Cryptography
Final Project – Fall 2018

**Due Monday, December 17**

Choose one (and only one) of the following topics. When you choose a topic you must get my approval (I don't want everyone choosing the same topic). Write an essay of 2 – 5 pages clearly explaining the given topic. You are expected to cite all resources that you used for the paper. Also, all quotations must be properly cited. You **must** email me your final paper (hard copy will not be accepted).

## POSSIBLE TOPICS

(1) Explain how Bitcoin and blockchain work. You must discuss their relevance to cryptography.

(2) Explain how DES and AES work. Be sure to discuss the algorithms and how they are actually used.

(3) Explain the concept of a zero knowledge proof in cryptography. Be sure to include real world applications.

(4) Discuss the man-in-the-middle attack. Be sure to explain how it works and how it can be detected.

(5) Discuss non-malleable cryptography. What is it, how does it work, and is it practical?

(6) Compare and contrast the random oracle model and standard model of cryptography.

(7) Security is the essential feature of cryptography protocols. Discuss universally composable security and the guarantees it makes. Discuss the importance of this new paradigm.

(8) The concept of confidentiality in databases has been a topic of recent discussion. Write a paper on the topic of differential privacy.

(9) Write a paper discussing the connections between cryptography and game theory.

(10) Cryptography is used to protect communications over a computer network. Explain and compare SSL (Secure Sockets Layer) and TSL (Transport Layer Security).

(11) In class we discussed Pollard's $p - 1$ algorithm for factoring large numbers. Discuss the number field sieve method for factoring.

(12) Discuss the MD5 hash function and its vulnerabilities.

(13) Discuss timing attacks and their relevance to RSA and Diffie-Hellman.

(14) One type of attack is called power analysis. Discuss both simple and differential power analysis and what measures can be done to protect against these attacks.

(15) Discuss the history of the German Engima machine and how it was finally broken.

(16) Discuss CRIME attacks and how it can be prevented. You should also discuss the related BREACH attack.

(17) Discuss the class of RSA attacks known as Coppersmith's attack. Include the LLL lattice basis reduction algorithm.

(18) Discuss the RSA attack known as the ROCA vulnerability. Is it possible to prevent this attack?

(19) Discuss the history and continuing relevance of PGP (Pretty Good Privacy).

(20) Discuss codes that have never been broken. You may want to look at the following (but do not limit yourself to only these examples): Beale ciphers, the Shugborough inscription, and the Zodiac killer.

(21) Discuss the Playfair cipher and possible attacks on it.

(22) Discuss ID-based cryptography. What is the purpose of this and what limitations does it have?

(23) We discussed Diffie-Hellman key exchange between two people. Explain how this would work if you wanted to share keys among three people. You should include a discussion of the Weil pairing.

(24) Discuss the potential impact of quantum computing on cryptography.

(25) Homomorphic encryption is a topic of interest in the areas of secure cloud computing and secure voting systems. Discuss this topic, including information on fully homomorphic encryption.

(26) Discuss password cracking, including the topic of Rainbow tables.

(27) A robust combiner combines different encryption schemes. The idea being that even if some of the individual parts are insecure, the whole scheme remains secure. Discuss robust combiners.

(28) Compare and contrast deterministic versus probabilistic encryption.

(29) Discuss garbled circuits. This allows to parties who do not trust each other to communicate securely.

(30) Discuss the topic of verifiable computations, include Pinocchio.