Extra Credit 3

Due: May 7, 2018 at 11:59pm **Points:** 20

Questions

1. (*10 points*) Alice enciphers messages m and m' using the El Gamal cipher. Unfortunately, she uses the same random integer k. Eve intercepts the ciphers C and c' corresponding to the two messages, respectively. She learns m through various sources. But she only has the ciphertext c' corresponding to m'. Show how she can get m'.

2. (*10 points*) Assume that a cryptographic checksum function computes hashes of 128 bits. Prove that the probability is approximately 0.5 that at least one collision will occur after hashing $O(2^{64})$ randomly selected messages.