Extra Credit 2

Due: October 21, 2022 **Points:** 20

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