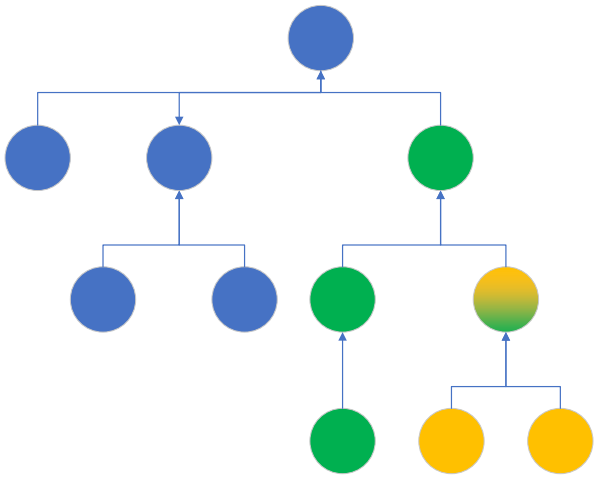
Project proposal

Team members:

Aleksander Przybylo (Student ID: 1673047)

Project abstract:

Research techniques for partially encrypting structured datasets (trees and graphs) using multiple keys where each key decrypts different portions of the dataset. The sub-datasets could potentially overlap, in which case several keys would decrypt common portions of the dataset but not the portions which it doesn't have access to. The figure below shows a tree where the green key decrypts all green nodes and the yellow key decrypts the yellow nodes. There is one node being decrypted by both keys: green and yellow.



The chosen method will need to work on any kind of structured dataset such as: XML, JSON (trees) or RDF (graphs).

Project outline:

1. Industrial motivation
   Describe the motivation for the project: data sharing between an OEM and its suppliers.
2. Existing research review – research existing papers on the topic
   Research existing papers on the topic of multi-key and partial data encryption. Search for ideas from other domains such as image and audio processing, unstructured data encryption etc.
3. Description of chosen approach
   Summarize the best candidate method for the chosen use case.
4. Implementation on sample datasets
   Implement the above described method and test on sample RDF and XML/JSON datasets.