資訊安全 HW3

F84086171 黃盈盛

1. 相同明文，金鑰差 1 bit:
   明文:Hello

   金鑰 1 : abcdefgh
   密文 1 : a618f2dc495b4774

   金鑰 2 : ibcdefgh
   密文 2 : 1e205ec12d64cd42

   兩個金鑰只有第一個 byte 不同，且在 ascii code 中 a 為 01100001，i 為 01101001，因此兩者相差 1 bit

   得出密文轉為二進制分別為

   1. 1010 0110 0001 1000 1111 0010 1101 1100 0100 1001 0101 1011 0100 0111 0111 0100

   2. 0001 1110 0010 0000 0101 1110 1100 0001 0010 1101 0110 0100 1100 1101 0100 0010

   於 64 bit 中有 31 個 bit 不同，差異比例為 31/64 * 100% = 48.4%

   密文差異比例:48.4%

2. 相同金鑰，明文差 1 bit:
   金鑰: abcdefgh
   明文 1 : Hello
   密文 1 : a618f2dc495b4774

   明文 2 : Helln
   密文 2 : a50d635449cd6b6c

   兩個明文只有最後一個 byte 不同，且在 ascii code 中 o 為 01101111，n 為 01101110，因此兩者相差 1 bit

得出密文轉為二進制分別為

1. 1010 0110 0001 1000 1111 0010 1101 1100 0100 1001 0101 1011 0100 0111 0111 0100

2. 1010 0101 0000 1101 0110 0011 0101 0100 0100 1001 1100 1101 0110 1011 0110 1100

於 64 bit 中有 19 個 bit 不同，差異比例為 19/64 * 100% = 29.7%

密文差異比例:29.7%