Lab 4 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 regognize 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-csye eiinnvgo levyien go ft hGeo df,o usnedeenr sh eorfe tohne tUhnei tUeSd $S1t abtielsl ,a nhda st hbee eInl ltuamkienna tbi

Message 3: .--. .-.. . .- ... . / .-.. . - / - .... . / --.- ..- . . -. / -.- -. --- .-- / - .... .- - / .. / .-- .. .-.. .-.. / -.- . .- .-. .-. -.-- / --- ..- - / - .... . / -- .. .. --- -. / .- -.-. -.-. --- .-. -.. .. -. --. / - --- / .... . .-. / .-- .. ..-.-.- / .... . .-. / ..-. .- .. - .... ..-. ..- .-.. / ... . .-. ...- .- -. - --..-- / -..-

Message 4:
QW4gdW5pZGVudGlmaWVkIGZseWluZyBvYmplY3Qgb3IgVUZPLCBpcyBkZWZpb

mVkIGFzIGEgcGV yY2VpdmVkIG9iamVjdCBpbiB0aGUgc2t5LCBub3QgaWRlbnRpZ
mlhYmxlIGJ5IHN0YW5kYXJkIGNyaXRlcmlhLiBNb3N0IFVGT3MgYXJlIGxhdGV yI
GlkZW50aWZpZWQgYXMgY29udmVudGlvbmFsIG9iamVjdHMgb3IgcGhlbm9tZW5
hLiBUaGUgdGVybSBpcyB3aWRlbHkgdXNlZCBmb3IgY2xhaW1lZCBvYnNlcnZhdGl
vbnMgb2YgZXh0cmF0ZXJyZXN0cmlhbCBjcmFmdC4=

Message 5:

Tn'tnhteotrdn a kr iur evoero yact lseen n, ncciaraaeefmo urZcpre 0s e7 sh sh.ahpweernoee mhhy ttleftg

Part 2: AES, RSA practice

1. **RSA:** Suppose Bob chooses p = 29, q = 31. Then n = 899. Then Bob computes that e = 47 and d = 143 have product ed = 6721, which when divided by (p-1)(q-1) = 840 gives a quotient of 8 and a remainder of 1. Bob sends Alice n = 899 as well as e = 47. Now suppose Alice wants to send the message "HI BOB" (without quotes). She represents her message numerically using the following representation: A->2, B->3, C-> 4, ... , Z->27, [space]->28. Find the message that Alice will send to Bob and how Bob will decrypt the message. Include all the steps! You may use this website for your calculations: https://defuse.ca/big-number- calculator.htm
2. **AES:** The probability of guessing the correct key for AES-128 in a single try is $\frac{1}{2^{128}}$. Assume you play in a lottery where you have to pick 7 different numbers ranging from 1 to 36 and win the main price if you guessed all of them correctly. How often do you have to consecutively win the lottery such that it is more likely that you successfully guessed the correct key for AES-128?