E0254: Network and Distributed Systems Security

Assignment No. 2

Date given: October 9, 2017

Submission Due Date: October 29, 2017

Use output feedback (OFB) mode of block encryption to generate a sequence of bytes using AES block encryption function. Carry out suitable tests (including next-bit test) to find out whether the sequence of bits generated is cryptographically secure. Get this result for at least three pairs of input vector and shared secret key, and three different sizes (128, 192, and 256) of shared secret key (a total of 9 outputs). Now reduce the number of rounds (by reducing the main round function) in the AES block encryption function by half (5 for 128-bit key, 6 for 192-bit key, 7 for 256-bit key), and carry out the same test again using the same pairs of input vector and shared secret key. Then submit the following by e-mail (tarred and compressed files in a directory on or before October 29, 2017). You may use an existing implementation of AES in your program.

1. Source code of the program.
2. Description of each test program used.
3. Results for each test program for each pair of input vector and shared secret key used.
4. Your conclusions from the experiment.