Department of Mathematics and Statistics
San José State University

Math 196W: Introduction to Mathematical Cryptography

Tues/Thurs 1:30-2:45 PM, MQH 424

What is this Course? We explore the **mathematics** under classical and modern cryptography, starting with classical Caesarian, substitution, Vigenere ciphers, through asymmetric-key cryptography such as RSA, Diffie-Helman, and ElGamal, and ending with relevant modern ideas such as hashing, the block chain / bitcoin, and elliptic curve cryptography. As an experimental course, the material is meant to be flexible, with topics based on class pace, background, and student influence(!).

What skills do I gain from it? The theoretical background of classical cryptography (such as number theory, probability, combinatorics, and algorithms), which will equip you with the mindset and mathematical skills to understand cryptography "under the hood." While the course certainly intends to help people with an interest in applied cryptography, we will **not** be working on implementation. After the course, you should become a stronger problem solver regarding problems that come up in cryptography. You will also gain the mathematical mindset to analyze, find weaknesses in, and create parts of cryptographic protocols on a theoretical level.

What background do I need? How hard is it? The only formal prerequisite is MATH 42 with a grade of "C" or better. As cryptography is related with many areas of mathematics, classes such as MATH 108, 126, 128A/B, 142, 179, or 161 are helpful (but not required), whether you are taking them now or have taken them in the past. This class will also serve to help prepare you for these classes if you have not taken them! The course requires some mathematical maturity. **You will be required to understand and write proofs.** As a course targetting math majors, we will *not* require background in or have work requiring computer programming; however, those skills would definitely help you learn the course!

What requirements does it satisfy? This class counts as an elective for the Applied and Computational Math major (both the standard and the Discrete Math tracks). It will also be allowed as an elective for CS on a case-by-case basis.

About the instructor: Yan X Zhang received his Ph.D. in Applied Mathematics from MIT in 2013 and recently completed the Morrey Visiting Assistant Professor postdoctoral appointment at UC Berkeley. He joined the faculty at SJSU in Fall 2016. This course will be based on his experience teaching an undergraduate cryptography course at UC Berkeley, also called "An Introduction to Mathematical Cryptography."