TATA52 DISCRETE MATHEMATICS

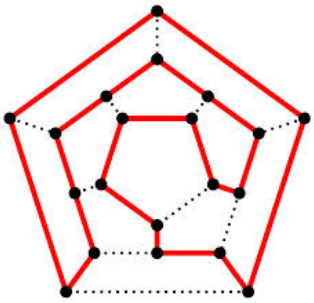
Discrete Mathematics is a problem-solving course with applications to different areas of every day life. For instance digital techniques are based in manipulations of sequences of numbers: 0's and 1's. PIN codes in all our credit cards are based in the fact that it is very complicated to factorize an integer number in prime factors.

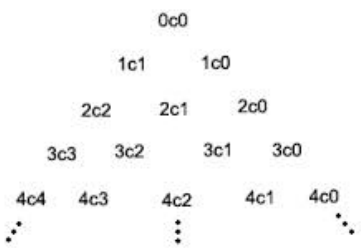
Problem solving requires different skills:

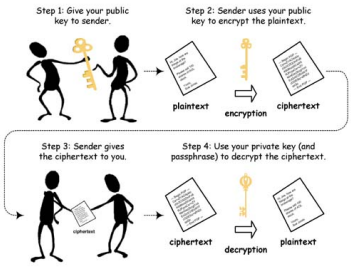
(1) **Counting**: First of all one has to count. Discrete mathematics teaches to count different kinds of objects. The mathematics of counting (finite structures) is **combinatorics**. One may count in different ways and different structures: one may count with **numbers** or **graphs**, etc.

(2) **Modeling**: To solve problems one has to find an appropriate (discrete) model of the problem. These mathematical models are built with **discrete structures**: sets, permutations relations, graphs, trees, relations, functions, numbers, etc.

(3) **Mathematical Thinking**: To be able to work with discrete structures, to represent different objects, to create or understand **algorithms** to solve problems, as well as communicating mathematics, one has to get used to think mathematically: here **proofs** take a prominent role, and for the purposes of the course, specially **mathematical induction**.







The figures illustrate three problems in branches of discrete mathematics with important applications: **Hamilton's traveling salesman problem** (Hamilton, 1857), **The problem of points** (Fermat-Pascal, 1654) and **public key cryptography**.

Consider twenty towns situated at the vertices of the graph above. Hamilton put the following question: can a salesman leave home, visit each town once and just once and come back home?

In the **problem of points** two players play different rounds of a game. The first player to have won a certain number of rounds (agreed in advance) wins the whole prize. Now suppose that the game is interrupted by external circumstances before either player has achieved victory. How does one then divide the prize pot fairly?

In public key cryptography the keys are functions on a **finite** system of numbers, the so called **modular numbers**