CSEP 590A Applied Cryptography - Spring 2019 – Project proposal

Project title: Merkle-Hellman cryptosystem, principles and vulnerabilities

Team members: Xuefei Li (Frank) and Bertrand Desmarest

Project Topic:

The Merkle-Hellman cryptosystem was one of the first systems based on public key encryption. It was published in 1978 by Ralph Merkel and Martin Hellman, around the same time as the RSA system, but did not achieve the same popularity, as it was quickly broken by several successful attacks in the early 80's. The Merkle-Hellman system is based on the subset sum problem (related to the "Knapsack" problem), which is known to be N-P complete, but solvable in polynomial time if the set of numbers is super increasing. The objective of this project is to understand and implement the Merkle-Hellman cryptosystem using Python. Then we will analyze the attack described by Adi Shamir in his paper "A polynomial time algorithm for breaking the basic Merkle Hellman" and provide an implementation of the attack using Python. We will then compare this system with the RSA system, and look at some recent knapsack-based cryptosystems.

Project Plan:

1. Introduce the Knapsack cryptosystem in a big picture – brief history, how it was applied in the real-world scenarios, implementation, and attacks that broke this system.
2. Discuss the difference between Merkle-Hellman Knapsack (MHK) algorithm with the current RSA algorithm, and what caused Knapsack algorithm to be vulnerable compared to RSA.
3. Understand the Merkle-Hellman Knapsack (MHK) encryption and decryption algorithms and implement it in Python to successfully encrypt and decrypt messages.
4. Discuss the challenges in Engineering perspective, for example, the data structures and performance of encryption and decryption.
5. Introduce one of the existing attacks that broke MHK – Shamir's method.
6. Reproduce the attack in Python.
7. Discuss any engineering issues, like data structures and performance, when implementing the attack.
8. Describe other Knapsack-based cryptosystem (tentatively the Chor-Rivest cryptosystem), and research whether they are considered secure or not.

Project Deliverables:

1. Paper report consisting of:
    a. Introduce the MHK cryptosystem, and compare it with the existing RSA algorithm from the perspectives of pseudocode, performance, security, etc.
    b. Introduce the Shamir's attack on MHK based cryptosystems (principle, pseudocode, performance, difficulty).
    c. Discuss other MHK-based cryptosystems.
2. Coding (in Python):
    a. The implementation of the MHK cryptosystem.
    b. The reproduction (implementation) of the Shamir's method that broke the MHK.