Tiến hành quá trình mã hoá, giải mã, ký và kiểm thử chữ ký trên hệ mật ElGamal với độ dài khoá 1024 bit

1. Qúa trình thiết lập bộ khoá

Thiết lập bộ khoá

Chọn ra số nguyên tố p có độ dài 1024 bit:

Ta có p = 125231265809222726728970019650121774493804896225910365064792226166487353775797796931785455604206755181334802469096700848527566877075439493995934841191174320575079010141682878332699335231415621518260793785612469656320824175699573521719164428362311624814657198994059191184783879937626200052642418234199576531791

Chọn ra alpha là một phần tử nguyên thuỷ theo modp, ta có alpha = 2

Chọn một số nguyên dương a bất kỳ nhỏ hơn p:

Ta có a = 46618656863102583631031885657269377328636014729529324148704685933048017132453841344367025981464152050262203379654240804616589471315071031099702903185259157513990215177510292145577560140561658243782113470915539149632026013994709026147739819371758330100632115139694434123887601678623349054154527200964949573816

Tính beta

Ta có beta = 79385606786239845289527287946591476180343117545267375117610117516945575444614804807267132355174077781443381922366530025785996601825908226566443846571146143267741834544383599669525768146170702917717523410844335233386529568354504963342118973310051836313091054500628488822395742975498253047718404865658658490963

Như vậy, ta đã thiết lập bộ khoá K gồm khoá công khai K' và khoá bí mật K''

Trong đó:

Khoá công khai K' = (p, alpha, beta)

Khoá bí mật K'' = a

2. Qúa trình mã hoá bản tin

Ta có bản tin với nội dung:chaomunghaimuoinamthanhlaptruongdhcn

Ta tiến hành chọn ngẫu nhiên k thuộc Z\_p\*

Ta có k = 29102002

Ta có bảng mã C = (y1, y2) = (55685590495113922505415159308927302383302679749356978701134673702337356627789595617787122603464382801867820630317842281940887562356633333947364317328081325186819395630999843041693628344390457468291200705808155453407825045222083447940283025367913779325052344562390372512119622062062722702779359598132509181357,102700708495243894627009691747507165207910876912895768275298895791552614645737697207427376934443603695147389106135750177582002591409875286048679274167269852225650703450455737148780938758797907999557365957796346900623994565312729724589696988613021919689009810268925263259395881203670287103590058484271760609668)

3. Tiến hành giải mã

Gía trị của d = 75875858014824466484081173862595213692501319439029

Bản tin được giải mã có nội dung như sau:chaomunghaimuoinamthanhlaptruongdhcn

Quá trình mã hoá và giải mã tiến hành thành công!

Qúa trình ký và kiểm thử chữ ký trên hệ mật ElGamal

1. Qúa trình ký

k và p - 1 không phải là số nguyên tố cùng nhau.

k và p - 1 không phải là số nguyên tố cùng nhau.

k và p - 1 không phải là số nguyên tố cùng nhau.

k và p - 1 không phải là số nguyên tố cùng nhau.

delta:-603228678120103672300397573090332954293305868822769201330408794286110810526503001095641439162598328254091124358624682056737290356763606552654997562608478449963250108524083620308869229490847857177026485236072172057427962016275739561515244569996163996172431257057627031999732631257131596311940005104361553959

Ta có hàm kỳ gồm bộ hai giá trị (gamma,delta) = 9156146112785755984381240350807033021094701203157015928351521471554879033675395393084307370861460593851060682304512117818234835894242697714704500529739410393207132929222726213950788310424097125960869707241061914671886203817832569859848067115825537271029577107813723308130382472053354863545699437301378733057,124628037131102623056669622077031441539511590357087595863461817372201242965271293930689814165044156853080711344738076166470829586718675887443279843628565842125115760033158794712390466001924773661083767300376397484263396213683297782157649183792315460818484767737001564152784147306369068456330478229095214977831)

2. Tiến hành thực hiện thuật toán kiểm thử chữ ký

Xác thực chữ ký thành công!