3. Thuật toán RSA - Bài toán 2:

Giả sử An chọn các giá trị p = 43 , q = 47 , e = 67 để tạo cặp khóa.

Hãy cho biết

1. Khóa công khai của An: PU = {e, n} ={67,2021}

n=p\*q=2021

phi(n)=42\*46=1932

e=67

d=67^-1 mod 1932

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| q | A1 | A2 | A3 | B1 | B2 | B3 |  |  |
| - | 1 | 0 | 1932 | 0 | 1 | 67 |  |  |
| 28 | 0 | 1 | 67 | 1 | -28 | 56 |  |  |
| 1 | 1 | -28 | 56 | -1 | 29 | 11 |  |  |
| 5 | -1 | 29 | 11 |  | -173 | 1 |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

D=-173

b) Cách An tạo ra khóa riêng: PR = {d, n} = {-173,2021}

c) Cách người gửi (Ba) mã hóa thông điệp M = 59 để gửi cho An:

C =M^e mod n=59^67 mod 2021=1896

//59^67 mod 2021=[(59^33 mod 2021)^2\*59] mod 2021=

d) Cách An giải mã bản mã C: e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.