

CSCI 283 - Computer Security I - Fall 2003
George Washington University

Project List.

You may suggest your own project too. In fact, all projects that have been assigned to students so far were suggested by the students themselves.

Implementation A project will consist of an implementation, a demo to the instructor, and a short written vulnerability analysis.

1. AES
2. DES
3. Digital Signature Schemes: MD4, SHA
4. Random number generators
5. Electronic voting
6. Copyright protection using cryptography
7. Watermarking (software or media)
8. Steganography
 - Characterization of images as channels for steganography
9. Computational Attacks on RSA
 - Computational factorization
10. Lying and data mining/statistics
11. Time Stamps
12. Biometrics
13. Visual cryptography

Theory A project will consist of a written survey of the field and an oral exam/presentation with the professor

1. Computational theory of secrecy: Micali-Goldwasser; Yao. (Needs knowledge of graduate level algorithms)
2. Blind signatures and electronic cash
3. Statistical Attacks (needs some comfort with statistics)
4. Quantum Crypto/Quantum computing and the security of standard crypto