Cryptology HW3

0916074
蔡馥旻

#1

ⓐ If $c=0$, choose $m_1, m_2 = 0$

$EL(k, 0\oplus 0) = EL(k,0) = EL(k,0) \oplus EL(k,0) = 0$

ⓑ

(i) C有bit是1

把 chosen ciphertext 只要 i^{th} 是1的就製造1個 C_i (其中ith bit=1, 其餘為0) 則 cipher c 可以被唯一的一組 C_i set ($i \in [1,256]$), 這些 C_i XOR 可以組成 c

↳ 這些 i 被收集在 $I_c = \{1, 2, \cdots, 256\}$

$$C = \bigoplus_{i \in I_c} C_i = \bigoplus_{i \in I_c} E(k, m_i) = E\left(k, \bigoplus_{i \in I_c} m_i\right)$$

ex. $11010 = 10000 \oplus 01000 \oplus 00010$

(ii) C為 all zero string

∵ linear 且 $E_L(k,0) = EL(k,0) \oplus EL(k,0) = 0$

∴ if $c=0$ then its plaintext $m=0$.

作法

Decrypt_without_key()

{ if C is zero string, then return $m=0$ ↗至多256次

else ask for the plaintext of C_i ($i \in I_c$)

($m_i, i \in I_c$)

return $m = \bigoplus_{i \in I_c} m_i$

#2

ⓐ $A \| B \xrightarrow{①} B \| F(B) \oplus A \to B \| 0 \oplus A \to B \| A$ $16 \div 2 = 8 \cdots 0$

$\xrightarrow{②} A \| B$

$\therefore A \| B$ #

ⓑ $F(M) = M$

$A \| B \xrightarrow{①} B \| F(B) \oplus A \to B \| B \oplus A \xrightarrow{②} B \oplus A \| B \oplus A \oplus B$

$\to B \oplus A \| 0 \oplus A \to B \oplus A \| A \xrightarrow{③} A \| B \oplus A \oplus A \to A \| B$

$16 \div 3 = 5 \cdots 1$

$\therefore B \| B \oplus A$ #

#3

ⓐ $L_{15} \| R_{15} \xrightarrow{T_{16}} R_{15} \| f(R_{15}) \oplus L_{15} \xrightarrow{T_{11}} f(R_{15}) \oplus L_{15} \| R_{15}$

$\xrightarrow{IP^{-1}\ IP\ T_{01}} R_{15} \| f(R_{15}) \oplus f(R_{15}) \oplus L_{15} \to R_{15} \| 0 \oplus L_{15}$

$\to R_{15} \| L_{15}$ #

ⓑ $L_{15} \| R_{15} \xrightarrow{T_{16}} R_{15} \| f(R_{15}) \oplus L_{15} \xrightarrow{IP^{-1}\ IP} \xrightarrow{T_{01}}$

$f(R_{15}) \oplus L_{15} \| f(f(R_{15}) \oplus L_{15}) \oplus R_{15}$

If we want to hold the above equals to $L_{15} \| R_{15}$.
then $f(R_{15}) = 0 \Rightarrow$ the righthand side become $f(L_{15}) \oplus R_{15}$
again, $f(L_{15}) = 0$, the condition is impossible because
function f is 1-to-1 (so that it exists inverse f^{-1})
$\Rightarrow$ It's impossible for $f(L_{15}) = f(R_{15}) = 0$

Hence, we disprove the equality.