

# RNGs

Code can be found here: <https://github.com/c2003-tamu/413>

## Environment Setup

- Clone git repository
- Navigate to 413/rng directory
- Ensure gdb is installed

## Finding the Necessary Values for Recovery

A quick demonstration video on how the values were found can be found here:  
<https://youtu.be/KyQuAhqzzg8>

## Recovery Process

- Navigate to 413/rng
- Run command: `gdb ./ransom`
- Inside gdb:
  - Run command: `b *<value under location in values.txt>`
  - Run command: `i r eax`
  - Note value that is stored in `eax` for later use
  - Continue through the execution of the script
- Run command: `cat myfile.txt`
  - `myfile.txt` is now encrypted :(
- Run command: `gdb ./ransom`
- Inside gdb:
  - Run command: `b *<value under location in values.txt>`
  - Run command: `set $eax = <value found during first execution>`
  - Continue through the execution of the script
- Run command: `cat myfile.txt`
  - `myfile.txt` is now back to its original glory!