CS/ECE/MATH 435: HOMEWORK 9, DUE NOV 30.

1. What is the output after the first Feistel round of the DES algorithm in the case when both the plaintext and the key are all zero?

2. Alice knows that she will want to send a single 128-bit message to Bob at some point in the future. To prepare, Alice and Bob first select a 128-bit key k uniformly at random. When the time comes to send a 128-bit message x to Bob, Alice considers two ways of doing so.

She can use the key as a one-time pad, sending Bob $k \oplus x$ (meaning bit-by-bit addition). Alternatively, she can use AES to encrypt x. Recall that AES is a 128-bit block cipher which can use a 128-bit key, so in this case she would encrypt x as a single block and send Bob its encryption $\mathrm{AES}_k(x)$. Assume Eve will see either $k \oplus x$ or $\mathrm{AES}_k(x)$, that Eve knows an initial portion of x (a standard header), and that she wishes to recover the remaining portion of x. If Eve has time to try out every possible 128-bit key k, which scheme would be more secure? Compare and evaluate the following arguments and indicate which one you agree with.

(a) The one-time pad would be more secure. Even if Eve tried all possible keys, she would not be able to recover the unknown portion of x. If AES was used, Eve could eventually learn the unknown portion of x.

(b) AES would be more secure. Even if Eve tried all possible keys, she would not be able to recover the unknown portion of x. If the one-time pad was used, Eve could eventually learn the unknown portion of x.

(c) They would be equally secure. Either way, Eve could eventually learn the unknown portion of x.

(d) They would be equally secure. Either way, Eve would not be able to learn the unknown portion of x.