Homework 3

Due Thursday, February 24th, in class

(10 pts) 1. Data compression is often used in data storage or transmission. Suppose you want to use data compression in conjunction with encryption. Does it make sense to compress and then encrypt the data, or to encrypt and then compress the data? Justify your answer.

(10 pts) 2. Problem 5.1 from Bellare and Rogaway

(10 pts) 3. It has been suggested to obfuscate IP addresses by hashing them with MD5. Why is it feasible to invert MD5-hashed IP addresses even though MD5 is preimage-resistant?

(15 pts) 4. [BR] Problem 6.2

(10 pts) 5. It has been suggested to make a MAC out of a hash function by embedding the secret key into the hash input. For example, let the MAC key $K$ be 512 bits long, and let $\text{MAC}_K(M) = \text{MD5}(K || M)$. Show that this is completely insecure as a MAC by forging a message-tag pair. Remember, MD5 is a hash function (built using the Merkle-Damgård construction) and so is publicly computable. You can compute the MD5 compression function for any chaining values and message blocks that you like.

(15 pts) 6. [BR] Problem 6.3