CS381 Exercise 6

Name: Zhang Yupeng

Student ID: 5130309468

1. Design a method of padding for DES, so that you can encrypt an 80-bit plaintext into 80-bit ciphertext in ECB mode. Can we do this with AES?

Solution:

Block cipher algorithms like AES and Triple DES in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) mode require their input to be an exact multiple of the block size. If the plaintext to be encrypted is not an exact multiple, we need to pad before encrypting by adding a padding string. When decrypting, the receiving party needs to know how to remove the padding in an unambiguous manner.

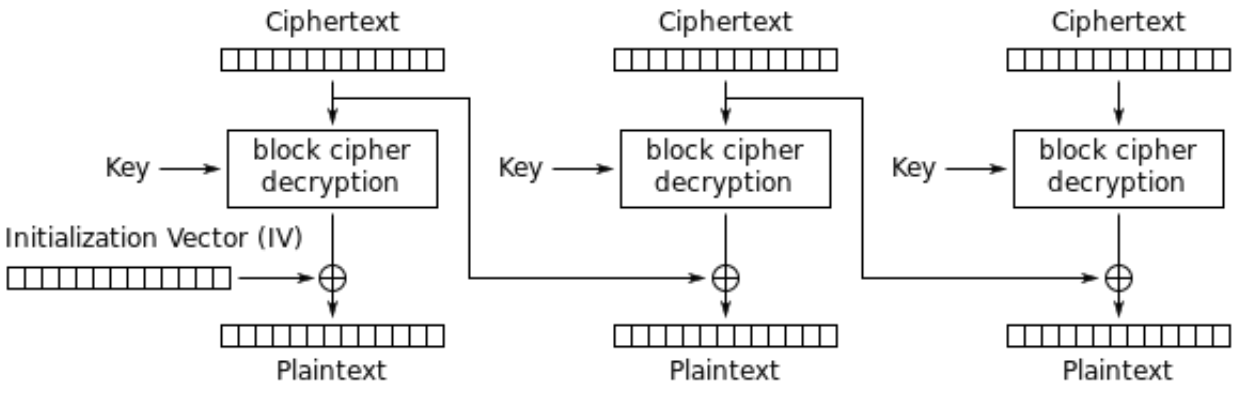
To solve the padding problem, we can pad with bytes all of the same value as the number of padding bytes. That is to pad the input with a padding string of between 1 and 8 bytes to make the total length an exact multiple of 8 bytes. The value of each byte of the padding string is set to the number of bytes added - i.e. 8 bytes of value 0x08, 7 bytes of value 0x07, ..., 2 bytes of 0x02, or one byte of value 0x01.

We can do this with AES as long as we change the padding string's length in order to match the AES's key's length.

2. Prove that in CBC mode, an error in ciphertext affects only 2 plaintext blocks;

Proof:

The following figure is the process of CBC mode decryption:



Cipher Block Chaining (CBC) mode decryption

By the picture we can see that mathematical formula for CBC decryption is:

$$P_i = D_k(C_i) \oplus C_{i-1}$$

So that the error occur in ciphertext block can only affect that plaintext block and the one immediately following it, but none after that.

3. Is pseudo-random number generator a one-way function, and why?

Solution:

Yes， a pseudo-random number generator is a one-way function.

Formally, pseudorandom generators exist if and only if one-way functions exist. That is

$$PRNG \leftrightarrow OWF$$

Consider a pseudorandom generator $Gl : \{0,1\}^l \rightarrow \{0,1\}^{2l}$. Let's create the following one-way function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ that uses the first half of the output of G_l as its output. Formally,

$$f(x,y) \rightarrow G_l(x)$$

A key observation that justifies such selection, is that the image of the function is of size 2^n and is a negligible fraction of the pre-image universe of size 2^{2n}.

To prove that f is indeed a one-way function let's construct an argument by contradiction. Assume there exists a circuit C that inverts f with advantage ε:

$$Prob[f(C(f(x,y))) = f(x,y)] > \varepsilon$$

Then we can create the following algorithm that will distinguish G_l from uniform, which contradicts the hypothesis. The algorithm would take an input of $2n$ bits z and compute $(x,y) = C(z)$. If $G_l(x) = z$ the algorithm would accept, otherwise it rejects.

Now, if z is drawn from uniform distribution, the probability that the above algorithm accepts is $\leq 1/2l$, since the size of image is $1/2l$ of the size of the pre-image. However, if z was drawn from the output of G_l then the probability of acceptance is $> \varepsilon$ by assumption of the existence of circuit C. Therefore, the advantage that circuit C has in distinguishing between the uniform U and output of G_l is $> \varepsilon - 1/2l$, which is non-negligible and thus contradicts our assumption of G_l being a pseudorandom generator.