對稱式密碼系統 補充3

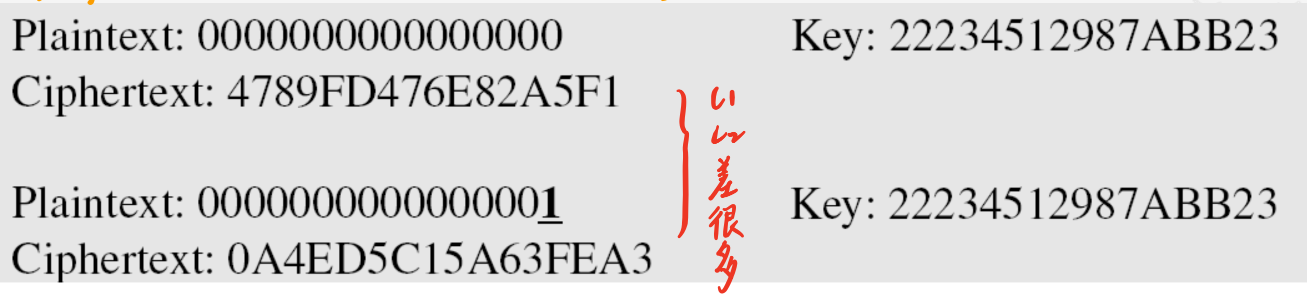
計網中心 網路與資訊安全組

李南逸

Avalanche effect 崩塌效應 ⇒ 好的密碼系統需具備

- Let us encrypt two plaintext blocks (with the same key) that differ only in one bit and observe the differences in the number of bits in each round.

↳ 改了其中 1 bit，也會造成加密後很大的改變



P1 Plaintext: 0000000000000000 Key: 22234512987ABB23

C1 Ciphertext: 4789FD476E82A5F1

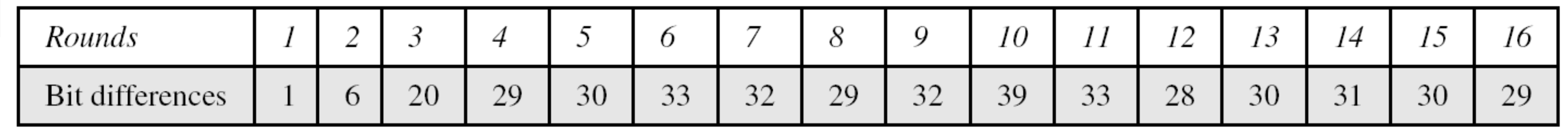
P2 Plaintext: 000000000000000**1** Key: 22234512987ABB23

C2 Ciphertext: 0A4ED5C15A63FEA3

C1 C2 差很多

Avalanche effect 崩塌效應

- Although the two plaintext blocks differ only in the rightmost bit, the ciphertext blocks differ in 29 bits. This means that changing approximately 1.5 percent of the plaintext creates a change of approximately 45 percent in the ciphertext. $\frac{29}{64} = 45\%$



Rounds	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*
Bit differences	1	6	20	29	30	33	32	29	32	39	33	28	30	31	30	29

作業3

- 請利用DES加密器舉出崩塌效應案例
  - 須包含兩類案例，第一是不同金鑰(相差1bit)加密相同明文，第二是相同金鑰加密不同明文(相差1bit)，計算其密文差異比例！
  - 繳交
    1. Pdf檔案
    2. 兩週內繳交
    3. 一人一組