Bài 2: Mã hóa họ tên bằng giải thuật RSA biết p=23, q=41, e=13. Trong đó các kí tự chữ cái được đánh theo số tương ứng dựa theo bảng mã ASCII

* n= p\*q = 23\*41 = 943
* φ(n) = (p-1)(q-1) = 880
* Gcd(e, φ(n))=1
* Public key: PU = {e,n} = {13,943}
* e × d = 1 (mod φ(n))
* Private key: d =677

Vậy với tên:”dang xuan cuong” sẽ có cipher text: 133 # 826 # 071 # 661 # 196 # 044 # 878 # 826 # 071 # 196 # 227 # 878 # 766 # 071 # 661

Bài 3. Với p=5, q=7, e=5, các chữ cái (viết hoa) được đánh số từ 0 trở đi, giả sử bạn nhận được một thông điệp: 17 19 7 9 0 12 24. Hãy giải mã thông điệp này. Từ các dữ liệu đã biết, thực hiện mã hóa thông điệp “BAO MAT THONG TIN”

* d= 5
* 17 19 7 9 0 12 24 sau khi được giải mã sẽ thành: 12 24 7 4 0 17 19 => thành chữ cái là m y h e a r t
* BAO MAT THONG TIN được mã hóa thành: 1, 0, 14, 17, 0, 24, 24, 7, 14, 13, 6, 24, 8, 13