Project 1

• Out of 85 points

• Grading
  – Submission (10 points + 10 points if submitted by Tu 11:59p)
  – Tarball worked (5 points)
  – Build worked (5 points)
  – Made keys (10 points)
  – MAC code (10 points)
  – Encrypt code (10 points)
  – Test on inputs (25 points)
    • Block-aligned, not block-aligned, less than one block, near max size, contains some 0 bytes
  – Test on attacks (10 points)
    • modify byte in data portion of encrypted message
    • modify byte in mac portion of encrypted message