# CSE 484 / CSE M 584 - Homework 3

This homework is focused on a variety of topics from the last ~third of the quarter, with the goal of giving you some more hands-on experience with various tools.

## Overview

- **Due Date:** Friday, May 31, 2019 at 5pm
- **Group or Individual:** Individual
- **How to Submit:** Submit a PDF via Canvas
- **Total Points:** 35 points across 3 parts

**Part 1: Web Tracking (10 points)**

Experiment with an anti-tracking browser add-on, such as Ghostery, Lightbeam, or Privacy Badger. Pick three websites (e.g., www.cnn.com, www.facebook.com, and www.weather.com -- though you may pick any sites), visit them with the add-on installed, and report on what you find.

**What to Submit:**

1. **(3 points):** Briefly describe (a few sentences) or sketch how third-party tracking allows advertisers or others to track users across multiple sites.
2. **(1 point):** Which add-on did you try?
3. **(6 points):** Include a screenshot of the add-on's output for each of the 3 pages you tested. How many trackers did you find on each page?

**Part 2: Android Encryption (15 points)**

In this part of the assignment, you will explore a vulnerability in how Android applications might use encryption. *Your goal:* Extract the encryption key from an Android application (without access to source code).

Download SimpleNotepad application here: SimpleNotepad.apk. This application lets users write notes, store them, and retrieve them. Because the developer knew that users might write private things in their notes, he/she decided to *encrypt* those notes before storing them on the device.

**What to Submit:**

1. **(5 points):** Find the encryption key used by SimpleNotepad, and briefly describe (one short paragraph) how and where you found it.

    *Hint:* You don't have any source code! :( But check out APKTool, which lets you decompile Android applications. (Note that you can download and run APKTool on attu without needing root; skip the step in the installation instructions about moving it to /usr/local/bin and just run it in place.)

2. **(5 points):** Briefly describe (one short paragraph) why it's a problem that SimpleNotepad's encryption key is hard-coded into the app, and explain what the developer of SimpleNotepad should have done instead.
3. **(5 points):** Identify at least one other way in which the developer of SimpleNotepad is not using best practices for encryption.

**Part 3: Password Security (10 points)**

Below we give you the entry for a password stored on a Linux machine. The password is weak. *Your goal:* find the password.

To do this, we recommend using either john or hashcat. We strongly recommend using Linux for this question (Use attu or a VM if you don't have a native Linux). You can likely install John the Ripper from the repository using apt-get or yum. The Linux package name is most likely john, e.g., for Ubuntu, run "sudo apt-get install john". Or, you can download john (John the Ripper 1.9.0 core release, from the link above) and build it from source (you will have to use this option if you are using attu; during build specify the architecture as linux-x86-64).

Here is the password entry, from a Linux machine (this should all be one line, without a line break or spacing in between):

```
charizard:$6$DKqj.x2L$TNkUAoEdXWMnaEt/6y.xfIWt/du/9Nq7dDUNsM174.cjXZXcn3bklz9lo5jWs2U7cw5dhQcMfNESqsWLW67JW/:17490:0:99999:7:::
```

**What to Submit:**

1. **(8 points)** The password
2. **(1 point)** What tool you used to crack the password
3. **(1 point)** Approximately how long it took the tool you used to crack the password