CS359: Grading and projects

There will be one programming project that can be chosen on a first-come, first-serve basis from a list below. The project can be done in pairs (collaboration is strictly encouraged).

The goal of the project is to emphasize the algorithmic aspect of the problem, not the implementation details. In particular, you need not simulate a real-life environment with the server and the attacker residing on different computers. In timing attacks you can assume that you have access to the exact timing of encryption/decryption operations.

The project is due before the last class of the quarter (Dec 8). Project deliverables are expected to be the following: code, 2–4 page report explaining your attack method and summary of the results, and a 20 min oral presentation in the class.

Projects: (references are clickable in the electronic version of the document)

1. Find collision for MD4.
   X. Wang et al., "Cryptanalysis of the Hash Functions MD4 and RIPEMD."
   H. Dobbertin, "Cryptanalysis of MD4."
2. Implement Bleichenbacher's attack on PKCS #1.
   D. Bleichenbacher, "Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1."
3. Implement Wiener's attack on RSA with short private exponent.
   M.J. Wiener, "Cryptanalysis of short RSA secret exponents."

4–7. Mount a cache-timing attack against any of the AES process finalists, excluding Rijndael (MARS, RC6, Serpent, Twofish).
   Timing attack: D. Bernstein, "Cache-timing attacks on AES."
   AES finalists optimized C implementations: AES Source Code (web-page).

After you choose your partner and project, let Ilya know your selection by e-mail. If your project will not be covered in the class until late into the quarter, you should self-study relevant literature. Please schedule at least one meeting with Ilya in November to discuss your progress and any problems you may have with the project.