

MATH 445, SPRING 2008

PROJECT SUGGESTIONS

Standards. Your project may be on any topic related to cryptology, and does not need to be purely technical; for instance, it is perfectly fine to produce an analysis of some historical incident in which cryptology played a role, or a discussion of social or political aspects of cryptography. However, simply recounting a narrative of events will not suffice – your paper needs to have a thesis.

Projects may be roughly divided into two types: *study projects* and *implementation projects*. Study projects will involve researching a topic and writing a paper of roughly 10 pages. In an implementation project, you will implement a cryptographic protocol, an attack on a cryptosystem, or something of this nature. It is permitted to mix aspects of both types.

An “A” study project will involve significant analysis and synthesis, and it will be well-written and professionally presented. An “A” implementation project will be a complete package allowing for easy compilation, demonstration, and testing of the algorithms involved, it will perform well on standard hardware, and it will adhere to high standards of coding and documentation.

Dates. A proposed topic will be due on **Monday, March 10**. A longer description of your project subject and goals (and, if possible, an outline) is due on **Friday, April 4**. The project itself is due on **Friday, April 25**. If revisions are required, they will be due on **Monday, May 5**.

Plagiarism. Plagiarism is the use of someone else’s ideas, words, code, etc., without proper attribution. It is an unforgivable offense in academic settings and will be dealt with harshly. Anyone caught plagiarizing in his or her paper will be very unlikely to pass the course. If you have any doubt about what is allowable, please ask me as soon as possible.

Suggested topics. This list is not exhaustive – you are welcome to propose another topic that interests you.

- (1) Brute force attacks on DES.
- (2) Common data compression algorithms – zip, tar, rar, etc. and their relative advantages and disadvantages.
- (3) Cryptography in a resource constrained application (such as smart cards, cell phones, or ATMs).
- (4) Cryptography on the internet: SSL, ssh, https, their strengths and weaknesses.
- (5) DVD encryption and how it was broken.
- (6) Electronic voting.

- (7) Elliptic curves in cryptography. (This topic is only reasonable if you have some knowledge of elliptic curves already.)
- (8) Factoring: the Elliptic Curve Method (mathematically sophisticated).
- (9) Factoring: the Number Field Sieve (mathematically sophisticated).
- (10) Finite fields, theory and computation.
- (11) Foreign export/import of cryptography – laws and surrounding issues.
- (12) Hashing.
- (13) Japanese ciphers in World War II.
- (14) Kerberos.
- (15) Magnetic stripe data storage and (in)security.
- (16) Pretty Good Privacy (PGP) – social, political, technical aspects.
- (17) Power analysis attacks.
- (18) Primality testing: probabilistic and deterministic tests, “primes is in P” (the AKS algorithm).
- (19) Random numbers: generating them and testing for randomness.
- (20) Review a book on cryptography or security. (One possibility, among many: “Privacy on the Line,” by Whitfield Diffie and Susan Landau.)
- (21) Simulation of a machine cryptosystem *other than* Enigma (e.g. PURPLE or a Hagelin machine).
- (22) Survey of the AES finalists.
- (23) The LLL (Lenstra-Lenstra-Lovasz) algorithm.
- (24) The Merkle-Hellman (knapsack) and McEliece (coding theory) cryptosystems.
- (25) The NTRU (lattice) cryptosystem (mathematically sophisticated).
- (26) The Solitaire cryptosystem.
- (27) The *U.S.S. Liberty* incident.
- (28) The *U.S.S. Pueblo* incident.
- (29) The VENONA project.
- (30) Timing attacks.
- (31) WEP and WPA wireless encryption.
- (32) William Friedman and the Black Chamber.