1. RSA

- Chọn 2 số nguyên tố p, q. Tính N=p\*q

- Tính

- Chọn e sao cho gcd(e,) = 1

- Tìm d, với d là nghịch dảo của e theo module : e-1 \* d = 1 mod

- Khóa công khai: KU = (e, N)

- Khóa bí mật: KR = (d, N)

- Mã hóa: C = Me mod N

- Giải mã: M = Cd mod N

Ví dụ: p,q >50 ; p>q+50; e: ngày sinh; M=123

Chọn: p = 107, q = 53, e = 10

- N = 53\*107 = 5671

-

- e = 10 , gcd(10,5512) = 2 loại

- e = 9 , gcd(9,5512) = 1 => Chọn e =9

- d-1 \*9 = 1 mod 5512 => d = 1225. Vì 9\*1225 = 5512\*2 + 1

5512\*1/9

(5512\*2)+1 chia hết cho 9 thì đấy là nghịch đảo

- Khóa công khai: KU = (9, 5671)

- Khóa bí mật: KR = (1225, 5671)

- Mã hóa: C=1239 mod 5671

* (1234 mod 5671)2 \*123 mod 5671 =50812 mod 5671 =250
* (1232 mod 5671)2 mod 5671 =37872 mod 5671=5081
* 1232 mod 5671 = 3787

- Giải mã: M = 2501225 mod 5671

* (250612 mod 5671)2 \* 250 mod 5671 =35662\*250 mod 5671=123
* (250306 mod 5671 )2 mod 5617=17912 mod 5671=3566
* (250153 mod 5671)2 mod 5671 =47952 mod 5671=1791
* (25076 mod 5671)2 \* 250 mod 5671 =492\*250 mod 5671=4795
* (25038 mod 5671)2 mod 5671 =56642 mod 5671=49
* (25019 mod 5671)2 mod 5671 =20432 mod 5671=5664
* (2509 mod 5671)2 \* 250 mod 5671 =28462\*250 mod 5671=2043
* (2504 mod 5671)2 \* 250 mod 5671 =28192\*250 mod 5671=2846
* (2502 mod 5671)2 mod 5671 =1192 mod 5671=2819
* 2502 mod 5671 =119

Thực hiện thuật toán RSA để mã hóa dữ liệu

M = 123 (được bản mã C), và giải mã C (để có M’) so sánh với M

Yêu cầu`;

- P, Q: là 2 số nguyên tố. Trong đó P là số 2 chữ số, Q là số 3 chữ số > 150

- E là số lấy từ ngày sinh của SV

- Thực hiện đầy đủ các thuật toán, bước tính: Euclid, Euclide mở rộng, và lũy thừa modulo

P = 29;

Q = 157;

E = 27;

N = P\*Q = 4553;

e = 27 , gcd(27,) = 3 loại

e = 25, gcd(25, 4368) = 1 lấy

Khóa công khai: KU = (25, 4553)

Khóa bí mật: KR = (7513, 4553)

Mã hóa: C=12325 mod 4553

(12312 mod 4553)2 \* 123 mod 4553

- Mã hóa: C=1239 mod 5671

* (1234 mod 5671)2 \*123 mod 5671 =50812 mod 5671 =250
* (1232 mod 5671)2 mod 5671 =37872 mod 5671=5081
* 1232 mod 5671 = 3787

P = 11;

Q = 157;

E = 27;

N = P\*Q = 1727;

e = 27 , gcd(27,) = 1 lấy

Khóa công khai: KU = (27, 1727)

Khóa bí mật: KR = (, 1991)

2. Trao đổi khóa Diffie – Hellman

VD: Cho các giá trị dùng chung: q=353 , a=3

|  |  |
| --- | --- |
| Người A | Người B |
| 1. Chọn khóa riêng: XA=97 | 1. Chọn khóa riêng: XB=233 |
| 2. Tính khóa công khai  YA= 397 mod 353 = 40 | 2.Tính khóa công khai  YB= 3233 mod 353 = 248 |
| Hai người A và B trao đổi giá trị khóa công khai với nhau | |
| 3. Tính khóa bí mật chung  KAB=24897 mod 353 = 160 | 3. Tính khóa bí mật chung  KAB=40233 mod 353 = 160 |