COMP6453 Tutorial Week 3

1 Linear Block Ciphers are not CCA Secure

For any block cipher, the fact that it is a nonlinear function is crucial to its security. To see this, suppose that we have a block cipher that encrypts 256-bit blocks of plaintext into 256-bit blocks of ciphertext. Assume the following property holds:

$$Enc(k, m_1 \oplus m_2) = Enc(k, m_1) \oplus Enc(k, m_2)$$

for all 256 bit messages m_1, m_2. Describe how, with 256 chosen ciphertexts, an adversary can decrypt any ciphertext without knowledge of the secret key k. (A “chosen ciphertext” means that an adversary has the ability to choose a ciphertext and then obtain its decryption. Here, you have 256 plaintext/ciphertext pairs to work with and you have the ability to choose the value of the ciphertexts.)

2 Compare AES vs. DES

For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES.

1. XOR of sub-key material with the input to the f function
2. XOR of the f function output with the left half of the block
3. f function
4. permutation P
5. swapping of halves of the block

3 Cryptanalysis of the RC4 PRG

Recall that a PRG is considered secure if and only if given some i bits of PRG output, an ”efficient” adversary cannot predict bit $i + 1$ with nonnegligible probability. In this problem, we look at the RC4 PRG, which was previously used to encrypt (as a stream cipher) web traffic until its cryptanalysis.

The RC4 PRG works in the following way: we start with an array S of n bytes. We have $S[0] = 0, S[1] = 1, ..., S[n-1] = n-1$. Our first step is to randomly permute this array to get a new array S'. Now to generate our bitstream we apply the following algorithm:

```
$i = 0$
$j = 0.$
repeat until we get a long enough stream:
    $i \leftarrow (i + 1) \pmod{n}$
    $j \leftarrow j + S'[i] \pmod{n}$
    swap $S'[i], S'[j]$.
    output $S'[S'[i] + S'[j] \pmod{n}]$.
```

Show that the second byte of the stream generated is equal to 0 with probability $\approx 2/n$. (*Hint: Consider the event where* $S'[2] = 0$ *and* $S'[1] \neq 2$).