**Môn: An toàn bảo mật thông tin**

**Nhóm: 3**

**Sinh viên: Vũ Bảo Lâm**

**BÀI 1:**

TÍNH LŨY THỪA MODULO 𝒃 = 𝒂 𝒎 𝒎𝒐𝒅 𝒏 BẰNG CÁCH HẠ BẬC LŨY THỪA

Input: a = 397; m = 6329; n = 6329 Tìm Output: b =

**Giải:**

B1: phân tích 6329 = 4096 + 2048 + 128 + 32 + 16 + 8 + 1

= 212 + 211 + 27 + 25 + 24 +23 + 20

B2: 3971 ≡ 397 (mod 6329)

3972 ≡ 5713 (mod 6329)

3974 ≡ 6045 (mod 6329)

3978 ≡ 4708 (mod 6329)

39716 ≡ 1106 (mod 6329)

39732 ≡ 1739 (mod 6329)

39764 ≡ 5188 (mod 6329)

397128 ≡ 4436 (mod 6329)

397256 ≡ 1235 (mod 6329)

397512 ≡ 6265 (mod 6329)

3971024 ≡ 4096 (mod 6329)

3972048 ≡ 5366 (mod 6329)

3974096 ≡ 3335 (mod 6329)

B3: Vậy 3976329 mod 6329 = 3335 \* 5366 \* 4436 \* 1739 \* 1106 \* 4708 \* 397≡397 (mod 6329 )

**BÀI 2:** TÌM NGHỊCH ĐẢO 𝒙 = 𝒂 −𝟏 𝒎𝒐𝒅 𝒏 THEO ĐỊNH NGHĨA VÀ THUẬT TOÁN EUCLID – MỞ RỘNG Input: a = 1885; n = 6563

Tìm Output: x =

**Giải:**

x = 1885-1 mod 6563

**CÁCH 1: THEO ĐỊNH NGHĨA**

B1: Tính gcd (6563,1885)

1. 6563 = 1885 \* 3 + 908
2. 1885 = 908 \* 2 + 69
3. 908 = 69 \* 13 + 11
4. 69 = 11\* 6 + 3
5. 11 = 3 \* 3 + 2
6. 3 = 2 \* 1 + 1
7. 2 = 2 \* 1 + 0

B2: Phân tích tính phần dư:

1. 908 = 6563 – 1885 \* 3
2. 1885 = (6563 – 1885 \* 3) \* 2 + 69

* 69 = 7 \* 1885 + (-2) \* 6563

1. 6563 – 1885 \* 3 = [7 \* 1885 + (-2) \* 6563] \* 13 + 11

* 11 = (-94) \* 1885 + 27 \* 6563

1. 7 \* 1885 + (-2) \* 6563 = [(-94) \* 1885 + 27 \* 6563] \* 6 + 3

* 3 = 571 \* 1885 + (-164) \* 6563

1. (-94) \* 1885 + 27 \* 6563 = [571 \* 1885 + (-164) \* 6563] \* 3 + 2

* 2 = (-1807) \* 1885 + 519 \* 6563

1. 571 \* 1885 + (-164) \* 6563 = (-1807) \* 1885 + 519 \* 6563 + 1

* 1 = 2378 \* 1885 + (-683) \* 6563

B3: Kết luận x= 2378 vì 1885 \* 2378 ≡ 1 (mod 6563)

**CÁCH 2: THEO THUẬT TOÁN EUCLID – MỞ RỘNG:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 6563 | 0 | 1 | 1885 |
| A3/B3 = 3 | 0(=B1) | 1(=B2) | 1885(=B3) | 1 | -3 | 908 |
| 1885/908 = 2 | 1 | -3 | 908 | 0 - 2\*1 = -2 | 1 - 2\*(-3) = 7 | 1885 - 2\*908=69 |
| 908/69 = 13 | -2 | 7 | 69 | 1 – 13\*(-2) = 27 | (-3) - 13\*7 = -94 | 908 - 13\*69=11 |
| 69/11 = 6 | 27 | -94 | 11 | (-2) - 6\*27 = -164 | 7 - 6\*(-94) = 571 | 69 - 6\*11 = 3 |
| 11/3 = 3 | -164 | 571 | 3 | 27 – 3\*(-164) = 519 | -94 -3\*571 = -1807 | 11 – 3\*3 = 2 |
| 3/2 = 1 | 519 | -1807 | 2 | -164 – 519= -683 | 571 +1807 = 2378 | 3 – 2 = 1 |

B2 = 2378 là kết quả của bài toán.

**BÀI 3:** SỬ DỤNG ĐỊNH LÝ FERMAT ĐỂ TÍNH LŨY THỪA MODULO 𝒃 = 𝒂 𝒎 𝒎𝒐𝒅 𝒏

Input: a = 439; m = 760; n = 6269

Tìm Output: b =

**Giải:**

B1: Phân tích 760 = 512 + 128 + 64 + 32 + 16 + 8

= 29 + 27 + 26 + 25 +24 + 23

B2: 4398 ≡ 2365 (mod 6269)

43916 ≡ 1277 (mod 6269)

43932 ≡ 789 (mod 6269)

43964 ≡ 1890 (mod 6269)

439128 ≡ 5039 (mod 6269)

439512 ≡ 1045 (mod 6269)

B3: Vậy 439760 mod 6269 = 2365 \* 1277 \* 789 \* 1890 \* 5039 \* 1045 (mod 6269)

= 2373 (mod 6269)

**BÀI 4:** TÍNH GIÁ TRỊ HÀM EULER φ(n). Input: n = 3992 Tìm Output: φ(n) =

**Giải:**

φ(3992) = φ(23 \* 499)

= φ(23) \* φ(499)

= (23 – 22) \* (499 – 1)

= 4 \* 498

= 1992

**BÀI 5:** SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO 𝒃 = 𝒂 𝒎 𝒎𝒐𝒅 𝒏

Input: a = 23; m = 3885; n = 395

Tìm Output: b =

**Giải:**

B1: Tìm φ(395) = φ(5) \* φ(79) = 4 \* 78 = 312

Ta có: gcd (a, n) = gcd (23,395) = 1.

Theo định lý aφ(n) ≡ 1 (mod n) => 23312 ≡ 1 (mod 395)

B2: 3885 = 312 \* 12 + 141

* 233885 = 23141 mod 395

B3:

|  |  |
| --- | --- |
| 141 = 70 \* 2 + 1 | 23141 = (2370)2 \* 23 = 3392 \* 23 mod 395= 238 |
| 70 = 35 \* 2 | 2370 = (2335)2 = 2922 mod 395= 339 |
| 35 = 17 \* 2 + 1 | 2335 = (2317)2 \* 23 = 213 \* 23 mod 395= 292 |
| 17 = 8 \* 2 + 1 | 2317 = (238)2 \* 23 = 371 \* 23 mod 395= 213 |
| 8 = 4 \* 2 | 238 = (234)2 = 1812 mod 395 = 371 |
| 4 = 2 \* 2 | 234 = (232)2 = 1342 mod 395 = 181 |
| 2 = 1 \* 2 | 232 = 232 mod 395 = 134 |
| 1 = 1 | 231 = 231 mod 395 = 23 |

Vậy b = 238