Task: Complete exercise 1.12 on page 50

To show that the provided algorithm computes the greatest common divisor g of the positive integers a and b, along with integers u and v such that $au + bv = g$, we can analyze the steps involved in the algorithm.

1. Start with the initial values $u = 1$, $g = a$, $x = 0$, and $y = b$.

   If $b = 0$, then we raise a ZeroDivisionError, since division by zero is not allowed, and the program terminates.

2. The algorithm enters a while loop that only terminates when the value of y is zero. Inside the loop, we compute the quotient $q = g//b$ and remainder $t = g\%y$ such that $g = qy + t, 0 \leq t < y$. But this step is crucial because it follows the principle of the Euclidean algorithm which is used to compute the gcd.

   In addition, we compute $s = u - qx$. This step updates s based on the previous values of u and x.

   The algorithm updates u to x and g to y. This prepares for the next iteration to find the *gcd* of the new pair (y, t).

   The values of x and y are updated to s and t, respectively. This ensures that we are always working with the most recent coefficients and remainders.

3. The algorithm loops back to the second step until y becomes zero. At this point, we can compute $v = \frac{g-au}{b}$. Since $y = 0$, then $g = a$, which is the last non-zero remainder. Thus $g = \gcd(a, b)$. The equation $au + bv = g$ simplifies to $au + 0 = g$, confirming that u is a valid coefficient.

   The coefficients u and v correspond to the integers that satisfy $au + bv = g$.

By following these steps, the algorithm implements the Extended Euclidean Algorithm. It computes the *gcd* of a and b. It also finds integers u and v such that

$$au + bv = \gcd(a, b).$$

This shows that algorithm computes the greatest common divisor g of the positive integers a and b, along with integers u and v such that $au + bv = g$.

The private key used by Alice and Bob to decode their messages $c1 = 12849217045006222$ and $c2 = 6485880443666222$ is $k = 174385766$. The private key is obtained from the above algorithm. See the python function extended_gcd(12849217045006222, 6485880443666222) in the python file.