Starting position
Selected nodes = private key
Perfect code – we’ll build one

Each node is connected to exactly one selected node. Perfect code: there exists a selection of nodes so that each node is in the neighborhood of exactly one selected node (a selected node is in its own neighborhood.)
Additional edges

To hide the structure of the selected nodes, further edges are included under the condition that they are connected to one of the selected nodes. This gives a perfect code – proof it!
Public key

All edges, no highlighting.
Encryption of $m = 13$

$13 = 1 + 2 + 3 - 4 + 5 + 4 + 3 - 1$. Partition 13, one share per node.
Encryption of $m = 13$

For each node compute the sum of values at all nodes at distance at most 1, i.e. the value at the node itself plus all nodes directly connected to it.

\[ 5 = 1 + 2 + 3 - 1 \]
Encrypted message

For each node write the sum computed in the previous step next to it.
Decryption

Add values at points selected as secret key.

\[4 + 2 + 7 = 13.\] Why does this work?
Overview

1. Sheet: secret key (1),
intermediate steps (1–3)

2. Sheet: public key (4)

3. Decryption (8)

4. Sheet: computations (5–6)

5. “Black” numbers next to nodes (7)

A: 1. sheet: secret key (1), 2. sheet: public key (4)

B: 1. sheet: computations (5–6) 2. sheet: “black” numbers next to nodes (7)