MAT 4930, Fall 2013

Cryptography and Coding

Topics for the second test

Discrete Logarithms:

- Definition
- Computing discrete logarithms (Pohlig-Hellman, Baby Step Giant step, Index Calculus)
- Diffie-Hellman key exchange
- ElGamal public key cryptosystem

Digital Signatures:

- The RSA signature scheme (signing/verification)
- ElGamal signature scheme (signing/verification)
- Concept and basic definitions of hash functions
- Birthday paradox and attack

Error Correcting Codes

- Hamming distance and code parameters ((*n*,*M*,*d*)-codes)
- Bounds on general codes (Singleton, Sphere packing, Gilbert-Varshamov)
- Linear codes (definitions, generating and parity check matrices, error detection and correction)
- Hamming codes