Lab 05 (2 hrs): Key Exchange

Program 1: Diffie–Hellman key exchange (on group)

In this part, you are required to implement the Diffie–Hellman key exchange algorithm in $\mathbb{Z}_p$ from scratch. (Hint: review the procedure of ElGamal algorithm). As the Setup procedure is the same as ElGamal algorithm, it is assumed that the public parameters of p and α are both set to constants in this part.

```
p:
11483166658585481347156601461652228747628274304826764495442296421425015253161813
634115028572768478982068325434874240950329795338367115426954714853905429627
alpha:
93123612106739002595637103855679271290606811352088163142392761286132360571529739
46513124497622387244317947113336161405537229616593187205949777328006346729
```

In this program, two parties, Alice and Bob, want to get a symmetric key for future symmetric encryption via Diffie–Hellman key exchange, and hope that adversaries learn nothing about the shared symmetric key. In this program, it is assumed that only Honest-but-Curious adversaries exist.

Your program will output the following items:

- All the transmission data on the communicate channel (in correct order, if necessary), e.g. `Alice to Bob: blah blah blah`.
- The symmetric key that Alice gets, that is the result of Diffie–Hellman key exchange.
- The symmetric key that Bob gets, that is the result of Diffie–Hellman key exchange.

Example Output

```
Alice to Bob:
89409599039198926463693830769882362634141492835897894175340938238797026437301383
01746710316972043367005133179322397075568692734123174632487566957931486431
Bob to Alice:
43846833528735576355623689642480687270382945292545979871802586846515202962045016
42442796366842225710992904070529210926322430373646688781391733323295711438
Result (Alice view):
11340178546045069617516325240966622435238310460224925781433563012664618800006804
703149537436309299281476260328893892580363729101975655852342449233799172983
Result (Bob view):
11340178546045069617516325240966622435238310460224925781433563012664618800006804
703149537436309299281476260328893892580363729101975655852342449233799172983
```