INFSCI 2170/TELCOM 2820: Cryptography

Homework 7

Reading Assignment: Chapter 4.

1. Describe two ways in which you can generate a Message Authentication Code from a hash function. Draw block diagrams for each.
2. Why is using DES not secure for generating a hash function? Is triple-DES more secure?
3. Read Section 4.4.2 of the textbook and describe the operation of authenticated encryption using CCM.
4. Draw the block diagrams for generating a hash from a block cipher using the following algorithms:

   $$g_i = e_{g_{i-1}}(x_i \oplus g_{i-1}) \oplus g_{i-1} \oplus x_i$$

   $$g_i = e_{g_{i-1} \oplus x_i}(x_i) \oplus x_i$$

   $$g_i = e_{g_{i-1}}(x_i) \oplus x_i \oplus g_{i-1}$$

   In each case assume that there are n blocks of plaintext $x_1 || x_2 || x_3 || x_4 || \ldots || x_n$.
5. Do problem 4.7 from the textbook. Plot your results (q Vs ε) for both cases.
6. Go to http://csrc.nist.gov/groups/ST/hash/sha-3/index.html and describe in one paragraph the competition for SHA-3 and its result. Explain the pros and cons of the various candidate algorithms for secure hashing.