Possible topics for Math 116 project

Here are some possible topics for your term paper/project. These are just suggestions, just some of many possibilities. If you think of a cryptography-related topic that interests you that's not on this list, just run it by me for approval.

The list is roughly organized as follows: topics that are more abstract and/or rely more heavily on pure math are closer to the top of the list. Topics closer to the end of the list are more about real-world applications, and in many cases are somewhat softer on the abstract math. The last three items on the list are more historical than mathematical, but if you choose to do something like this, you are still expected to explore some mathematical aspects of the topic (for example, of some historical ciphers and/or their cryptanalysis.

Information theory

Homomorphic encryption (Probabilistic encryption of a group, preserving the group operation)

Zero knowledge proofs

Lattice methods in cryptography and cryptanalysis

Private information retrieval

Identity-based cryptography (Public-key cryptography in which a person's identity is their public key)

Secure multi-party computation

DC-nets (Perfectly anonymous communication, simple form of secure multi-party computation)

Threshold cryptosystems (A more general form of secret sharing)

Secret sharing (a.k.a. secret splitting: Encryption so that multiple parties must collaborate to decrypt)

Strong pseudo-random number generators (Especially Blum–Blum–Shub, Mersenne Twister)

Probabilistic encryption (Many possible ciphertexts for each plaintext. Examples, applications)

Enigma (The WWII German cipher: how it worked, possibly its cryptanalysis, etc)

Cryptanalysis of the Japanese “Purple” cipher from WWII

Digital cash systems (For example, Bitcoin. How they work, practical and theoretical issues)

Anonymous communication in practice (For example, anonymous remailers, the Tor network)

User authentication systems (OAuth, Kerberos, password authentication, single sign-on, etc)

SSL and related technology, such as X.509 (This makes up probably 95% of encrypted internet traffic)

WEP and WPA (WiFi encryption and authentication)

Describe an actual cryptography-related computer security incident, in depth: what went wrong, etc

Steganography: Hiding information “in plain sight”

Cryptography history from the WWII and early Cold War era

Cryptography history from ancient times through the 19th century

The politics of cryptography (esp. the “crypto wars” of the 80s–90s)