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 =

5. SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO

𝒃 = 𝒂𝒎 𝒎𝒐𝒅 𝒏

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

Tìm Output: b =

b = 233885 mod 395

Ta có 23 và 395 là 2 số nguyên tố cùng nhau:

=> 23ɸ(395) mod 395 = 1

ɸ(395) = ɸ(5\*79) =4\*78 = 312

233885 mod 395 = 23312\*12+141 mod 395 = 23141 mod 395

a=23,m=141,n=395

23^141 mod 395=[(23^70 mod 395)^2\*23] mod 395=238

23^70 mod 395=[(23^35 mod 395)^2] mod 395=339

23^35 mod 395=[(23^17 mod 395)^2\*23] mod 395=292

23^17 mod 395=[(23^8 mod 395)^2\*23] mod 395=213

23^8 mod 395=[(23^4 mod 395)^2] mod 395=371

23^4 mod 395=[(23^2 mod 395)^2] mod 395=181

23^2 mod 395=[(23 mod 395)^2] mod 395=134

23 mod 395=23

b = 238