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 = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF 00000000 00000000 FFFFFFFF
    - a = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF 00000000 00000000 FFFFFFFC
    - b = B3312FA7 E23EE7E4 988E056B E3F82D19 181D9C6E FE814112 0314088F 5013875A C656398D 8A2ED19D 2A85C8ED D3EC2AEF
    - G(x) = AA87CA22 BE8B0537 8EB1C71E F320AD74 6E1D3B62 8BA79B98 59F741E0 82542A38 5502F25D BF55296C 3A545E38 72760AB7
    - G(y) = 3617DE4A 96262C6F 5D9E98BF 9292DC29 F8F41DBD 289A147C E9DA3113 B5F0B8C0 0A60B1CE 1D7E819D 7A431D7C 90EA0E5F
    - n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF C7634D81 F4372DDF 581A0DB2 48B0A77A ECEC196A CCC52973
    - h = 01 (hex)

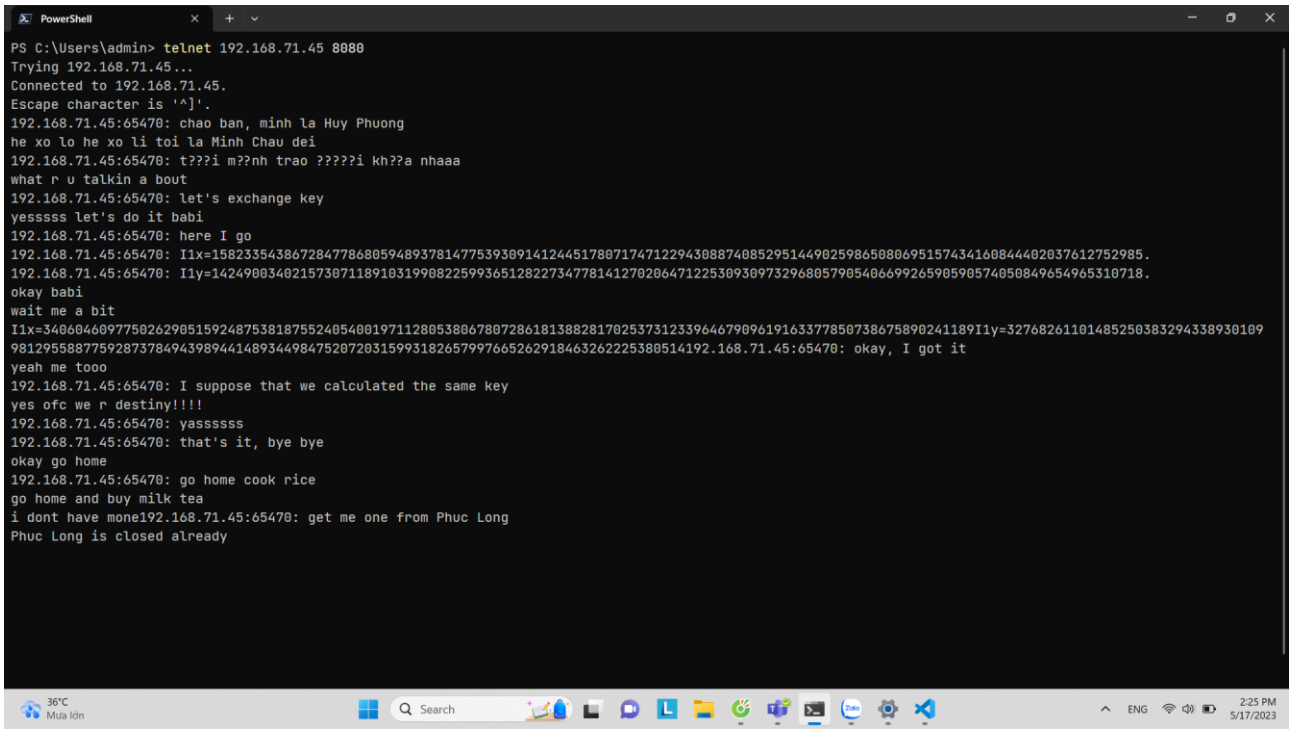
- Bước 2: Mỗi bên tạo một secret number (PrivateKey) và giữ kín.
    - Secret number của MC
      priKeyHP = 23402

- Bước 3: Tạo publicKey từ privateKey và điểm G, có cặp khóa:
  pubKeyMC = priKeyMC * G
    - pubKeyMCx = 29780957869510744203933376759191092142095414828659849298235314955179536830386915447870136315155556027711362950288460
    - pubKeyMCy = 35057914743983864601952011123624636013848301617134024857432517700701973087090678133644076933956030081272064206273058
- Bước 4: Trao đổi publicKey với nhau qua giao thức TCP (telnet) thu được Public của parner (HP)
    - pubKeyHPx = 15823354386728477868059489378147753930914124451780717471229430887408529514490259865080695157434160844402037612752985
    - pubKeyHPy = 14249003402157307118910319908225993651282273477814127020

64712253093097329680579054066992659059057405084965496531
0718

- Bước 5: Tính toán sharedKey: shareKey = pubKeyHP * priKeyMC
  - shareKeyx = 122805284214342150742625629310024558306276935592317113319934756808985799726086044962519871600552193244481880615326666
  - shareKeyy = 135432322148869622355156958045922818626543243721884265052354421079265662621037311453511572286557145314543522818323 82

- Hình ảnh HP và MC trao đổi khóa thông qua giao thức TCP



- Hình ảnh sau khi chạy chương trình: