Thuật toán RSA - Bài toán 1

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} =

Tính n=p\*q=2021

Phi(n)=42\*46=1932

Chon e =67

gcd(e, 1200)=1=>1<e<1932=>e=67

tinh d=e^-1(mod Phi(n))=67^-1 mod 1200

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| q | A1 | A2 | A3 | B1 | B2 | B3 |  |
| - | 1 | 0 | 1932 | 0 | 1 | 67 |  |
| 28 | 0 | 1 | 67 | 1 | -28 | 61 |  |
| 1 | 1 | -28 | 61 | -1 | 29 | 6 |  |
| 10 | -1 | 29 | 6 | 11 | -318 | 1 |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

d=-318

PU = {e, n} ={67,2021}

b) cách An tạo ra khóa riêng: PR = {d, n} = {-318,2021}

c) Cách An tạo bản mã hóa thông điệp M = 59: C =

C=59^67 mod 2021=1896

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

Vạy C=1896

d) Hãy cho biết cách người nhận giải mã bản mã C:

M=1896^-318 mod 2021

e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.