April 20, 2000

Policy review for the final exam

Exam conditions Again, the final exam will be "open book, open notes". You may bring to the exam anything additional to help you which is *non-living*.

Students in this course should be able to discuss with some knowledge certain issues intertwining mathematics, communications, and social and political policy. What *can* be done according to currently understood technology? What is politically and socially feasible? What is legal? Some specific topics are listed below.

- Write a paragraph or two making a case on behalf of the FBI regarding the regulation of import and export of cryptographic material.
- Write a paragraph or two explaining the controversies that surrounded the introduction of the Data Encryption Standard in the 1970's.
- Write a paragraph or two explaining why an encryption standard might be useful.
- Write a paragraph or two on how encryption might affect an electronic marketplace.
- Write a paragraph or two arguing on behalf of an insurance company regarding the privacy of medical records.
- Write a paragraph or two explaining real world uses of hash functions and digital signatures. Try to give at least one example where a mistake or weakness in the system used could have serious real-world consequences.
- Intellectual property: suppose you are a young jazz performing artist. Realistically, there may be 3,000 people in the U.S. who'd like to listen to you. What's your position on copyright?