Exercise 1

To show that $(m_1, m_2) = (m_1', m_2')$, we have to show that $m_1 \equiv x_T^{-1} c_1 \pmod{p}$ and $m_2 \equiv y_T^{-1} c_2 \pmod{p}$.

$$
\begin{aligned}
m_1 \equiv x_T^{-1} c_1 \pmod{p} \;\wedge\; m_2 \equiv y_T^{-1} c_2 \pmod{p} & \\
& \quad c_1 \equiv x_S m_1 \pmod{p} \textit{ and } c_2 \equiv y_S m_2 \pmod{p} \\
m_1 \equiv x_T^{-1} x_S m_1 \pmod{p} \wedge m_2 \equiv y_T^{-1} y_S m_2 \pmod{p} &
\end{aligned}
$$

For $(m_1, m_2) = (m_1', m_2')$ to hold, we just have to show that $T^{-1}S \equiv 1 \pmod{p}$.

$$
\begin{aligned}
& & & T = n_A R \textit{ and } S = k Q_A \\
T^{-1}S &\equiv (n_A R)^{-1} k Q_A \pmod{p} & & \\
& & & R = kP \textit{ and } Q_A = n_A P \\
&\equiv n_A^{-1} (kP)^{-1} k n_A P \pmod{p} & & \\
& & & n_A n_A^{-1} = 1,\ kk^{-1} = 1 \textit{ and } PP^{-1} = 1 \\
&\equiv 1 \pmod{p} & &
\end{aligned}
$$

Thus, $(m_1, m_2) = (m_1', m_2')$.

Exercise 2

```
from sage.all import *

def gen_pub_key(A, B, p, x_p, y_p):
    Fp = FiniteField(p)
    E = EllipticCurve(Fp, [A, B])
    assert(E.is_on_curve(x_p, y_p))

    P = E([x_p, y_p])
    n_a = ZZ(Fp.random_element())
    Q_A = n_a * P

    return (Q_A, n_a)


def encrypt(A, B, p, x_p, y_p, Q_A, m_1, m_2):
    Fp = FiniteField(p)
    E = EllipticCurve(Fp, [A, B])
    assert(E.is_on_curve(x_p, y_p))

    P = E([x_p, y_p])
    k = ZZ(Fp.random_element())
    R = k * P

    S = k * Q_A
    c_1 = (S[0] * m_1) % p
    c_2 = (S[1] * m_2) % p

    return (R, c_1, c_2)
```

```
def decrypt(A, B, p, x_p, y_p, R, n_a, c_1, c_2):
    Fp = FiniteField(p)
    E = EllipticCurve(Fp, [A, B])
    assert(E.is_on_curve(x_p, y_p))

    T = n_a * R
    m_1 = (T[0] ** (-1) * c_1) % p
    m_2 = (T[1] ** (-1) * c_2) % p

    return (m_1, m_2)
```

Running this functions with the Curve P-384, we can see the functions are defined correctly (Fig. 1).

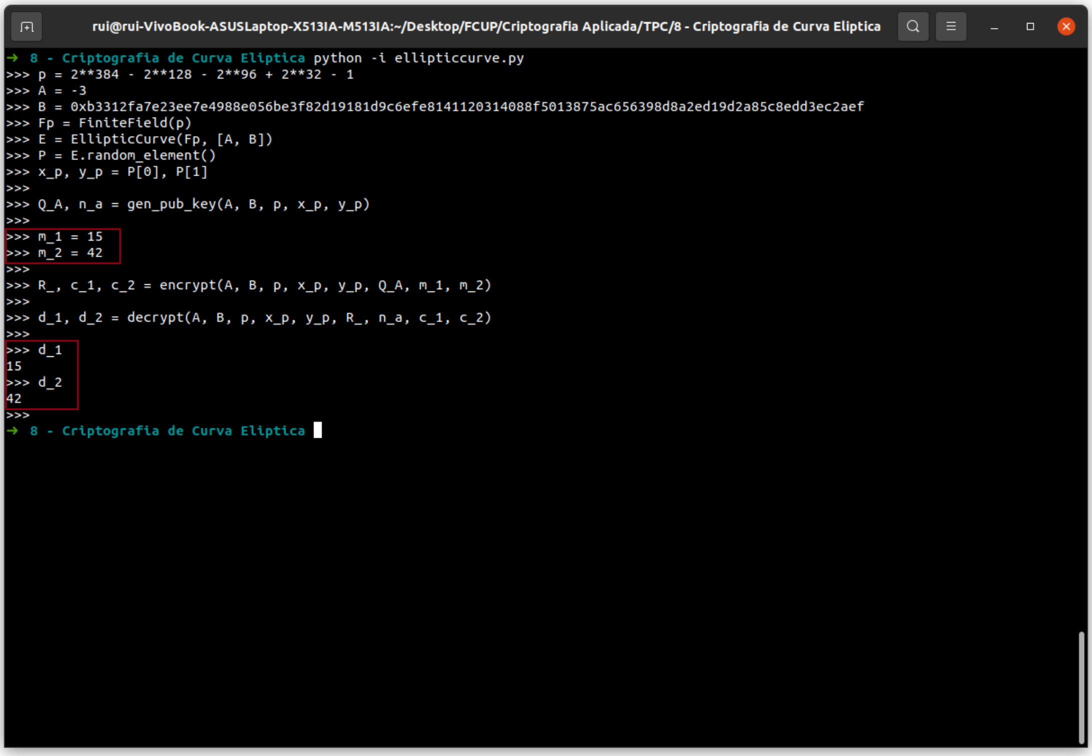

Figure 1: Menezes–Vanstone variant for ECC ElGamal