IDENTITIES

Enlightening
Interdisciplinarity
in STEM
for Teaching

Decryption activity (Group B)

Cryptography module

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

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

Introduction

A secret message (a number) has been encrypted with the encryption technique showed before.

Your task is to decrypt the secret message.

In the following, you will be given some information

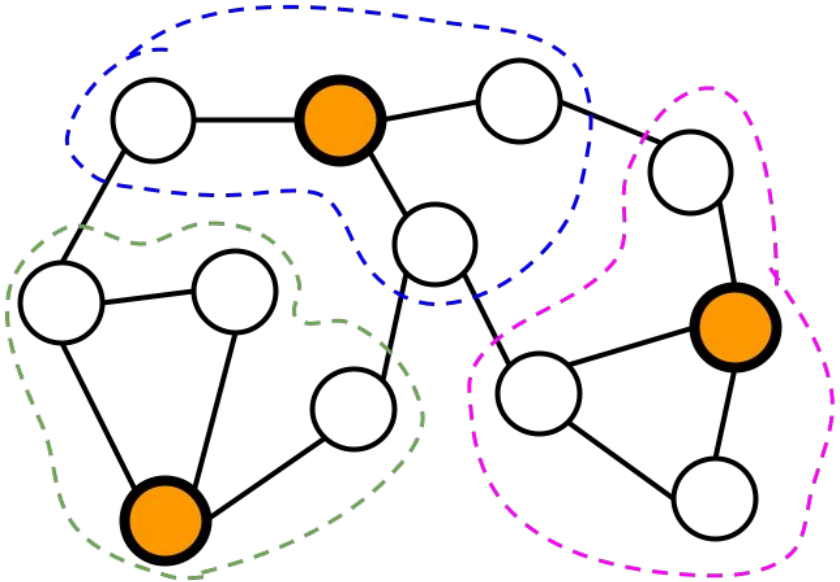
- the definition of a perfect dominating set (PDS)
- the decryption algorithm on the example showed before
- a secret message encrypted on a particular (different) graph
- a link to verify if you decrypted the secret message correctly

Domination, dominating sets, perfect dominating sets (PDS)

A vertex *v* of a graph G dominates vertex *u* if there is an edge from *v* to *u*. The vertex *v* also dominates itself.

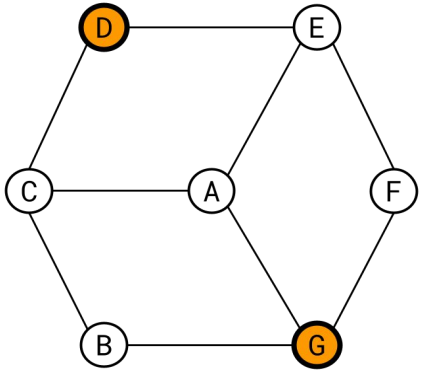
A set S of vertices of G is a dominating set of G if every vertex of G is dominated by a vertex in S.

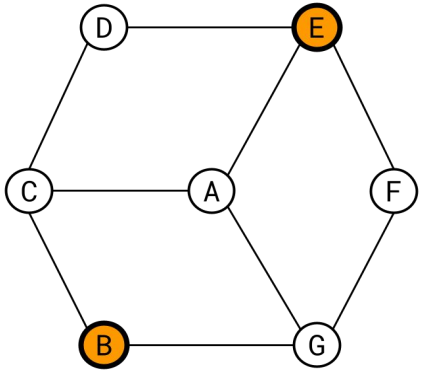
A set **S** of vertices of G is a *perfect dominating set* (PDS) if each vertex of G is dominated by exactly one vertex in S.

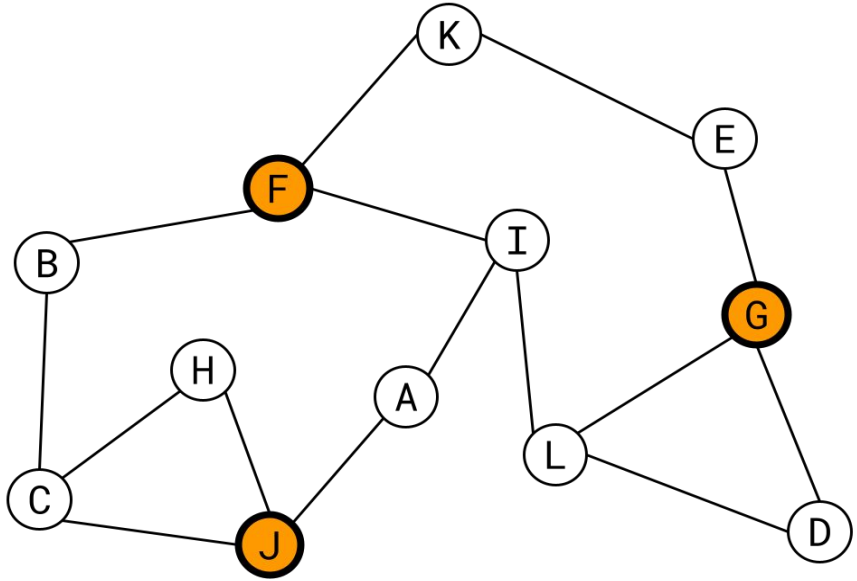


Perfect dominating set (PDS)

A **set S** of vertices of G a *perfect dominating set* (PDS) if each vertex of G is dominated by exactly one vertex in S.

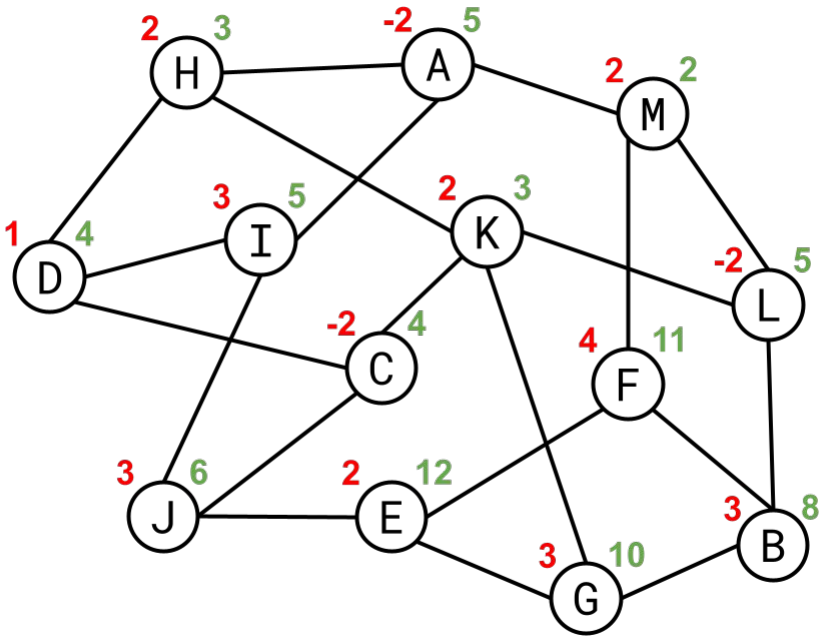






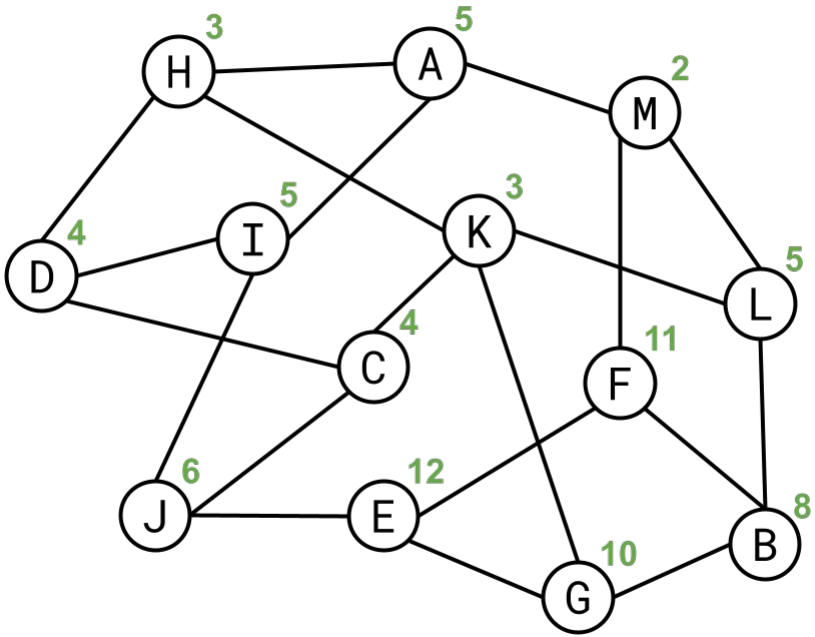
Recall how we encrypted a secret message

- Decide which number is the message m to be encrypted. Here **m = 19**
- 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**
- 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.
- Erase the red numbers. The encrypted message is the graph with only the green numbers on the nodes.



Recall how we encrypted a secret message

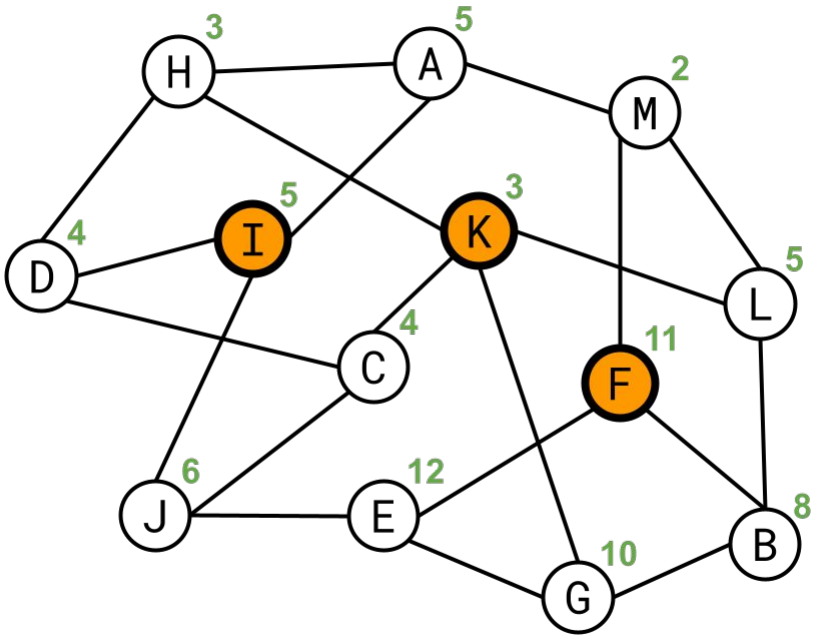
- Decide which number is the message m to be encrypted. Here **m = 19**
- Using a red pen, place random numbers on each node of the graph, so that the random numbers add up to the number m. These numbers are called secret values.
  Here the decomposition is [3, 2, 4, 3, -2, 1, -2, 2, 3, -2, 2, 3, 2].
  We can check that: 3 + 2 + 4 + 3 + (-2) + 1+ (-2) + 2 + 3 + (-2) + 2 + 3 + 2 = **19**
- 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.
- Erase the red numbers. The encrypted message is the graph with only the green numbers on the nodes.



Decryption

Enlightening
Interdisciplinarity
in STEM for Teaching

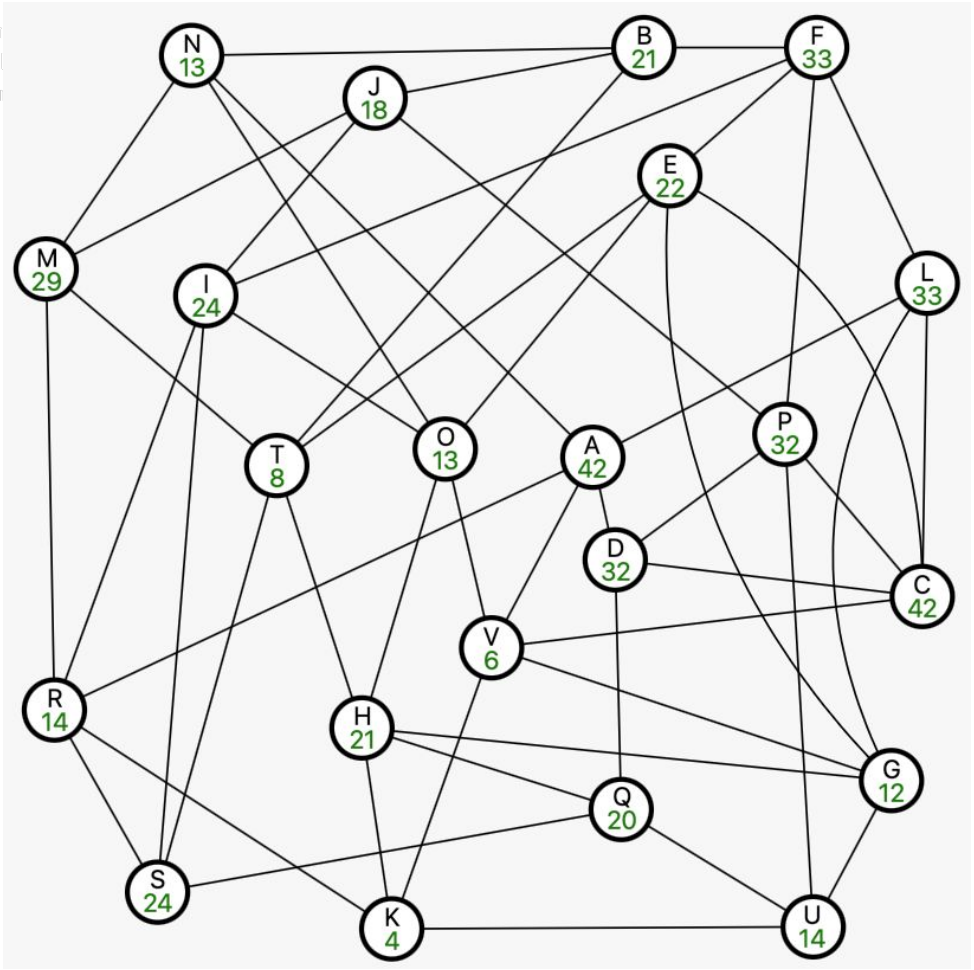
If you know a PDS on the graph, you can decode the secret message by summing the public (green) values on the PDS nodes.
Here the nodes I, K and F are a PDS of the graph.
I + K + F = 5 + 3 + 11 = 19 which is the secret message.



PDS: I, K, F

Enlightening
Interdisciplinarity
in STEM for Teaching

Secret message



Verify your decryption

A secret message (a number) has been encrypted.

Go to the following link to verify if you found the plaintext message on the graph.

The number is the key to open this treasure chest.

https://bit.ly/2Se6Jes

or, equivalently

https://snap.berkeley.edu/embed?project=Lock&user=mycol&pauseButton=true

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