ĐỀ THI PHƯƠNG PHÁP TOÁN

(120 phút – được phép dùng tài liệu)

Bài 1.

a) Tập hợp U($\mathbb{Z}_{135}$) có bao nhiêu phần tử? Hãy liệt kê 5 phần tử lớn hơn 10 của tập này.

b) Những cặp số nguyên dương (***E***, ***D***) thỏa mãn $(\mathbf{a}^{E})^{D} = \mathbf{a}$ với mọi $\mathbf{a} \in$ U($\mathbb{Z}_{135}$) phải thỏa mãn điều kiện gì?

c) Hãy chỉ ra 3 cặp số nguyên dương (***E***, ***D***) với $E < D$ mà ta có thể mã hóa các phần tử của U($\mathbb{Z}_{135}$) bằng ***E*** để có các bản mã và giải mã các bản mã bằng ***D*** để có các bản rõ.

Bài 2.

a) Trong vành đa thức $\mathbb{Z}_9$[x], hãy đơn giản đa thức $f(x) = \left(\bar{3}x^2 + \bar{1}\right)^3$.

b) Cho ví dụ về một vài đa thức trong U($\mathbb{Z}_9$[x]).

Bài 3. Xét trường **GF**(2^5) có 32 phần tử.

a) Trường này có thể sinh ra bởi một đa thức bất khả quy bậc mấy trong $\mathbb{Z}_2$[x] ?

b) Trình bày mô hình mã hóa công khai có thể thực hiện được nhờ phép nhân trong **GF**(2^5).

c) Những cặp số nguyên dương (***E***, ***D***) thỏa mãn $(\mathbf{a}^{E})^{D} = \mathbf{a}$ với mọi $\mathbf{a} \in$ **GF**(2^5) phải thỏa mãn điều kiện gì?

d) Tìm 3 cặp số nguyên dương (***E***, ***D***) như điều kiện trong câu c) nói trên.

HẾT