Assignment -1

Problem 1. Kleptography

Alice has purchased a closed-source encryption box from the Acme Corporation. The specification of the box says that it will take as input a 128 bit key K and a variable length message M, and will output EncCBC(K,M) with a random IV. Unfortunately, Alice can't check that the IVs are truly random. Alice can't inspect the box's internals, so it could have a mutable internal state that it uses to generate pseudorandom IVs.

(a) How can the Acme corporation effectively backdoor the hardware in a way that will be undetectable by polynomial-time black box analysis. That is, you should describe a back door which allows the Acme Corporation to find Alice and Bob's shared key in time which is polynomial in the number of messages sent by Alice.

However, if Alice (adaptively) tests her box on inputs of her choosing, she should not be able to distinguish between a back-doored box and an honest box. You may assume that every message plaintext is distinguishable from random bytes in time polynomial in the message length. Can you make your backdoor work even if Acme sees just one of the cipher texts generated by Alice?

Hint: The IV has as much information content as the key does, but the box generated it deterministically as a function of the key, that would be detectable.

(b) Now Alice is convinced that she can't trust the box, so she demands proof that she can trust Acme. Design a new specification for the generation of the IVs such that:

- Alice can verify the correctness of her box's outputs.
- A correct box does not compromise the confidentiality of encrypted messages.

Problem 2. Kalns

Ben Bitdiddle has designed a new cryptosystem called Kalns, but we suspect it might not be as strong as we would like to be. Therefore we ask your help to break it.

In this problem we will be working with a finite field GF16. The elements of our field are all 4-bit strings. The field addition is computed as XOR: GF16(x) + GF16(y)= GF16(x $\oplus$ y). We provide the two tables describing addition and multiplication laws on the course web page.

If you are curious, these tables are obtained by interpreting 4-bit field elements as degree ≤ 4 polynomials

over GF2 and performing addition and multiplication modulo the irreducible polynomial $x^4 + x + 1$. However, for the purposes of this problem you do not need to understand how our GF16 is constructed; the solutions we know assume black-box access to GF16. We have provided a GF16 implementation for you. Kalns is a 64-bit block cipher. The secret key consists of three parts:

- an invertible 16-by-16 matrix A over GF16;
- a 16-element vector b over GF16; and
- a permutation (bijection) S that maps GF16 one-to-one and onto GF16.

To encrypt a 64-bit block B we first break it up in sixteen 4-bit chunks and interpret each of them as a GF16 element. So block B corresponds to length 16 vector x =(x0,...,x15) over GF16.
The encryptions consists of the following: y = S(Ax + b), where the permutation S is individually applied to each of 16 elements of v = Ax + b. The 16-element vector y is later re-interpreted as 64-bit integer to obtain the encrypted block B'.

a) Ben suspects that his cryptosystem is very secure. After all it has around 1616 ^2 . 1616 ^2 . 1616 ^2 ≈ 21132.25 possible keys. However, we suspect that there are many equivalent keys. These keys have different values for (A, b, S), but produce the same ciphertext for any given plaintext. Is our suspicion well-founded?

b) Describe a chosen-ciphertext attack on Kalns that recovers the unknown key (A, b, S) or an equivalent key.