Computational Logic

Interactive Theorem Proving	SS 2015	703641
Week 12		June 08, 2015

Homework

The task of the exercise is to provide a minimal formalization of cryptography in your favorite prover. You are not limited to HOL Light, Mizar, Coq, or Isabelle.
Please add comments in your formalization code where choices have been made.

1. Each formalization starts with choosing of the concepts and properties of the formalization that you will formalize. Choose the informal concepts and their properties. Select those that will realize:

   - the concept of "knowing" a key / message
   - a function that performs encryption / decryption.

   You need to support at least simplest symmetric and asymmetric cryptography.

2. Choose:

   - The types in your formalization. Various possible representations of messages are possible, comment on your choices.
   - The encryption algorithms that you will formalize. For example you could choose the Caesar cipher and RSA.
   - How will your formalization add to the safety of the algorithm?

3. Find the needed theories and theorems in your prover's library.

   - For example you may need the Fermat's little theorem. If it is there, find it.
   - If a big numeric prerequisite, such as Fermat is not there, make an axiom and clearly mark it.

4. Formalize the chosen properties.