# UEE4611 Assignment #6 Solution

**1.With the ECB mode, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode, this error propagates. For example, an error in the transmitted $C_1$ (Figure 7.4) obviously corrupts $P_1$ and $P_2$.**

**(a) Are any blocks beyond $P_2$ affected?**

**(b) Suppose that there is a bit error in the source version of $P_1$. Through how many ciphertext blocks is this error propagated?**

**(c) How many plantext blocks are affected at the receiver (after decryption)?**

(a)

No, since $P_j = C_{j-1} \oplus D(k, C_j)$ for $j \geq 2$.
So for any $P_j$, $j \geq 3$, $P_j$ is not related to $C_1$.

(b)

$C_1 = E(k, IV \oplus P_1)$
$C_j = E(k, C_{j-1} \oplus M_j)$
So, it can be obviously seen that all ciphertext blocks will be affected by the error of $P_1$.

(c)

After the decryption of the ciphertext, we will get the plaintext before it is encrypted.
So, we will get the plaintext with only $P_1$ occurs error.

**2.**

**(a) Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in CBC mode?**

**(b) How about decryption?**

(a)

No. Since the outcome of the previous block is needed for the encryption of present block, we cannot do the encryption parallelly.

(b)

Yes. While decryption only depends on ciphertexts which are known, so parallel decryption can be performed.

**3.Consider DES in CFB mode with $b = 64$ and $s = 8$. Suppose the Plaintexts $P_1, P_2, ..., P_{80} \in \{0,1\}^8$ are encrypted to the ciphertexts $C_1, C_2, ..., C_{80} \in \{0,1\}^8$, respectively, and then the ciphertexts are transmitted. If a bit error occurs in the transmission of $C_2$, which plaintexts are affected in decryption?**

The error occurs in the transmission of $C_2$, and $C_2$ will affect $P_2$, $P_3$,...,$P_{10}$ in the decryption. The reason why this happens is that every decryption we perform will shift 8 bits in the shift register. After $\frac{64}{8}$ rounds, the error disappears.

**4. Consider the following random number generator**

$$X_{n+1} = (aX_n) \mod 2^4.$$

**(a) What is the maximum possible period of this generator?**

**(b) What should be the value of $a$ with the maximum period?**

**(c) What restrictions are required on the seed in the case with maximum period?**

(a)

When a is even, we can easily find out that $a^4 \mod 16 = 0$, so the period does not exist.
When a is odd, $a^4 \mod 16 = (2n+1)^4 \mod 16 = 16n^4 + 32n^3 + 24n^2 + 8n + 1$
$\equiv 8n^2 + 8n + 1( \mod 16)$.
No matter n is even or odd, $8n^2 + 8n + 1 \mod 16 = 1$.
By the above conditions, we can know that the maximum period is 4.

(b)

Test all the odd number, we can find out the answer is $3, 5, 11, 13$.

(c)

The seed cannot be even, while it may cause $X_{n+1}$ be divided by 16 before it can reach the maximum period.

**5. RC4 has a secret internal state which is a permutation of all the possible values of the vector $S$ and the two indices $i$ and $j$.**

**(a) Using a straightforward scheme to store the internal state, how many bits are used?**

**(b) Suppose we think of it from the point of view of how much information is represented by the state. In that case, we need to determine how may different states there are, then take the log to base 2 to find out how many bits of information this represents. Using this approach, how many bits would be needed to represent the state?**

(a)

$256 \times 8 = 2048$
And we also need to store two indices i and j.
So we need a total of 2064 bits.

(b)

$\log_2(256!) + \log_2(2^8)^2 \approx 1700$ bits.

**6. Suppose you have a true random bit generator where each bit in the generated stream has the same probability of being a 0 or 1 as any other bit in the stream and that the bits are not correlated; that is the bits are generated from identical independent distribution. However, the bit stream is biased. The probability of a 1 is 0.5 $+\delta$ and the probability of a 0 is 0.5 $-\delta$, where $0 < \delta < 0.5$.A simple conditioning algorithm is as follows: Examine the bit stream as a sequence of nonoverlapping pairs.Then discard all 00 and 11 pairs. Replace each 01 pair with 0 and each 10 pair with 1.˜**

**(a) What is the probability of occurrence of each pair in the original sequence?**

**(b) What is the probability of occurrence of 0 and 1 in the modified sequence?**

**(c) What is the expected number of input bits to produce x output bits?**

(a)

$\text{P}(\text{pair}(0,0) \text{ occurs}) = (0.5-\delta)(0.5-\delta)$.
$\text{P}(\text{pair}(0,1) \text{ occurs}) = (0.5-\delta)(0.5+\delta)$.
$\text{P}(\text{pair}(1,0) \text{ occurs}) = (0.5+\delta)(0.5-\delta)$.
$\text{P}(\text{pair}(1,1) \text{ occurs}) = (0.5+\delta)(0.5+\delta)$.

(b)

$\text{P}(0 \text{ occurs}) = \text{P}(\text{pair}(0,1) \text{ occurs} \mid \text{pair}(0,1) \text{ occurs and the next pair is } (1,0))$
$= \frac{1}{2}$
$\text{P}(1 \text{ occurs}) = \text{P}(\text{pair}(1,0) \text{ occurs} \mid \text{pair}(1,0) \text{ occurs and the next pair is } (0,1))$
$= \frac{1}{2}$

(C)

For every two input bits, we output a bit if the input is 01 or 10 with probability $2(0.5-\delta)(0.5+\delta)$.

$E[x] = \frac{2x}{2(0.5-\delta)(0.5+\delta)} = \frac{x}{(0.5-\delta)(0.5+\delta)}$.