Cryptography Hw6 0716074 蔡育呈

#1
(a) No, ∵ P_3 只有和他的 input C_2, C_3 有关，更别說其他的
(b) P_1 會影响 C_1，C_1 影响 C_2，C_2 影响 C_3，... 其会影响 N 個 cipher text block.
(c) decryption 只有錯誤的 P_1 会有影响，其他 block 皆不受影响. ∴ 1個

#2
(a) No, ∵ CBC 的 encryption 需要上一個 block 的結果
(b) Yes, ∵ CBC 的 decryption 只需上一個对应 block input 的 ciphertext. 故可以同時執行.

#3 C_2 會作爲 input 影 P_2 和 P_3

#4 (a) $a=5, 3, 15, 11, 7$ ③ max period = 4
(b) a can be 3, 5, 11, 13
(c) $a=3 \rightarrow x_0 = 1 \text{ or } 5$ $a=11 \rightarrow x_0 = 1 \text{ or } 5$
$a=5 \rightarrow x_0 = 1 \text{ or } 3$ $a=13 \rightarrow x_0 = 1 \text{ or } 3$

#5 (a) $i=j=8$ (bits) $S=256 \times 8$ bits
$\Rightarrow 8+8+256\times 8 = 2064$
(b) $256 \times 256 \times 256! = 2^{1700} \xrightarrow{\log} 1700$

#6 (a) $P_{00} = (0.5-\delta)(0.5-\delta)$
$P_{11} = (0.5+\delta)(0.5+\delta)$
$P_{01} = (0.5-\delta)(0.5+\delta)$
$P_{10} = (0.5+\delta)(0.5-\delta)$
(b) $P_1 = \frac{P_{10}}{P_{01}+P_{10}} = 0.5$
$P_0 = \frac{P_{01}}{P_{01}+P_{10}} = 0.5$
(c) n = numbers of inputs pairs, $n(P_{01}+P_{10}) = X$
$n = \frac{X}{0.5-2\delta^2} \Rightarrow$ total input bit $= \frac{2X}{0.5-2\delta^2}$ #