

頁數	行數	錯誤	正確
44	2	沒有 L 的密文但是破解 Enigma 的也是一台機器	製作出難以破解的密碼，但是破解 Enigma 的也是一台機器
68	圖 3-7	圖中的箭頭畫反了	
73	倒數第 6 行	CUP	CPU
81	第 1 行	超級電腦「京」每秒的浮動小數點運算次數可達 1016 次，整個宇宙的基本粒子數量是 1087 個，所以宇宙的年齡為 1011 年。	因為超級電腦「京」每秒的浮動小數點運算次數可達 10^{16} 次，整個宇宙的基本粒子數量是 10^{87} 個，所以宇宙的年齡為 10^{11} 年。
100	圖 4-8	Alice 模擬的 CEC 模式	Alice 模擬的 CBC 模式
100	圖 4-8	明文(右上角區塊 4)	明文
110	3	前半部分的 8 位元是 nonce，每次加密時，必須是不同值。後半部分的 8 位元是區塊編號	前半部分的 8 位元組是 nonce，每次加密時，必須是不同值。後半部分的 8 位元組是區塊編號
142	倒數第 5 行	密文 = 明文 $E \bmod N$ (RSA 的加密)	密文 = 明文 $E \bmod N$ (RSA 的加密)
143	倒數第 3 行	密文 = 明文 $D \bmod N$ (RSA 的解密)	明文 = 密文 $D \bmod N$ (RSA 的解密)
144	表 5-2 最後一行	密文 = 密文 $E \bmod N$	明文 = 密文 $D \bmod N$
231	倒數第 9 行	使用 AEC 等區塊加密法也可以建立訊息認證碼	使用 AES 等區塊加密法也可以建立訊息認證碼
318	倒數第 9 行	這是利用金庫這個其他裝置來確保金鑰的機密性。	這是利用金庫這個其他裝置來確保金鑰的機密性。
329	圖 11-8	對話金鑰 (CKE)	對話金鑰 (CEK)
435	倒數第 3 行	PSP 網路	P2P 網路
449	5	混近公司裡	混進公司裡