Topics of projects - Applied Cryptography 2016/17

Analyze GCM (Galois Counter Mode) block mode of AES 128 operation a prove correctness of test vectors used in [1], p.28-29, test Case 3 and Test Case 4.

[1] **http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf**

Recommended sources of information and supporting materials:

[2] **http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf**
[3] **http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/carry-less-multiplication-instruction-in-gcm-mode-paper.pdf**
[4] C program for GF(128) multiplication used in GCM mode of encryption (see attached gf128.zip)
[5] any AES128 reference implementation (e.g. **https://github.com/kokke/tiny-AES128-C**
[6] **http://link.springer.com/book/10.1007%2F978-3-642-04101-3**

Final report must include:

- first page with identification of student, subject, and date
- detailed description of GCM mode functionality required for demonstrated proof
- commented C codes and makefiles that produce reference computations