

Lab 3 Crypto with websites and math!

Goals:

1. Use websites for encryption and decryption.
2. Learn how to recognize well known ciphers.
3. Apply private and public key cryptography.

Preliminary Information:

There are several “old” no longer used ciphers that may be encountered in a CTF competition. The reasons to learn how to use and recognize these are:

1. It teaches you how to think about cryptography, starting from easy ciphers,
2. You may recognize weak ciphers used improperly in third party applications,
3. When you try to break a cipher, there are no instructions. By practicing and thinking like a cryptographer, you develop the skill.
4. You may find cryptographic puzzles out in the wild or custom algorithms designed by third parties. If you recognize information leakage and patterns may make you a better security analyst.

How we solve old ciphers:

1. There is a wealth of websites that have crypto solving tools. One of the richest ones that I have found is Rumkin Cipher: <http://rumkin.com/tools/cipher/>.
2. Search github for existent tools. Here is a simple search on cipher solvers: <https://github.com/search?q=cipher+solver>.
3. Create your own tool: at the end of the day, you may create your own custom cipher solver. That’s why we learn programming, right?

Part 1: Simple Cipher Attack

A set of ciphers can be found in the rumkin.com website: <http://rumkin.com/tools/cipher/>.

1. Familiarize yourself with those ciphers. Use the website to encrypt different messages.
2. Now try to break the following ciphers. You could try all possible ciphers from Rumkin tools but my recommendation would be to first try to recognize the cipher. Specifically, messages 1, 3, and 4 have some very distinct characteristics that you can recognize if you have looked at the cipher tools.

Message 1: 1-20-20-1-3-11 1-20 4-1-23-14 23-9-20-8 4-18-15-14-5-19

Message 2: y. Tshoem eE yteo obfe Pervoivdiednecnec eo,f oar ctohnes pailrla-csyee eiinnvgo levyyien go ft hGeo df,o usnedeer sh eorfe tohne tUhnei tUeSd \$\$S1t abtielsl ,a nhda st hbee eInl ltuamkienna tbi

