1. In real world, how people combine symmetric key crypto and asymmetric key crypto to exchange messages? ==> Draw diagrams to show your concepts

2. Please base on these diagrams

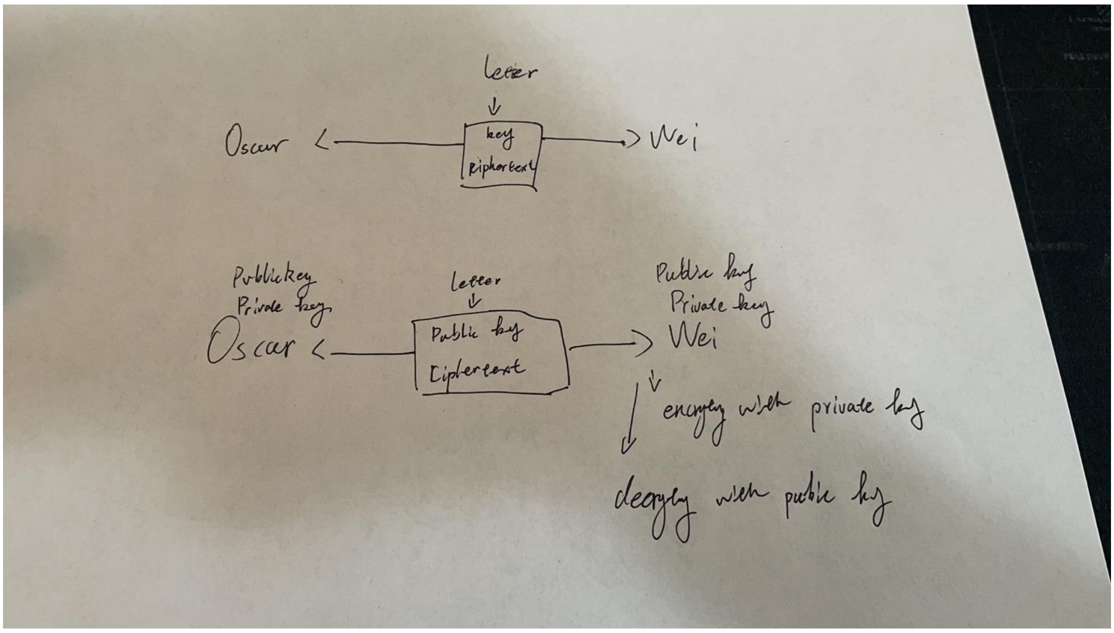
https://npu85.npu.edu/~henry/npu/classes/security/elliptic_curve/slide/elliptic_curve.html

and draw a diagram to show

3 * G

Ans:

1.



Symmetric key:

```
                  +-----------------------> K_A, K_B, . . . K_N  <------------------
--+
   (1)  |                    # +-------------+              #        |
(1)
   out  |                    # |             |  Alice        #        |
out
   of   |                    # |  I’m Alice  |  Bob          #        | of
   band |          +----------->|  I want to  |  TS           #        |
band
        |     (2) |           # |  talk to Bob|  TD           #        |
        |         |           # +-------------+  K_AB         #        |
        |         |           #                  |            #        |
        |         |           #                  v            #        |
        |         |           #      {//////{/////////}K_B}K_A #        |
        |         |           #                  |            #        |
#######|#######|############################|####################|###
###
       |   +---+--------+ #                  |            #       |
      K_A  |I'm Alice    | #                 |            #      K_B
           |I want to    | #                 |            #
           |talk to Bob  | #                 | (3)        #
           +-------------+ #                 |            #
What Alice knows &         # What Eve (the   |            # What Bob
knows
     does                  # public sees &   |            #   & does
                           # does)           |            #
   {//////{////}K_B}K_A <----------------------+          #
         |                 #                              #
Alice    | -K_A            #                              #
Bob      |                 #                              #
TS <-----+--->  {////}K_B -----------+                    #
TD                         #         |                    #
K_AB ------+               #     (4) +-> {msg}K_AB ---------> {msg}K_AB +
{///}K_B
 |         |               #         |   + {///}K_B       #     |
|
 |         v               #         |                    #     |
| -K_B
 |       +K_AB             #         |                    #     |
|
 |  msg ---> {msg}K_AB --------------+                    #     |
v
 |                         #                              #     |
Alice
 |                         #                              #     |
Bob
 |                         #                              #     |
TS
 |                         #                              #     |
TD
 |                         #                              #     |
K_AB
 |                         #                              #     |
|
 |                         #                              #     | -K_AB
<--+
 +---------+               #                              #     |
|
          |                #                              #     v
| (5)
          |                #                              #    msg
|
          v                #                              #
v
        -K_AB      (7)     #          (6)                 #
+K_AB
  msg_2 <----- {msg_2}K_AB <---------- {msg_2}K_AB <---------------{msg_2}K_AB <-
--- msg_2
                           #                              #
    (8)     +K_AB         #                              #          -
K_AB
  msg_2+ -----> {msg_2+}K_AB-----------> {msg_2+}K_AB -----------> {msg_2+}K_AB---->
msg_2+
```

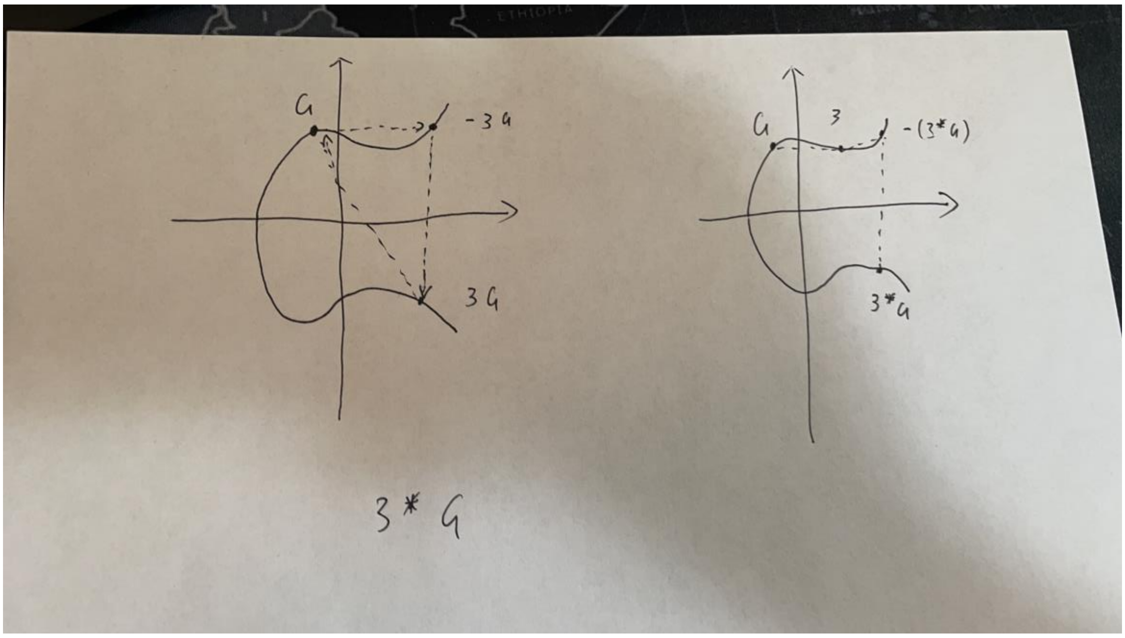
Asymmetric key:

```
What Alice knows & does   | What Eve (the public)    | What Bob
                          | knows & sees             | knows and does
--------------------------+--------------------------+------------------
-
        P_Bob (1)        | P_Bob                    | P_Bob (1)
                          |                          |  S_Bob
--------------------------+--------------------------+------------------
-
    (2)                   |                          |          (4)
    +P_Bob               | (3)                      |         -S_Bob
K_AB ------> {K_AB}P_Bob --------> {/////}P_Bob --------> {K_AB}P_Bob --> K_AB'

What Alice knows & does   | What Eve (the public)    | What Bob
                          | knows and sees           | knows and does
--------------------------+--------------------------+------------------
-
        MD (1)            | MD                       | MD (1)
        K_AB             |                          | K_AB
--------------------------+--------------------------+------------------
-
msg ----+                 |                          |
 | (2)  |                 |                          |
 | MD   +---> msg + HASH |                          |
 v      |       |(3)      |  (4)                     |
HASH ---+       |+K_AB ------------> {/////}K_AB -----------> {msg+HASH}K_AB
```

```
               v             |                                  |            | (5)
        {msg+HASH}KAB       |                                  |            | -KAB
                             |                                  |            V
                             |                                  |      msg’ + HASH’
                             |                                  |         | (6)
                             |                                  |         | MD
                             |                                  |         v
                             |                                  |      HASH
                             |                                  |
                             |                                  | (7)Does
HASH=HASH’?
```

2.


G
-3 G
3 G
G
3
-(3*G)
3*G
3* G