RSA on SMT

Jeremy Perez

March 2025

0.0.1 What was the objective of your project? State any subgoals, stretch goals, etc.

The main objective of my project was to model RSA in SMT and see the limitations of using Integers and Bitvectors. This requires me to

- Come up with a mathematical specification of RSA
- Implement the specifications in SMT using integers and bitvectors theories
- Come up with an "experiment" where I fix parameters and time how fast it is to be able to find a proper decryption exponent
- Compare the speed at which they are able to verify constants that satisfy the RSA properties

Some of my reach goals, was to run larger experiments. Also, I would of like to learn about *probabilistic logic* and probability based tooling like **EasyCrypt** to prove out probabilistic properties about RSA. I didn't learn about this until later into the project.

0.0.2 Explain any terms that one might need to understand to understand this objective.

- **Modeling RSA**: I'm referencing specifying RSA's number theoretical operations which are just modular exponentiation and modular arithmetic in terms of their corresponding theories and verifying the underlying ability to choose exponents such that they allow you to decrypt and encrypt a message and not change it.

0.0.3 Did you achieve the objective? If you have multiple goals, which ones did you achieve?

It's a little weird. Technically yes, but it's really unsatisfying because I couldn't really do it to the caliber I wanted, with larger values. The line between feasible problems and unfeasible ones was pretty much the same line between trivial and non-trivial problems which was underwhelming. That is, the problems I

was able to solve were pretty much the same problems that were easy, making my project a bit underwhelming.

I was able to accomplish all my subgoals except for verifying that all messages for a bitvector can be encoded and decoded properly.

0.0.4 What should I do to be able to verify that you achieved these goals? For example, which files should I view, how should I run your code etc.

You can mainly follow my readme file. Here I try to discuss the results.

But also in my submitted folder, you can check

- **./src**: Here you can find my SMT specifications
- **./plot_scripts**: Here you can find the graphs generators of the experiment
- **exp**: These are experiments that generate data