

## BÁO CÁO ASSIGNMENT

**Môn học:** Mật mã học

**Chủ đề:** Trao đổi khóa

*GVHD: TS. Nguyễn Ngọc Tự*

**1. THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT219.N21.ANTT

STT	Họ và tên	MSSV	Email
1	Đinh Bùi Huy Phương	21520090	21520090@gm.uit.edu.vn
2	Nguyễn Thị Minh Châu	21520645	21520645@gm.uit.edu.vn

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

# BÁO CÁO CHI TIẾT

Thực hiện trao đổi khóa ECDH sử dụng curve384:

- Bên A: HP (Huy Phương)
- Bên B: MC (Minh Châu)

Các bước thực hiện:

- Bước 1: Khởi tạo điểm G dựa trên curve384 với các thông số p, a, b, G(x, y), h nhập thủ công. Với các giá trị:
  - $p = \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF 00000000 00000000 FFFFFFFF}$
  - $a = \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF 00000000 00000000 FFFFFFFC}$
  - $b = \text{B3312FA7 E23EE7E4 988E056B E3F82D19 181D9C6E FE814112 0314088F 5013875A C656398D 8A2ED19D 2A85C8ED D3EC2AEF}$
  - $G(x) = \text{AA87CA22 BE8B0537 8EB1C71E F320AD74 6E1D3B62 8BA79B98 59F741E0 82542A38 5502F25D BF55296C 3A545E38 72760AB7}$
  - $G(y) = \text{3617DE4A 96262C6F 5D9E98BF 9292DC29 F8F41DBD 289A147C E9DA3113 B5F0B8C0 0A60B1CE 1D7E819D 7A431D7C 90EA0E5F}$
  - $n = \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF C7634D81 F4372DDF 581A0DB2 48B0A77A ECEC196A CCC52973}$
  - $h = 01$  (hex)
- Bước 2: Mỗi bên tạo một secret number (PrivateKey) và giữ kín.
  - Secret number của MC  
 $\text{priKeyHP} = 23402$
- Bước 3: Tạo publicKey từ privateKey và điểm G, có cặp khóa:
  - $\text{pubKeyMC} = \text{priKeyMC} * G$
  - $\text{pubKeyMCx} = 297809578695107442039333767591910921420954148286598492982353149 55179536830386915447870136315155556027711362950288460$
  - $\text{pubKeyMCy} = 350579147439838646019520111236246360138483016171340248574325177 00701973087090678133644076933956030081272064206273058$
- Bước 4: Trao đổi publicKey với nhau qua giao thức TCP (telnet) thu được Public của parner (HP)
  - $\text{pubKeyHPx} = 15823354386728477868059489378147753930914124451780717471 22943088740852951449025986508069515743416084440203761275 2985$
  - $\text{pubKeyHPy} = 14249003402157307118910319908225993651282273477814127020$

647122530930973296805790540669926590590574050849654965310718

- Bước 5: Tính toán sharedKey:  $\text{shareKey} = \text{pubKeyHP} * \text{priKeyMC}$ 
  - o  $\text{shareKey}_x =$   
122805284214342150742625629310024558306276935592317113319934756  
80898579972608604496251987160055219324448188061532666
  - o  $\text{shareKey}_y =$   
135432322148869622355156958045922818626543243721884265052354421  
07926566262103731145351157228655714531454352281832382
- Hình ảnh HP và MC trao đổi khóa thông qua giao thức TCP

```

PS C:\Users\admin> telnet 192.168.71.45 8080
Trying 192.168.71.45...
Connected to 192.168.71.45.
Escape character is '^]'.
192.168.71.45:65470: chào bạn, mình là Huy Phuong
he xò lo he xò lỉ toi là Minh Chau dei
192.168.71.45:65470: t???i m???nh trao ?????i kh??a nhaaa
what r u talkin a bout
192.168.71.45:65470: let's exchange key
yesssss let's do it babi
192.168.71.45:65470: here I go
192.168.71.45:65470: I1x=15823354386728477868059489378147753930914124451780717471229430887408529514490259865080695157434160844402037612752985.
192.168.71.45:65470: I1y=14249003402157307118910319908225993651282273477814127020647122530930973296805790540669926590590574050849654965310718.
okay babi
wait me a bit
I1x=340604609775026290515924875381875524054001971128053806780728618138828170253731233964679096191633778507386758902411891I1y=32768261101485250383294338930189
98129558877592873784943989441489344984752072031599318265799766526291846326225380514192.168.71.45:65470: okay, I got it
yeah me tooo
192.168.71.45:65470: I suppose that we calculated the same key
yes ofc we r destiny!!!!
192.168.71.45:65470: yassssss
192.168.71.45:65470: that's it, bye bye
okay go home
192.168.71.45:65470: go home cook rice
go home and buy milk tea
i dont have mone192.168.71.45:65470: get me one from Phuc Long
Phuc Long is closed already
  
```

- Hình ảnh sau khi chạy chương trình:

```

PS C:\Users\admin\Downloads\Lab02\Lab02> .\test
Cofactor h=1.
Subgroup Order n=39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643.
Gx=26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087.
Gy=8325710961489029985546751289520108179287853048861315594709205902480503199884419224438643760392947333078086511627871.
Coefficient a=39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643.
Coefficient b=27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575.
secret value=230402.
Public key to share
I1x=34060460977502629051592487538187552405400197112805380678072861813882817025373123396467909619163377850738675890241189.
I1y=3276826110148525038329433893010998129558877592873784943989441489344984752072031599318265799766526291846326225380514.
Public key received
Tx=15823354386728477868059489378147753930914124451780717471229430887408529514490259865080695157434160844402037612752985.
Ty=14249003402157307118910319908225993651282273477814127020647122530930973296805790540669926590590574050849654965310718.
Share key
Kx=11912442316819441005352778373982772749444225636741611971796365186833593158723637066821924310847880631577426811983144.
Ky=14032708525761334941882985172879537776555043395103016908739112109212591618697926001036914126451475563670013203347501.
PS C:\Users\admin\Downloads\Lab02\Lab02>
  
```

