

Bài kiểm tra giữa kỳ (số 2)

Câu 1: Cho hệ mã Knapsack có $A' = \{2, 7, 11, 21, 42, 89, 180, 354\}$, $M=881$ $u=588$

- Hãy tìm các khóa của hệ mã hóa trên
- Mã hóa và giải mã bản rõ $M=a$

Câu 2: Cho $N=1517$. Hãy tính $13^{1435} \bmod N$

Câu 3: Bob muốn liên lạc với Alice thông qua hệ mật mã RSA, để thực hiện Bob phải xây dựng khóa công khai và khóa bí mật và Bob chọn được hai số nguyên tố $p=29$, $q=43$.

- Nếu Bob chọn $e=11$ cho bộ khóa công khai (e,n) thì giá trị có phù hợp không? Tại sao?
- Anh (chị) hãy tìm ra khóa công khai và khóa bí mật cho Bob?
- Mã hóa $M=16$, sau đó giải mã.