NHẬP MÔN MÃ HÓA MẬT MÃ

TUẦN 2: ĐỒNG DƯ VÀ MỘT SỐ TÍNH CHẤT

Ngày 14 tháng 10 năm 2024

Bài 1. Giải các phương trình sau.

a) $6x \equiv 4 \pmod 8$

b) $5x \equiv 8 \pmod{10}$

c) $8x \equiv 5 \pmod{13}$

d) $6x \equiv 7 \pmod{23}$

Bài 2. Áp dụng định lí thặng dư Trung Hoa giải các hệ phương trình đồng dư sau:

a) $\begin{cases} x \equiv 4 \pmod{11} \\ x \equiv 3 \pmod{17} \end{cases}$

b) $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$

c) $\begin{cases} x \equiv 3 \pmod{12} \\ x \equiv 4 \pmod{13} \\ x \equiv 5 \pmod{17} \end{cases}$

Bài 3. Cho số nguyên tố p, số nguyên b được gọi là nghịch đảo của a modulo p nếu thỏa mãn $ab \equiv 1 \pmod p$. Hãy tìm nghịch đảo của a (modulo p) trong các trường hợp sau bằng hai cách: Cách thứ nhất dùng thuật toán Euclide mở rộng, cách thứ hai sử dụng định lý Fermat nhỏ.

a) $a = 11$ và $p = 47$.

b) $a = 345$ và $p = 587$.

c) $a = 78467$ và $p = 104801$.

Bài 4. Bob và Alice sử dụng môt hệ thống mật mã trong đó khóa riêng của họ là một số nguyên tố (lớn) k, bản rõ (plaintexts) và bản mã (ciphertexts) là các số nguyên. Bob mã hóa thông điệp m bằng cách tính tích $c = km$. Eve chặn được hai bản mã sau:

$$c_1 = 12849217045006222 \text{ và } c_2 = 6485880443666222.$$

Hãy sử dụng giải thuật tìm ước chung lớn nhất để tìm khóa (private key) của Alice và Bob.