Cryptographic Tools

In this lab you will be required to use the following tools: OpenSSL, CrypTool, Sage and TrueCrypt to demonstrate the use of modern encryption ciphers. Make sure that OpenSSL (http://www.openssl.org/), CrypTool (http://www.cryptool.org/), Sage (http://www.sagemath.org/) and TrueCrypt (http://www.truecrypt.org/) are installed in your computer. OpenSSL, CrypTool, Sage and TrueCrypt are available in Windows and Linux Operating Systems.

The OpenSSL developers have built a benchmarking suite directly into the OpenSSL binary. It's accessible via the speed option. It tests how many operations it can perform in a given time. Run the benchmark test (using the $openssl speed command) and comment on the results you are going to get in one paragraph.

Investigate the use of CrypTool and Sage using the tutorial provided. You will be required to demonstrate its use on three ciphers during the lab.

Tutorials you may wish to use

1. http://www.madboa.com/geek/openssl/#benchmark-speed
2. http://soa.sys-con.com/node/1938050
3. http://security.sys-con.com/node/1947620
4. https://www.owasp.org/index.php/Cheat_Sheets
5. http://www.sagemath.org/doc/reference/cryptography.html