Tommy Huynh

April 29, 2015

CS 24: CS Scholars

Cryptography: From Mathematical Magic to Secure Computation

April 29 | 5:45 – 7:15 pm

The seminar I went to was about the science of communicating securely and the mechanisms that enable secure communication across the Internet. He had talked about a lot about the different programs and projects that he had worked on; be it physical or just some code. He went through the general seminar stuff, but there was one part that really intrigued me. At one point he brought up the topic of cryptography in a lot of Hollywood movies now a days that have to do with heists and stuff. He noted these crazy “matrix” looking machines that could crack encryption codes and that although that stuff sounds like crazy “mumble-jumble” it is quite possible in the near future. The field of cryptography is growing to the point where these movie things are becoming possible.

This, however, made me think of something that seems very obvious, but he did not really go over this fact. So if they’re making programs and mechanisms that could crack some of the most difficult encryption codes, then if they can in fact theoretically crack it, than does that not mean that that code is actually “smarter” than the encryption itself? So which one is harder to create, the encryption or decryption? It was a question that I was still pondering after I had left the seminar. But if I had to try to answer that question, I would say that trying to crack a code is harder than making a good code because you have to essentially create a program that has like a bunch of trial-error mechanisms and one that learns from each try, which seems very difficult and sounds like its approaching on AI territory. But then again, why not use AI to crack a code? Or just unplug the power cord to the encryption device.