UC, Berkeley, CS294-90, Cryptanalysis, Spring, 2013, Homework 3

John Manferdelli

1. A linear recurrence of length three generates the sequence 0011110. Find the next three elements of the sequence. (You've just broken an LFSR cipher).
2. Let a=(a_3, a_2, a_1, a_0) and b=(b_3, b_2, b_1, b_0) be a four bit quantities with a_0 and b_0 the least significant bits. Instead of making a non linear substitution using a table lookup, suppose c=(c_3, c_2, c_1, c_0)= a+b (mod 32) where "+" is ordinary addition with carry. Write each "c" bit as a boolean function over GF(2) of the "a" bits and "b" bits. Is it non-linear? What is the best linear approximation of c_0? c_2? Compute some differential characteristics of this function.
3. Suppose the linear equation α(p)+β(c)= γ(k) over GF(2) is true with probability p=.6, γ is linear, p represents the plaintext, c represents the cipher text, and k represents the key. You collect 20 corresponding plain/ciphertext pairs observe that α(p)+β(c) =1 for 11 pairs and 0 for 9 pairs. What is the probability that α(p)+β(c) =1?
4. Compute (symbolically) the key first 6 key bits for the second round of DES (no fair cheating).
5. (a) Prove that a single round of DES is a bijective transformation from $GF(2)^{64} \rightarrow GF(2)^{64}$, what percentage of such bijective transformations (over all possible round keys) does a single round of DES generate? Does a single round of DES have any fixed points? (A fixed point for a transformation T is a point x: T(x)= x)
6. Find a function f(x_1, x_2, x_3) whose best linear approximation is as bad as possible. What characterizes such functions?
7. Suppose g(x_1, x_2, x_3)= f(x_1, x_2, x_3)+ x_1+1. When will g have a better linear approximation than f? (+ is over GF(2)).
8. For S-box 1 of DES, what is the probability that the input difference 0x34, produces the output difference 0x4?