ECE: Information and Network Security
Computer Project 1, Due Date: December 6, 2016

Project Description

In this project, your team (consisting of at most three students) will implement code to "break" AES using a brute-force search and conduct timing measurements for different (effective) key sizes. You are allowed to use whatever language you desire, and whatever library you desire. Of course, some languages will have advantages over other languages.

You will be provided a collection of files corresponding to four different plaintexts that were encrypted to produce four different ciphertexts using different 128-bit AES keys. To facilitate faster search, we provide starting points for your search that correspond to the first X bytes of the encryption key. These starting points correspond to "IV files" (motivated by the poor design of WEP, where the design gave away a significant fraction of the RC4 keyspace as a cleartext IV). Here are the specifics of the encryption

1. AES was used in ECB mode with 128-bit encryption.
2. Zero padding was applied for the last block to fill out the last 128bit block.
3. The four IV files range from 14 bytes down to 11bytes.
4. The actual 128-bit key can be represented as $K = [IV||\text{Unknown}]$. Your job is to find the unknown portion of the key for each of the four encryption cases.
5. All plaintext correspond to English phrases with punctuation (so commas and such are allowed).

To facilitate testing of your encryption/decryption code, we will also provide an additional *fifth* set of files that include plaintext, ciphertext and encryption key. You should use these to verify that your code is working properly before attempting to jump headlong into breaking the encryption. All files will be found on the class Sakai resource page.

You and your team must develop an effective search method for finding the missing key. It is recommended that you review the design of the EFF Cracker. You and your team must find each of the four keys and successfully decrypt the ciphertexts to produce the correct plaintexts. Additionally, all teams are expected to perform timing measurements to estimate how long it took to find the unknown key bits for all four cases.

Your team will turn in a short report (roughly 8 pages) that describes the approach you used and the explains your observations. Make certain to describe which language and libraries you used (if they are public), and submit a copy of your code. Your grade will be based upon the clarity and thoroughness of your report. Be sure to include the name of all team members on the report.