ITIS 6200/8200 Principles of Information Security and Privacy

Weichao Wang

Fall Semester of 2018

Homework 1

Hand out: August 31th, 2018

Due time: September 7th, 2018, Friday, 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 RSA 3072 asymmetric encryption algorithm, how long does the key need to be for a symmetric encryption 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. Encryption usually needs a feature called “Avalanche Effect”, which means a small change in the input will cause large changes in the output. In this task we will do some experiments. You will need: (1) a plaintext file you generate (not need to be large, 1k byte or so should be fine); (2) an encryption software (I use AEScrypt); and (3) a binary editor/viewer (such as CFF Explorer).

Use the encryption software to encrypt your text file. Then change 1 byte or 1 bit in the text file, encrypt it again. Now use the binary editor to compare the two cipher text files. Are the differences big or small? In your homework submission, you need to attach the screenshots of the text files, and two files opened with the binary editor.

Extra question: Use your binary editor to change 1 bit in the cipher text file. Then use the software to decrypt. What do you get? Do you get a decrypted file similar to the original text file? Or will the software refuse to decrypt? Why do you think this happens?