Tính modulo

1. Tính lũy thừa MODULO b = a^m mod n bằng cách hạ bậc lũy thừa

Input: a = 499, m = 6337, n = 6337

Tìm output =

1. Tìm nghịch đảo x = a^-1 mod n theo định nghĩa và thuật toán euclid - mở rộng

Input: a = 281, n = 6577

Tìm output x =

1. Sử dụng định lý fermat để tính lũy thừa MODULO b = a^m mod n

Input: a = 281, m = 764, n = 6967

Tìm ouput: b =

1. Tính giá trị hàm EULEN (n)

Input: n = 2863

Tìm output: (n) =

1. Sử dụng định lý EULER để tính lũy thừa MODULO b = a^m mod n

Input a = 27, m = 2201, n = 5400

Tìm output: b =

1. Sử dụng định lý số dư trung hoa để tính lúy thừa modulo b = a^k mod n

Input a = 101, k = 76, n = 49913

Tìm output: b =

1. Sử dụng định lý số dư trong trung hoa để giải hệ phương trình modulo:

- x mod m1 = a1

- x mod m2 = a2

- x mod m3 = a3

Input: m1 = 11, m2 = 13, m3 = 17, a1 = 6, a2 = 2, a3 = 4

Tìm output: x =

1. Kiểm tra só nguyên a có là một nguyên căn nguyên thủy của số nguyên n?

Input: a = 11, n = 293

Tìm output: a có là nguyên căn nguyên thủy của n không?

1. Tìm logarithm rời rạc của số b với cơ số a(mod n), k = loga b(mod n)

Input: a = 3, b = 8, n = 19

Tìm output: k =

1. Tìm các biểu thức modulo cơ bản

A1 = (a^x + b^y) mod n A2 = (a^x - b^y) mod n

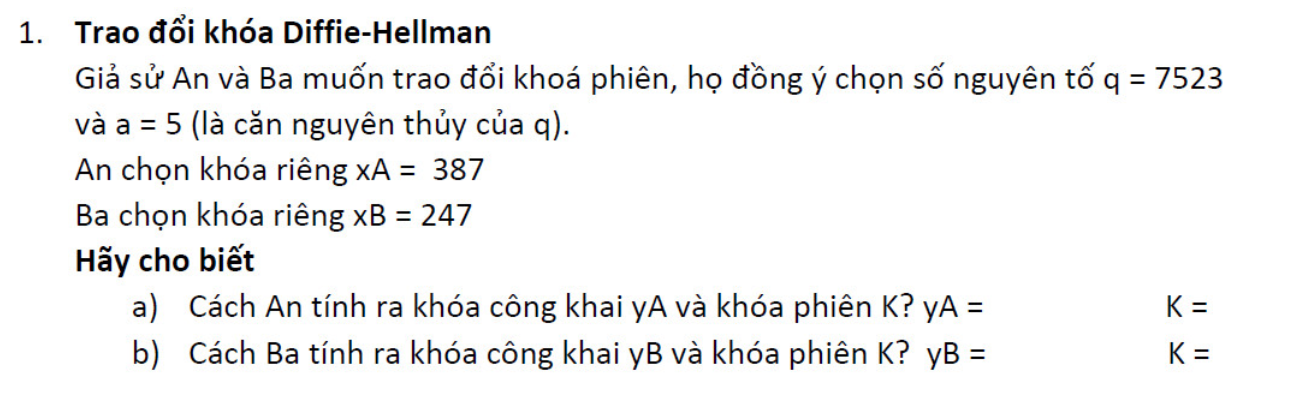
A3 = (a^x \* b^y) mod n A4 = (b^y^-1) mod n

A5 = (a^x / b^y) mod n

Input: a = 83, b=17, x = 354, y = 314, n = 241

Tìm output: A1, A2, A3, A4, A5

Mã hóa khóa công khai



Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated