Evaluating the Strength of AES

(Project Option #1)

Task Description

Your task is to evaluate the strength of the AES encryption algorithm, specifically its avalanche effect and bit independence among the various criteria (you may choose to do more). Try to be rigorous in the design of the evaluation processes, in particular the test cases. For the ease of demonstration, a Web interface to the evaluation processes is highly desirable. You may reuse free or open source software implementation of the AES encryption algorithm. Be sure to give due credits and provide proper references.

Consult the general guidelines (also on the course website) for deadlines and regulations.

Grading

Your project will be graded according to the quality of results achieved and the amount of work involved.

Useful Links

These links are provided for your convenience. You should always try to make sure that a downloaded program is safe to execute before actually executing it.

- The AES Lounge:
  `http://www.iaik.tugraz.at/content/research/krypto/AES/`
- AES Animation: `http://www.formaestudio.com/rijndaelinspector/`
- SAGE: `http://www.sagemath.org/index.html` (see also Appendix B.5 of Stallings' book, 5th or 6th edition)