

TD 1. Cryptography and security

You probably know more security than you think !

- (1) **Assets:** identify your assets
 - privately
 - inside the university
- (2) What are the threats against your assets? Focus on the threats against availability, integrity, confidentiality and traceability
- (3) Can you give the different security policy for the surface mail? The access control policy for your home, computer rooms, INRIA's library or a military site like the radar center from Mount Boron near Nice.
- (4) Give a security policy for your home, for the university buildings;
- (5) Give some example of attacks and counter-measures against the threats which were previously identified.
- (6) What is the difference between data security and network security?
- (7) What is the goal of traceability and how can you ensure it?
- (8) Give some examples of passive attacks and tools to achieve it.
- (9) Same as above but for active attacks.
- (10) Why "security by obscurity" is equivalent to no protection at all?
- (11) What are the differences between an integrity service and a confidentiality service?
- (12) Provide an example to illustrate the four basic principles of security.