Suggested Projects List
Cryptography and Coding Theory (MAT 4930, Fall 2014)

Dmytro Savchuk

1. Implement automatic cracking of the Vigenère cipher
2. Implement automatic Hill cipher text encryption/decryption
3. Implement known plaintext attack for the Hill cipher
4. Implement RSA key generator that produces strong primes
5. Implement automatic RSA text encryption/decryption
6. Implement automatic ElGamal text encryption/decryption
7. Implement Miller-Rabin pseudo-primality test
8. Implement short plaintext attack on RSA
9. Implement Pohlig-Hellman algorithm for finding discrete logarithms
10. Implement index calculus algorithm for finding discrete logarithms
11. Implement the quadratic sieve method (see ex.28, p.196)
12. Implement the procedure that finds the smallest primitive root mod p that is greater than or equal to a given number
13. Implement digital signature algorithm and its verification for messages of length 160
14. Implement error-correction for the Hadamard code (p.396)
15. Implement error-correction for the Hamming codes (p.416)
16. Factor the 617-digit RSA-2048 challenge number (just kidding - but if you do factor it, let me know!)

Each project has to consist of 2 parts:

- Descriptive part describing the problem, introducing terminology, and explaining the ways the problem is being attacked. The quality (clarity, structure, and neatness) of this part will be evaluated.
- Implementation itself (the code) + examples of how it is applied. You can use any programming language of your choice.

All projects will be due on Dec 2, 2014 at 9:30am.