POSSIBLE PROJECT TOPICS

Guidelines:

- Each person should talk for around 10 minutes. Some project topics are big enough to accomodate a few people - in that case each person would still have to talk 10 minutes. You are strongly encouraged to work in groups/discuss among yourselves.
- Please let me know what your topic is once you have decided. Your topic should be finalized by **Tuesday, Jun 30**. The earlier you start, the more time you have to prepare for your presentation.
- The following are just some possible ideas. Feel free to come up with your own topic and talk to me about it.

1 Ciphers

1.1 Distinguishing Ciphers

In class we saw two classical ciphers: substitution cipher and Vigenere cipher. Given a ciphertext without knowing which cipher was being used, is it possible to tell which is which?

The answer is yes, by looking at frequency of letters. Substitution ciphers permute but do not change letter frequency, whereas Vigenere ciphers do change letter frequency, thus may look like random letters. Friedman's index of coincidence is a way to quantify and compare different profiles of letter frequency. It can also be applied to calculate key length of Vigenere cipher. *Reference:* [1, Chapter 5.4, 5.5], [2, Chapter 4.2].

1.2 Markov Chains and Substitution ciphers

Markov chain is an important concept in statistics, which can actually be used to attack substitution ciphers. This happened in real life - two former Stanford students Marc Coram and Phil Beineke introduced this idea to break a code by prisoner. The goal of this project is to understand what Markov chains are, and how they can be applied to attack substitution ciphers.

Reference: [1, Chapter 14].

2 Public Key Cryptography

2.1 AKS primality test

AKS primality test is a method to test whether a number is a prime. It is theoretically fast (provably polynomial time) and deterministic (in contrast with probabilistic tests like Miller-Rabin we see in class). The goal of this project is to understand what AKS primality test is, and why it works.

Reference: Andrew Granville's article here.

2.2 Solovay-Strassen primality test (1 person)

Solovay-Strassen primality test is another probabilistic testing for primes, which is based on Euler's criterion of quadratic reciprocity. The goal of this project is to understand what the test is, why it works, and its running time.

Reference: See here

2.3 Pollard's ρ method for discrete log problem (1 person)

Pollard's ρ method for factorization can be adapted for the discrete log problem as well. The goal of this project is to understand how this is done.

Reference: See [2, Chapter 4.5]

2.4 Merkel-Hellman knapsack cryptosystem

Merkel-Hellman knapsack crpytosystem was proposed in 1978, slightly earlier than RSA. It has since been broken, so is not used anymore. The goal of this project is to understand how it works, and how it can be attacked.

2.5 Introduction to elliptic curves

Elliptic curves are ubiquitous in Mathematics. The goal of this project is to understand what elliptic curves are, how to add points on elliptic curves, to prepare for later talks on cryptography or factorization.

Reference: See [1, Chapter 13]

2.6 Elliptic curves Cryptography

Diffie-Hellman Key Exchange is an idea that can be applied to other groups as well, so long as the Diffie-Hellman problem is hard to solve.

Elliptic curves over finite fields give rise to one such group. The goal of this project is to understand how Elliptic curve Diffie-Hellman works, and the hardness of Elliptic Curve Discrete Logarithm Problem.

Reference: See [1, Chapter 13], [2, Chapter 5.1-5.4].

2.7 Elliptic curves Factorization

Lenstra invented an algorithm to factorize large numbers, based on elliptic curves over finite fields. This is one of the fastest current algorithms. The goal of this project is to understand how this algorithm works.

Reference: See [1, Chapter 13], [2, Chapter 5.1-5.2, 5.6].

2.8 Lattice Cryptography

Although Quantum Computing is still at its infancy, a quantum computer (once built) will break Diffie-Hellman/RSA, making them unusable. There are known algorithms however, based on lattices, that are still secure against quantum computers. The goal of this project is to understand how lattices come in , for example, understanding the shortest vector problem.

Reference: See [2, Chapter 6]

3 Security of Cryptosystems

3.1 Information theory

Security/secrecy of a cryptosystem can be formalized in information theory. The goal of this project is to understand some basic notion of information theory (entropy, perfect secrecy).

Reference: See [2, Chapter 4.6]

3.2 Zero-knowledge proofs

Zero-knowledge proof is a protocol used in authentication. Peggy (the prover) will prove to Victor (the verifier) that certain facts are true, with giving Victor any information so that he can convince others the fact is true. The goal of this project is to understand how this works.

Reference: See [2, Chapter 8.3]

3.3 How does bitcoin work?

Bitcoin is one of the best known cybercurrency to date. The goal of this project is to understand how bitcoin works, and the cryptography involved in bitcoin.

Reference: See here.

3.4 What happened to Adobe?

Adobe was hacked back in 2013, resulting in password leakage of 150 million people. The goal of this project is to understand what happened, using the concepts we learnt in class.

Reference: See here.

3.5 Logjam

A new attack, Logjam, for Diffie Hellman was found last month. The goal of this project is to understand how it works.

Reference: See here.

4 Miscellaneous

4.1 The Enigma machine

The Enigma machine is a rotor cipher machine used in world war II by Germany and several other countries. This project would describe how the machine works, the history around it, and successful attacks against it in the war.

Reference: See here.

4.2 Coding theory

We do not discuss coding theory in class, but it is useful in several key steps of cryptography. For example,

- How does one effectively convert a literal message to strings of 0s and 1s?
- When Alice sends Bob the message, network issues may introduce errors in Bob's received message. Is there any way Bob can recover the original message?

The goal of this project is to understand how to solve the above two problems (and beyond).

Reference: See [1, Chapter 15].

4.3 Quantum Computing

Quantum computing is still at its infancy. But once a quantum computer is built, current encryption algorithms (For example, Diffie-Hellman and RSA) would be broken. The goal of this project is to understand one instance of this - Shor's polynomial time algorithm of factorizing large numbers, using quantum computer.

Reference: See here.

References

[1] *Cryptography*, by Simon Rubinstein-Salzedo

[2] *An Introduction to Mathematical Cryptography*, by Hoffstein, Pipher and Silverman