jirafaGraph Asymmetric Encryption

Let G be a complete graph of order n s.t. each node is weighted with an ordered pair from $\{(e_i, p_i) | p_i \in Z \ni p \text{ is prime}, e_i \in Z \ni \leq x < p\}$. Then, we can consider each e_i to be an encryption key with a corresponding decryption key in the set $\{(p_i - e_i, p_i) | i \in Z \ni 0 \leq i \leq n\}$.

Suppose Alice sends Bob a message that is represented by the number b, where $0 \leq b < i$, where i is the minimum of $\{p_i\}$. Now, let $p = (p_0, p_1, \ldots, p_{n-1}) = ((a_0, b_0), \ldots, (a_{l-1}, b_{l-1})$ be a path through the graph of length l. Without loss of generalization, assume $l = 3$.

Then, we can describe a sequence of applications of asymmetric encryption where we apply each encryption key to the message m knowing that this is a bijective mapping producing ciphertext c, as follows:

$$c = \left(\left(m^{a_0} \right)^{a_1} \right)^{a_2}.$$

Similarly, we observe that we can decrypt the ciphertext c as follows:

$$m = \left(\left(c^{b_0} \right)^{b_1} \right)^{b_2}.$$