb{Z}_{13}$ là gì?

Bài 3

Hãy tính giá trị của x thoả mãn phương trình dưới đây mà không dùng máy tính:

- $x = 3^2 \mod 13$
- $x = 7^2 \mod 13$
- $x = 3^{10} \mod 13$
- $x = 7^{100} \mod 13$
- $x = \sqrt{3} \mod 13$
- $7^x = 11 \mod 13$