Perfect-code cryptosystem

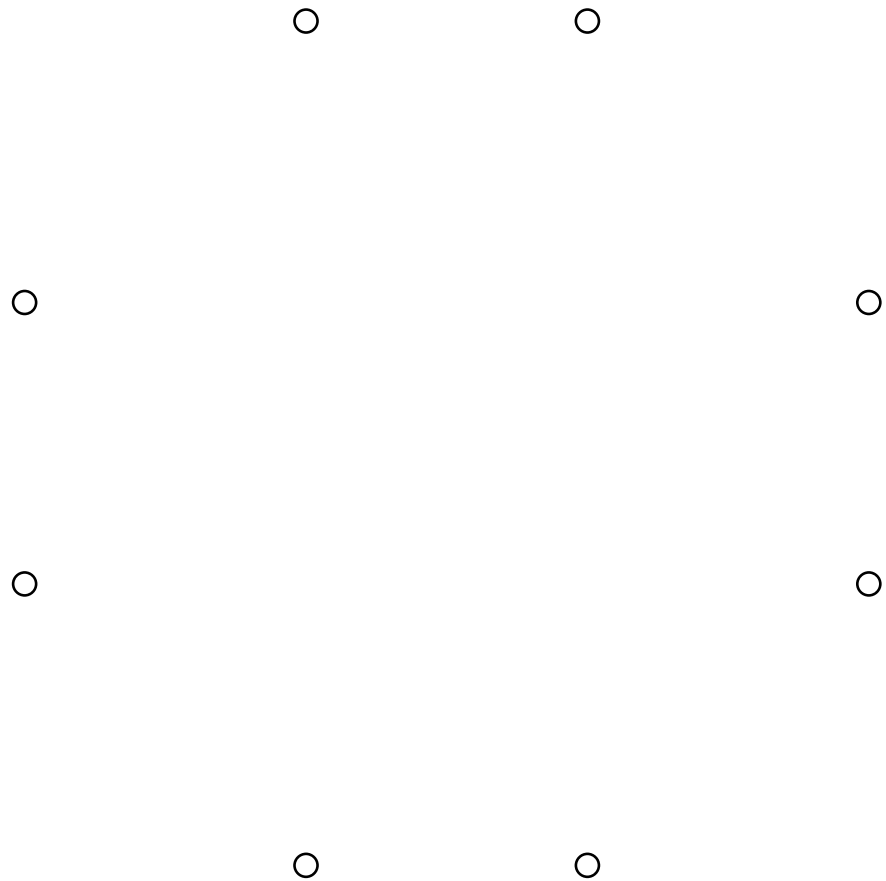
A teaching example for public-key cryptography

Tanja Lange

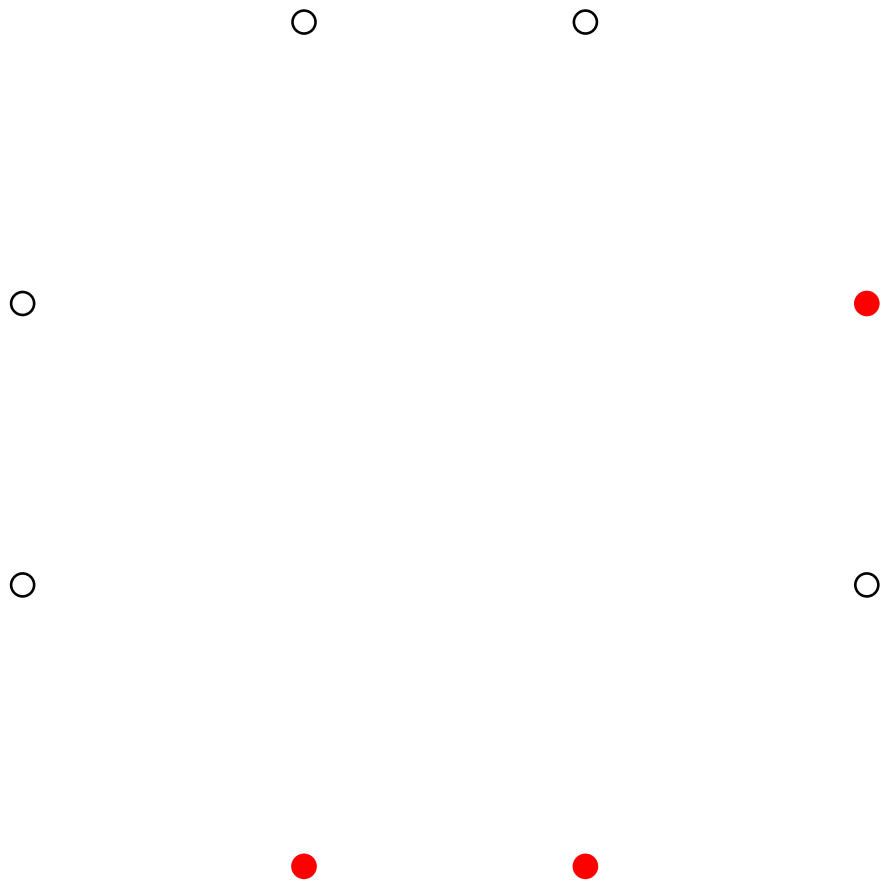
Eindhoven University of Technology

2MMC10 – Cryptology

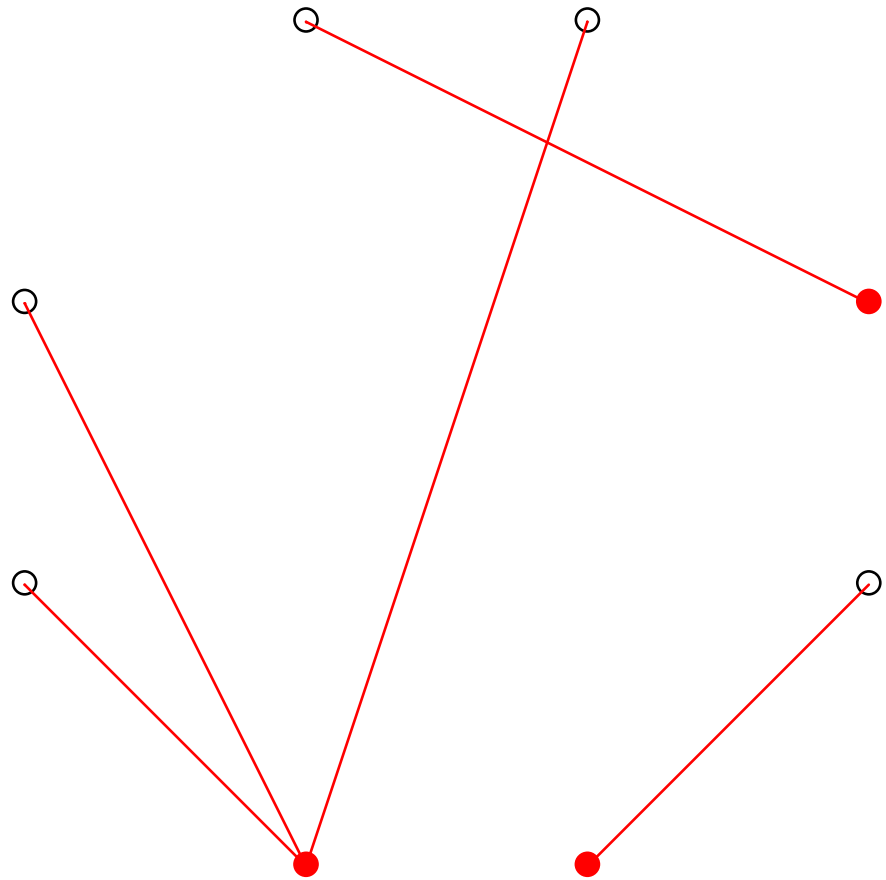
Starting position



Selected nodes = private key

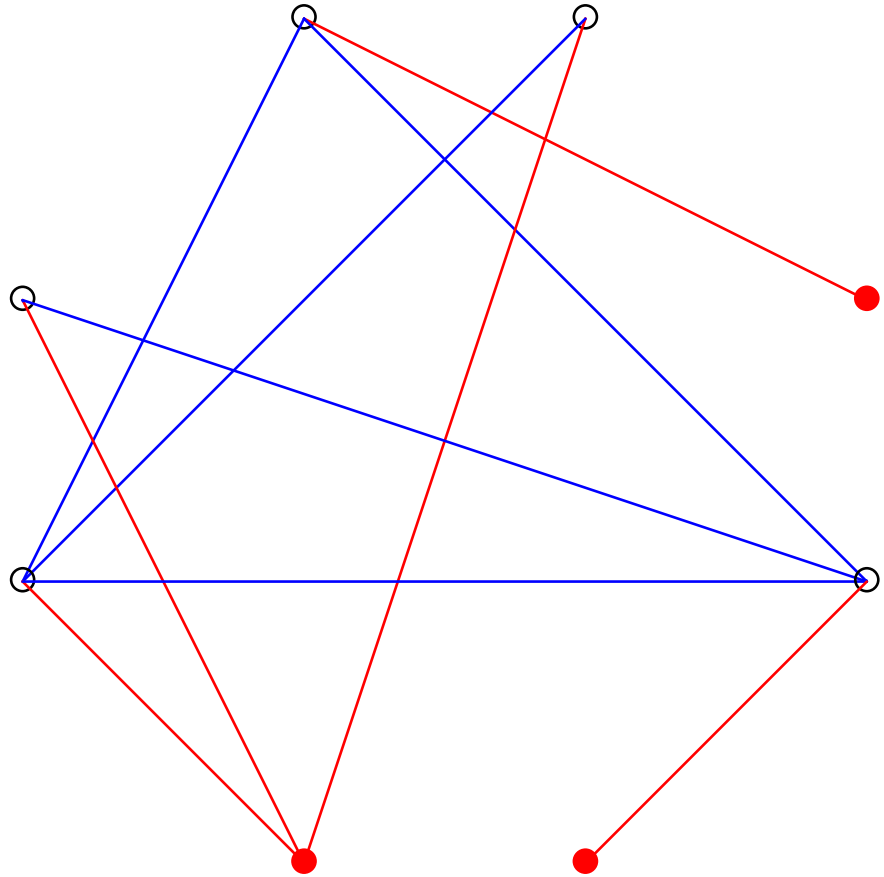


Perfect code – we'll build one



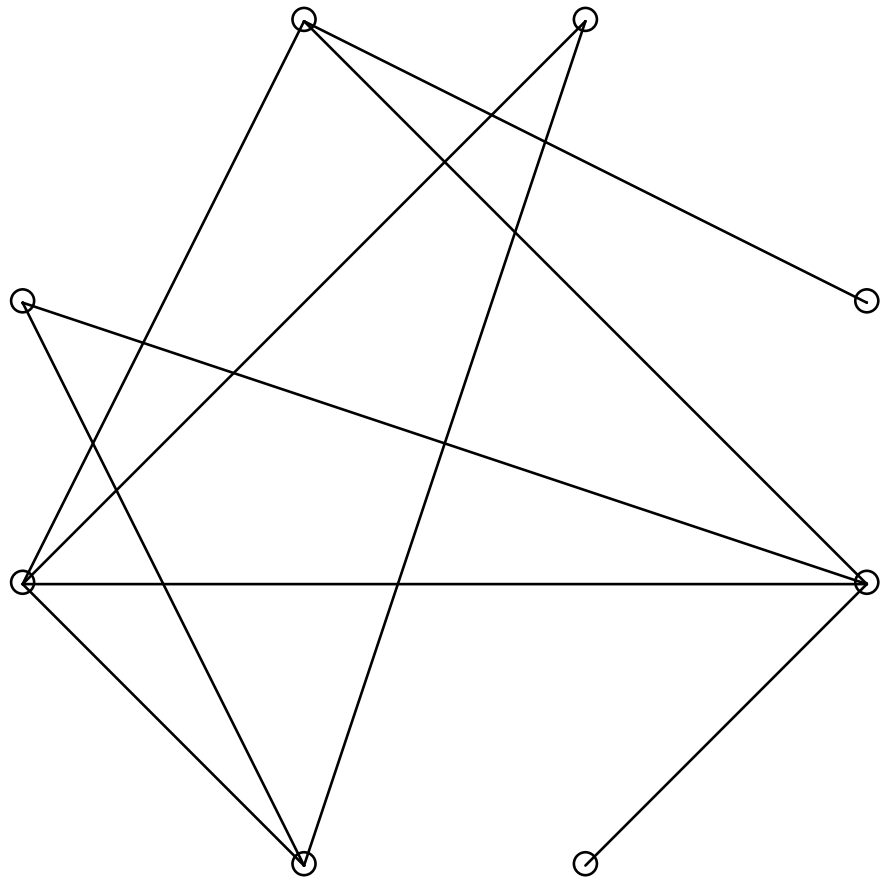
Each node is connected to exactly one selected node.
Perfect code: there exists a selection of nodes so that each node is in the neighborhood of exactly one selected node (a selected node is in its own neighborhood.)

Additional edges



To hide the structure of the selected nodes, further edges are included. These edges must not touch the selected nodes. This gives a perfect code – prove it!

Public key



Same edges, no highlighting.

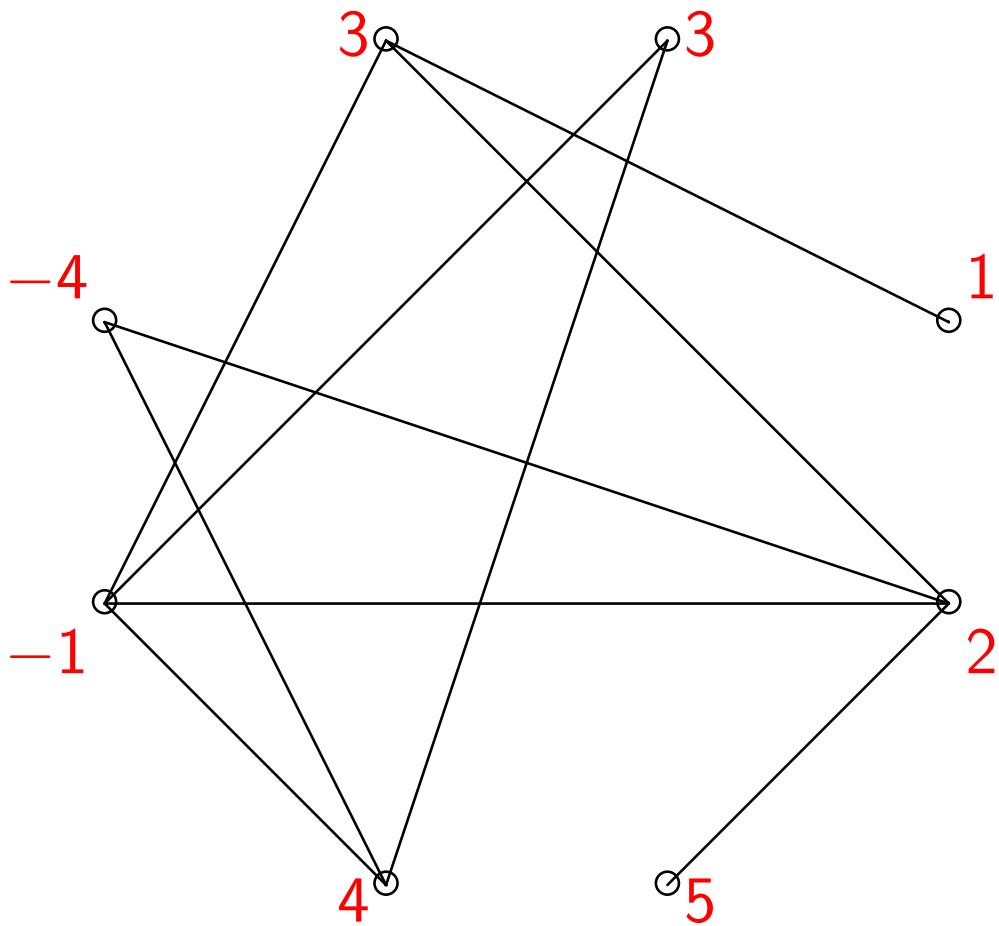
Encryption of $m = 13$ – step 1

Partition 13, one share per node.

Encryption of $m = 13$ – step 1

Partition 13, one share per node.

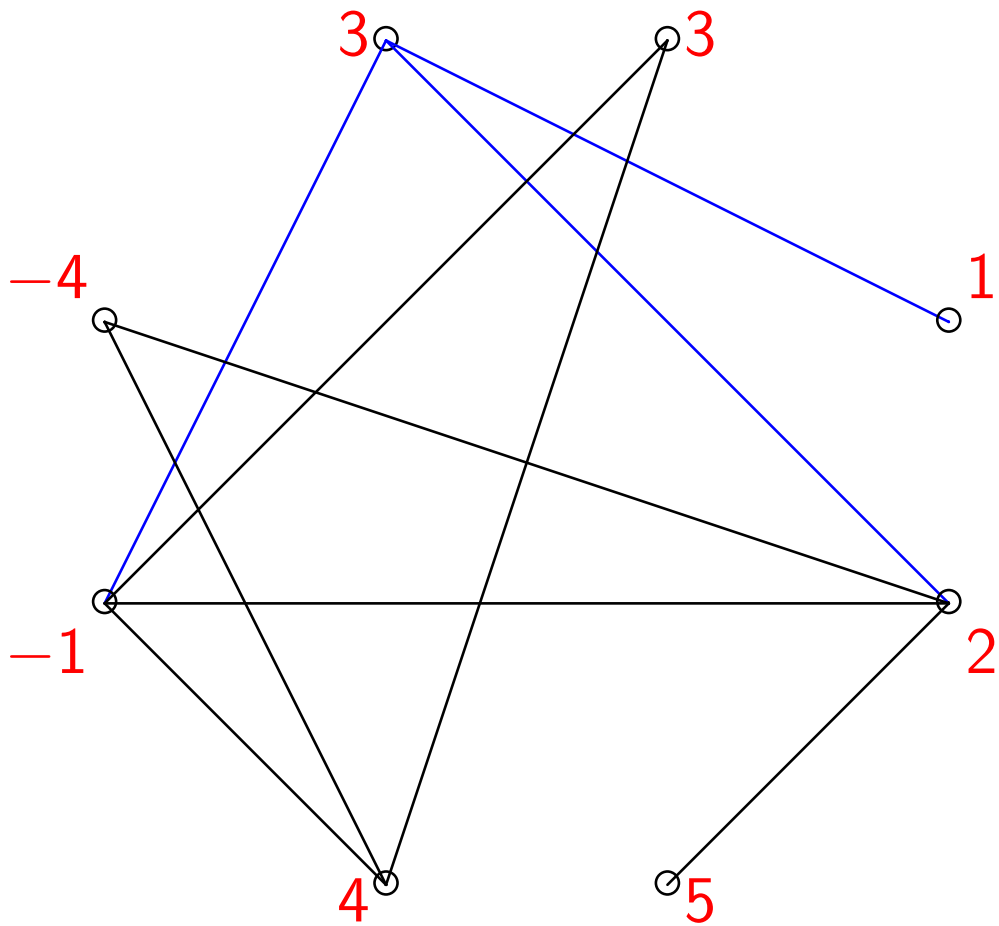
$13 = 1 + 2 + 3 - 4 + 5 + 4 + 3 - 1$.



Encryption of $m = 13$ – step 2

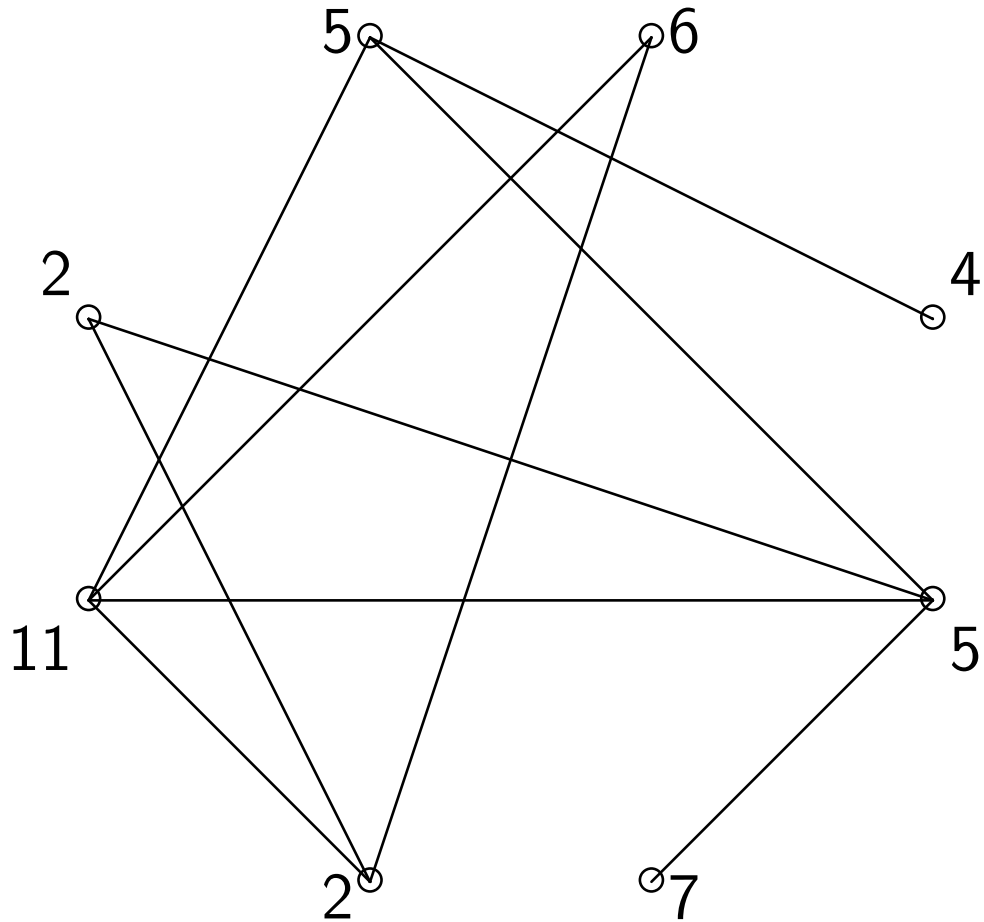
For each node compute the sum of values at all nodes at distance at most 1, i.e. the value at the node itself plus all nodes directly connected to it.

$1 + 2 + 3 - 1 = 5$



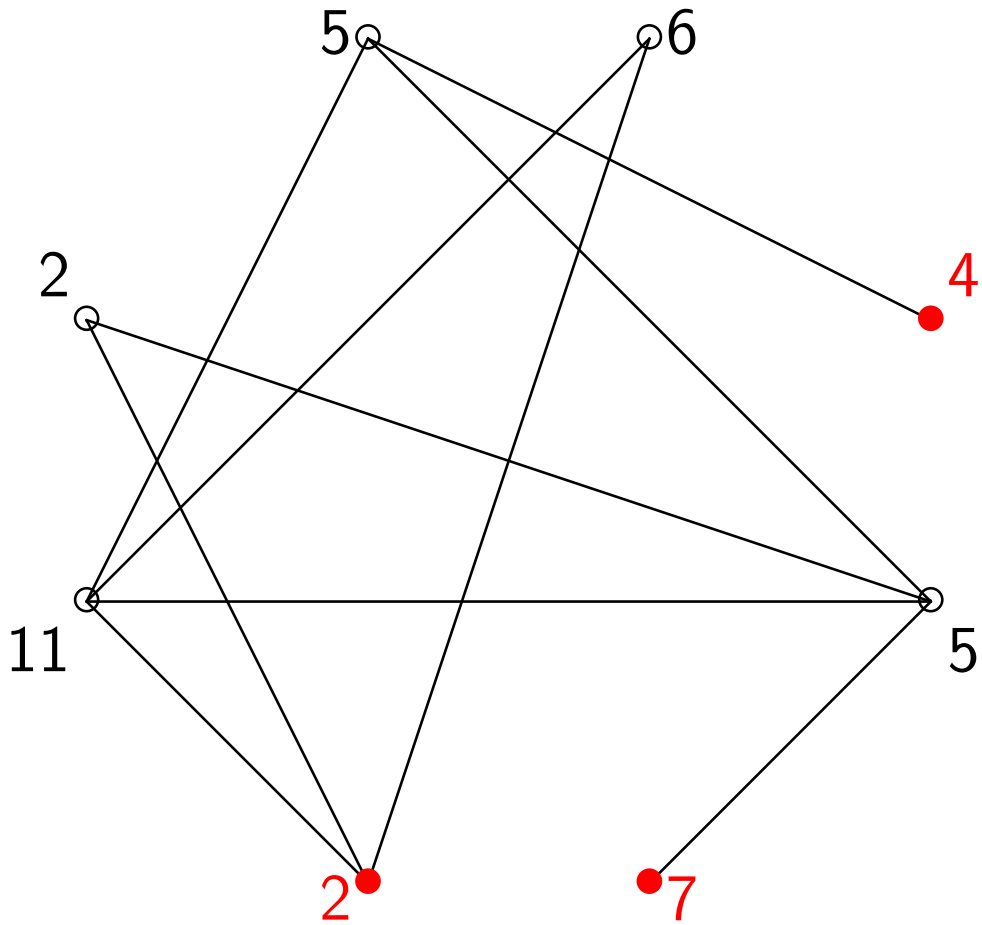
Encrypted message

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



Decryption

Add values at points selected as secret key.

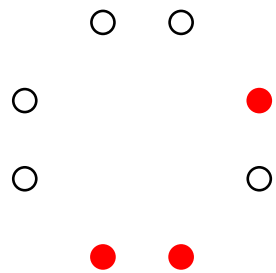


$4 + 2 + 7 = 13$. Why does this work?

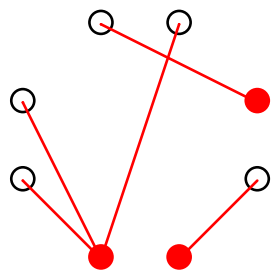
Overview

Use https://webwhiteboard.com/ to exchange public keys and ciphertexts. Click on 'share board' for URL to your board.

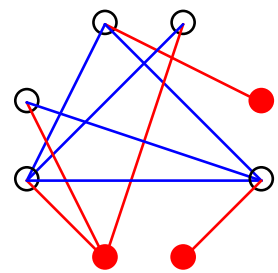
1.



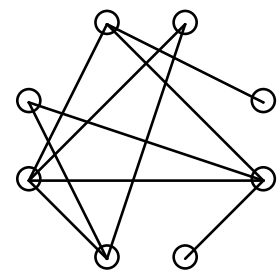
2.



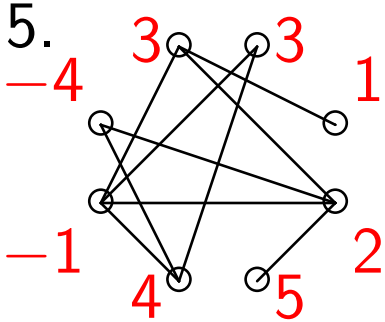
3.



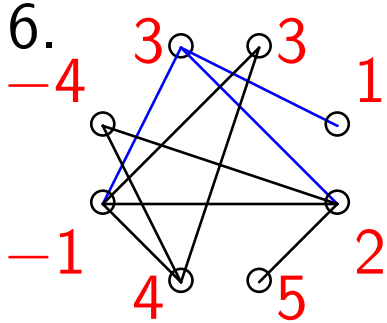
4.



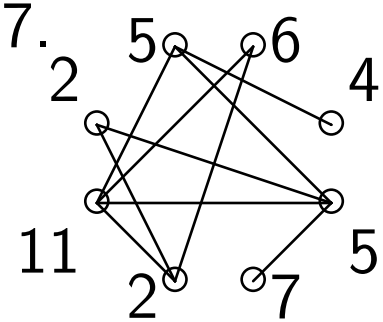
5.



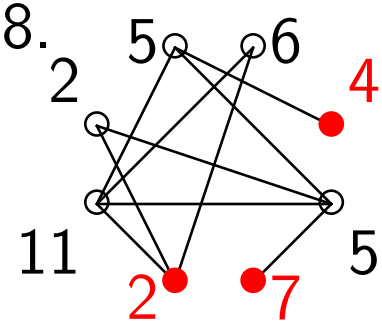
6.



7.



8.



A: 1. sheet: secret key (1), intermediate steps (1–3) 2. sheet: public key (4) decryption (8)

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

Why does this system work? Break the examples. Break this for graphs with 1000 nodes.