Comparing the Speeds of HMAC and CMAC

(Project Option #3)

Task Description

Your task is to compare the speeds of HMAC and CMAC (Pages 390-391 and 395 of [Stallings 2014] respectively). For HMAC please use one of the SHA-2 algorithms as the hash function and for CMAC please use AES. Try to be rigorous in the design of the evaluation processes, in particular the test cases. It should be interesting to experiment with different hash-code sizes for the SHA-2 function and different key sizes for AES. 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 various algorithms. 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 Wikipedia page of HMAC contains links to several HMAC implementations; similarly for CMAC.
- 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)