

IDENTITIES

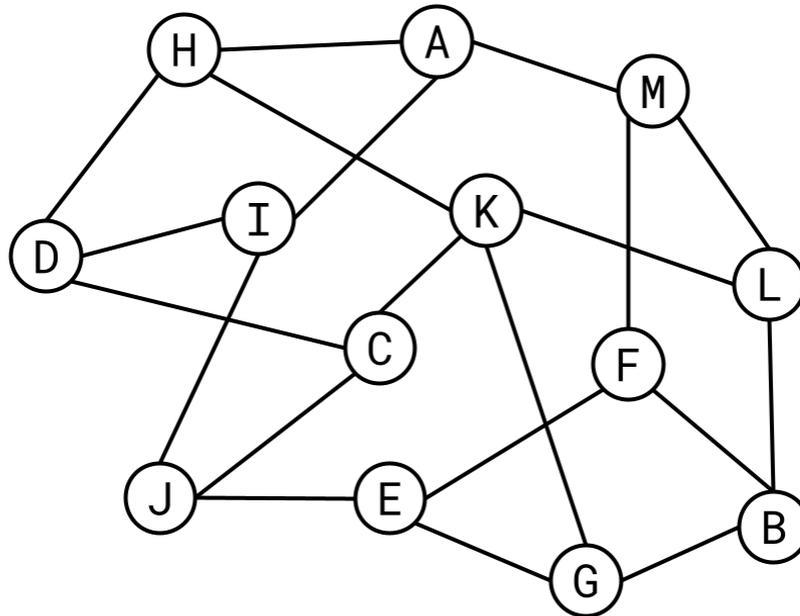
Enlightening
Interdisciplinarity
in STEM
for Teaching

Common introduction to Encryption with the PDS cryptosystem

Cryptography module

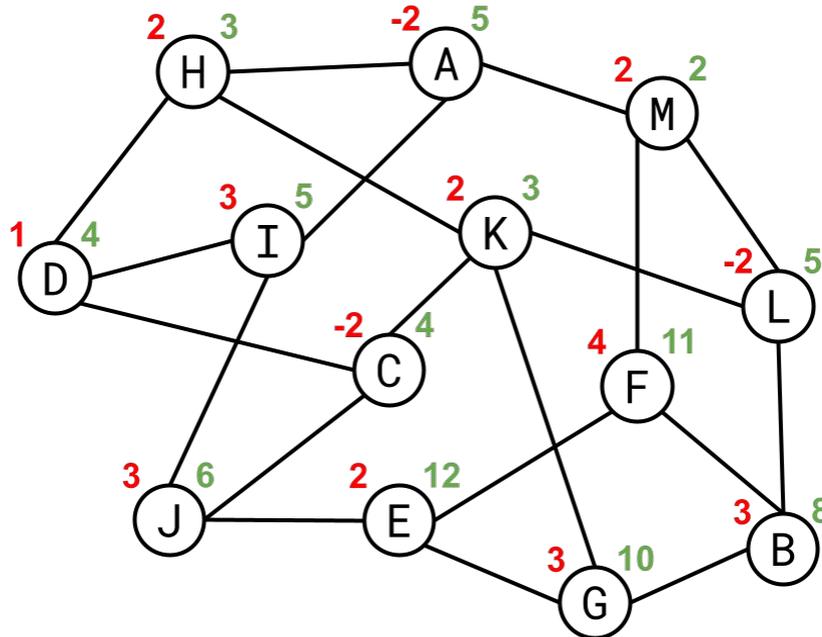
Encryption

1. Decide which number is the message m to be encrypted. Here $m = 19$
2. Using a **red pen**, place random numbers on each node of the graph, so that the random numbers add up to the number m . These numbers are called **secret values**.
Here the **decomposition** is $[3, 2, 4, 3, -2, 1, -2, 2, 3, -2, 2, 3, 2]$.
We can check that: $3 + 2 + 4 + 3 + (-2) + 1 + (-2) + 2 + 3 + (-2) + 2 + 3 + 2 = 19$
3. Choose any node, look at it and its neighbours and sum the numbers on them. Write this number at the node using a **green pen**. These values are called **public values**.
4. Erase the red numbers. The encrypted message is the graph with only the green numbers on the nodes.



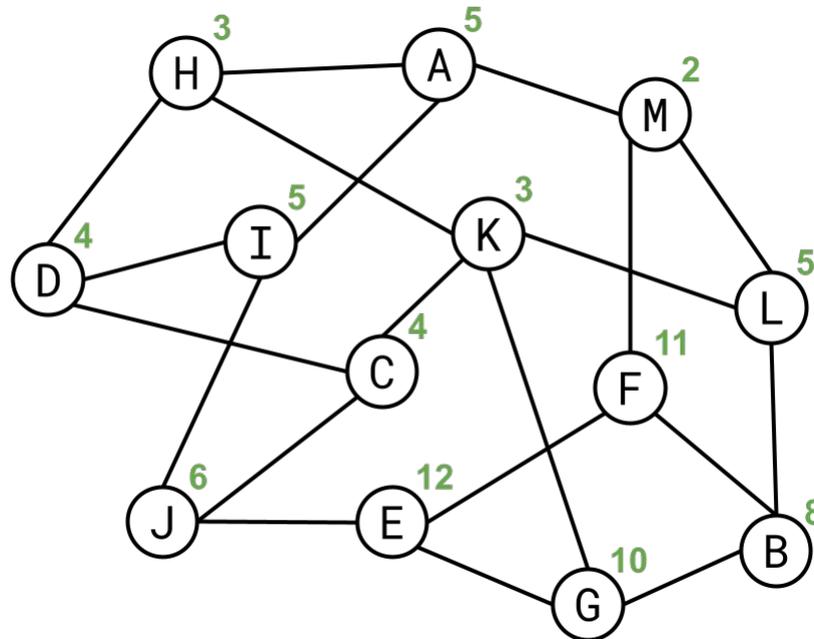
Encryption

1. Decide which number is the message m to be encrypted. Here $m = 19$
2. Using a **red pen**, place random numbers on each node of the graph, so that the random numbers add up to the number m . These numbers are called **secret values**.
Here the **decomposition** is $[3, 2, 4, 3, -2, 1, -2, 2, 3, -2, 2, 3, 2]$.
We can check that: $3 + 2 + 4 + 3 + (-2) + 1 + (-2) + 2 + 3 + (-2) + 2 + 3 + 2 = 19$
3. Choose any node, look at it and its neighbours and sum the numbers on them. Write this number at the node using a **green pen**. These values are called **public values**.
4. Erase the red numbers. The encrypted message is the graph with only the green numbers on the nodes.



Encryption

1. Decide which number is the message m to be encrypted. Here $m = 19$
2. Using a **red pen**, place random numbers on each node of the graph, so that the random numbers add up to the number m . These numbers are called **secret values**.
Here the **decomposition** is $[3, 2, 4, 3, -2, 1, -2, 2, 3, -2, 2, 3, 2]$.
We can check that: $3 + 2 + 4 + 3 + (-2) + 1 + (-2) + 2 + 3 + (-2) + 2 + 3 + 2 = 19$
3. Choose any node, look at it and its neighbours and sum the numbers on them. Write this number at the node using a **green pen**. These values are called **public values**.
4. Erase the red numbers. The encrypted message is the graph with only the green numbers on the nodes.



IDENTITIES

Enlightening
Interdisciplinarity
in STEM
for Teaching



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA



UNIVERSITAT DE
BARCELONA



ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE



UNIVERSITÀ
DI PARMA

Co-funded by the
Erasmus+ Programme
of the European Union



Grant Agreement n°2019-1-IT02-KA203-063184