Cryptographic Algorithms, Evan, Daniel

RC4: For this portion of the project, I will implement and research RC4 in depth. When presenting on this info I will talk about RC4, what it is, it's history, and how it is implemented. RC4 is on the shorter and more concise side so I will be able to explain how it works during the presentation . In fact, covering how it works will be ~1/2 of this portion of the project's presentation. The example I will give is encrypting JSON data. This portion of the presentation will be composed of a PowerPoint and a Python example.

Resources:

Python, PowerPoint

References:

Leyden, John. "That Earth-Shattering NSA Crypto-Cracking: Have Spooks Smashed RC4?" *The Register® - Biting the Hand That Feeds IT*, The Register, 22 Dec. 2013, www.theregister.co.uk/2013/09/06/nsa_cryptobreaking_bullrun_analysis/?page=1.

WaterJuice. "WaterJuice/WjCryptLib." *GitHub*, github.com/WaterJuice/WjCryptLib/blob/master/lib/WjCryptLib_Rc4.c.

AES: For this portion of the project I will talk about the history behind AES, what it's impact is. Moreover, through code, I will show how to implement ciphertext stealing to shorten a ciphertext before running the AES algorithm. The idea is that I won't explain how AES works nor why it works, but just give an overview of what it is and what it is known for. Then, I will go into an example of using a package/packages to invoke an AES algorithm. Then utilizing a concept that is explained but not exemplified in our classes main textbook, Serious Cryptography, I will present a piece of code in Python I've written to perform ciphertext stealing. The deliverables will include the PowerPoint presentation, and the Python code example.

Resources:

Python, PowerPoint
Non-standard Python Libraries: cryptography, os

References:

Aumasson, Jean-Philippe. *Serious Cryptography: a Practical Introduction to Modern Encryption*. No Starch Press, 2018.

Computer Security Division, et al. "AES Development - Cryptographic Standards and Guidelines | CSRC." *NISTIR 8179 Criticality Analysis Process Model | CSRC*, csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development.