

## MATH 340: CODING THEORY PROJECT SUGGESTIONS

GREGORY D. LANDWEBER

- (1) Advanced Encryption Standard (AES). See, for example,  
<http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html>
- (2) Number theoretic cryptography
- (3) Data compression algorithms, such as Huffman compression
- (4) Quadratic Reciprocity codes (Section 6.8)
- (5) Codes modulo 4 (Sections 12.1 – 12.2)
- (6) Counting self-dual codes, mass formulas (Sections 9.5 – 9.6)
- (7) Lattices and sphere packings (Section 10.6)
- (8) Shannon's theorem (Section 1.11)
- (9) Reed-Simon codes and compact discs (Section 5.6)
- (10) Generating doubly-even codes. See the appendix to  
<http://arxiv.org/pdf/0806.0050>
- (11) MDS codes (Sections 2.4, 7.4)
- (12) Weight distributions (Sections 7.1, 7.2, 7.3)
- (13) Weight preserving linear transformations (Section 7.9)
- (14) Clifford codes (Viriya's senior project)