COMP 754 — Cryptography & Security — Aj. Phillip Rogaway
Problem Set #2 — Out: 10 July 02 — Due: 30 July 02 (in class)

Problem 1 Using the conventions used in AES, compute $\{\texttt{05}\} \bullet \{\texttt{a1}\}$.

Problem 2 Implement the encryption-direction of AES directly from FIPS-197. You may use any programming language you like. Use your implementation to compute $\text{AES}_K(M)$ where $K = M = 0^{128}$. Tell me the answer. Make *simplicity* the goal of your implementation, not speed. **There are many implementations of AES on-line; do not consult any implementation that others have done.**