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%

**加密後差異比例:48.4%**

1. 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%

**加密後差異比例:29.7%**