ITIS 6200/8200 Principles of Information Security and Privacy

Weichao Wang

Fall Semester of 2017

Homework 1

Hand out: August 30th, 2017

Due time: September 6th, 2017, Wednesday, 11:00 am

1. There are two types of encryption algorithms: symmetric key encryption and asymmetric key encryption (also called public key encryption). To reach the same level of security, the key length for different algorithms can vary greatly. Please answer: to reach the same level of security as the 128 bit key for symmetric encryption algorithms, how long does the key need to be for RSA algorithm, and how long does the key need to be for elliptic curve cryptography?

Hint: You can search in Wikipedia and you will find the answers. This is to help you to understand the security comparison between the two encryption algorithm types. Remember, asymmetric encryption algorithms are not always more secure than their symmetric companions. Actually, if Quantum Computers become available, many asymmetric encryption algorithms may be cracked.

1. Please describe one example in computer security to show that cryptography cannot solve all problems in security.
2. Alice has a large text file (try a file at least 500KB). She wants to apply two operations to the file: compression (zip), and AES encryption. Please answer: when she applies the two operations in different orders, what will be the impacts and why?

To answer this question, I will need you to do two steps:

* 1. Generate (or download) a large text file (at least 500KB). Locate two software: one for AES encryption and one for compression. Now to the same source file, you apply the two operations in different orders. At the end, you will get two result files: one is encrypted then zipped, and the other is zipped then encrypted.

Now write down the file size of all five files: the original file, two intermediate files, and two final result files. Which result file is smaller?

* 1. Please explain why the zipped-then-encrypted file is smaller in size.

We do not restrict you to any specific software. But in my experiment, I use 7-zip and AEScrypt, both of which are free.

When you discuss the size of the files, please consider the following question. Which type of files have better compression ratio? A file that contains a lot of repeated patterns? Or a file that looks totally random? Which type of files contain higher randomness (or higher entropy): a text file or an encrypted file?