Exercises Lecture 7-8: Crypto!

July 23, 2020

1 Setup

Download and install openSSL for your appropriate platform, or use the Kali machine which has it pre-installed:
Windows: osradar.com
Mac: macappstore.org

2 Crypto - Defending against passive snooping

2.1 Old timey Caesar Cipher

The following message has been encrypted using ROT9.

CQRBR BJBCJ CNBNL ANC

When using alpha characters forciphertext it is normal to group the letters into 5 letter clusters, regardless of wordboundaries. This helps obfuscate any patterns.
Recover the message, and write it as a sentence. (I.e. 'PNRFN EPVCU RE' is 'CAESARCIPHER').

2.2 Diffie-Hellman

A shift cipher key is exchanged using the Diffie-Hellman method with g = 2 and p = 11. The actual numbers exchanged were X = 6 and Y = 5.
Find the resulting shared key.

Recall that Alice and Bob after agreeing on a g and p generates the secret keys x and y where after starting the key-exchange protocol

Alice $\rightarrow Bob : X = g^x \ mod \ p$
Bob $\rightarrow Alice : Y = g^y \ mod \ p$
Alice and Bob can then compute the shared secret
$k = X^y \ mod \ p = (g^x)^y \ mod \ p = (g^y)^x \ mod \ p = Y^x \ mod \ p$
Finding the keys is an infeasible task for very large primes in the place of variables g and p, but since the g and p here are the relatively low numbers 2 and 11, the keys can be broken by Brute-Force

2.3 AES

On learnit, you will find the files first.enc, second.enc and thirds.enc in a zip folder.
Each of these files are encrypted using openssl and use sha256 to generate keys from passwords. (-md sha256)

1. first.enc is encrypted using aes256-cbc with initialization vector 0
   - The password is the output of the Caesar cipher from earlier, written out as a proper sentence (Capitalization at the start, no punctuation)
2. second.enc is encrypted using aes128-cbc without a specified initialization vector
   - The password is the output of first.enc
3. third.enc is encrypted using camellia-256-ecb and outputs a pdf.
   - The password is the output of second.enc

Decrypt all of the files, then follow the instructions in the pdf.

Guide:
-iv lets you input an initialization vector
-in lets you input a file with text
-out lets you output a file as the result
-pass pass:"GoFish" inputs GoFish as a password

3 Crypto - Defending against active attacks

3.1 Java implementation

A blank file has been provided on learnit under the second lecture today. It is the skeleton for implementing symmetric encryption and MAC in Java (Probably useful in the future, who knows?)

Read up on the documentation of the libraries, then write yourself a program to transmit a message using symmetric encryption.