SPCS CRYPTOGRAPHY CLASS SYLLABUS

Instructor: Ho Chung Siu
Email: soarer@stanford.edu
Website: http://web.stanford.edu/ soarer/cryptography.html
Course Textbook: The course will be based on *Cryptography*, by Simon Rubinstein-Salzedo. We will also use *An Introduction to Mathematical Cryptography* by Hoffstein, Pipher and Silverman as a reference.

1 Course Description

This class is an introduction to cryptography and related Mathematics. The basic setup is the following: the innocent Alice and Bob wish to send messages to each other, and an eavesdropper Eve will try to intercept the message. How can Alice and Bob send messages so that they can understand each other, but the messages are unintelligible to Eve?

2000 years ago Julius Caesar approaches this problem using a cipher. Alice and Bob agree on a way to code messages so that each alphabet is replaced by another, for example A by D and B by E and so forth. Without knowing the coding scheme, Eve would not know how to understand the message. However, as we will see in the course, Eve can do a simple analysis to decode the message anyway.

In the 1970s, several mathematicians had another approach to this issue, discovering the idea of public key cryptography. Such ideas are now applied everywhere in life, for example when we use credit cards to buy things online. We will understand two basic public key cryptosystems in this course, the ElGamal cryptosystem and the RSA cryptosystem. We will also learn a few things about the practical security issues of such cryptosystems.

We will end the course with student presentations. Each student will do a short presentation on a topic related to number theory or cryptography not covered in class.

2 Course Syllabus

The syllabus is as follows,

1. Introduction
   - Classical cryptosystems and attacks to them: Caesar ciphers, Substitution ciphers, Vigenere ciphers, Autokey cipher, One time pad.
   - Number theoretic background: primes, Euclidean algorithm, modular arithmetic, Chinese remainder theorem, basic group theory.
   - Big O notation; Time complexity of algorithms.
2. Public-key cryptography
   - What is it, and why?
   - Diffie-Hellman Key Exchange, ElGamal Cryptosystem.
   - Hardness of ElGamal: the Diffie-Hellman Problem (DHP) and the Discrete Log Problem (DLP).
   - Basic algorithms for DLP: Baby step-Giant step algorithm, Pohlig-Hellman algorithm.
   - RSA and its hardness: the RSA problem and the factorization problem.
   - Basic algorithms for factorization problem: Pollard's ρ-method, $(p-1)$-method, quadratic sieve.
   - Implementation of RSA: Primality testing. Fermat test. Miller-Rabin test.
3. General attacks on Cryptosystem and defenses.
   - Ingredients of security: authentication, confidentiality, integrity, and non-repudiation.
   - Some information theory: Perfect secrecy, semantic security.
   - Attacks: Plaintext/Ciphertext attacks, Man-in-the-middle attack etc.
   - Defense: Hashing, MAC, Signatures, Padding
4. (If time permits) Symmetric-key cryptography. Block ciphers
   - Modern Standards: DES and AES.
   - Encrypting longer messages: Modes of operation. Initialization vectors.
   - Example modes of operation: CTR, CBC, OFB.