2022 암호분석경진대회

1번 문제

다음은 n-bit 블록암호 E_K를 사용하는 한 인증모드에 대한 설명이다.

[블록암호 기반 인증모드 암호화 정의]

입력: nonce N, 메시지 $M = M_1 \| M_1 \| \cdots \| M_m$

출력: 암호문 $C = C_1 \| C_2 \| \cdots \| C_m$, 태그 값 T

$L = E_K(N)$

$\Sigma = 0$

$For\ i = 1 \sim m-1:$

$\Sigma = \Sigma \oplus M_i$

$C_i = E_K(M_i \oplus L) \oplus L$

$Pad = E_K(len(M_m) \oplus L)$

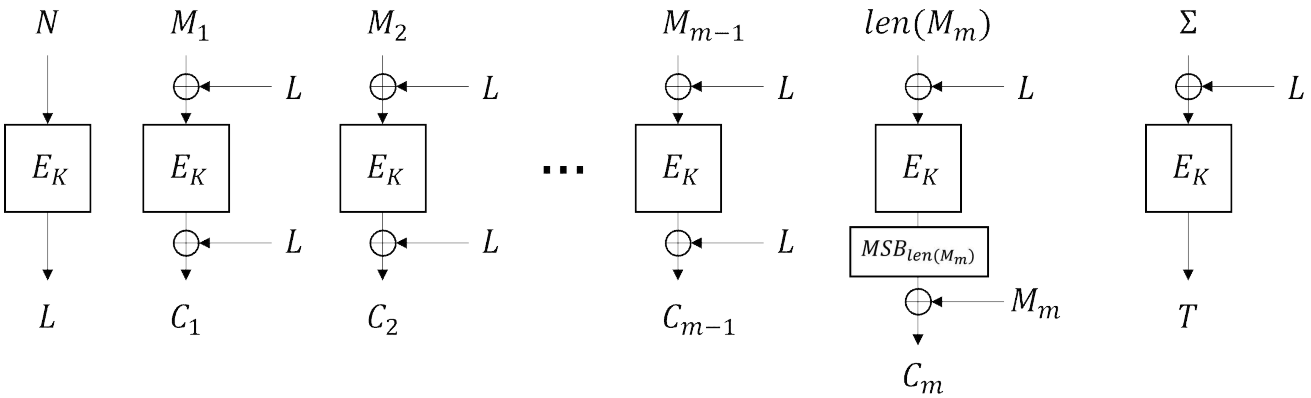
$C_m = M_m \oplus MSB_{len(M_m)}(Pad)$

$\Sigma = \Sigma \oplus Pad \oplus C_m \| 0^*$

$T = E_K(\Sigma \oplus L)$

$C = C_1 \| C_2 \| \cdots \| C_m$

return C, T



<블록암호 기반 인증모드 암호화 과정>

[블록암호 기반 인증모드 복호화 정의]

입력: nonce N, 암호문 $C = C_1 \| C_2 \| \cdots \| C_m$, 태그 값 T

출력: 메시지 $M = M_1 \| M_2 \| \cdots \| M_m$, 또는 False

$L = E_K(N)$

$\Sigma = 0$

$For\ i = 1 \sim m-1:$

$M_i = D_K(C_i \oplus L) \oplus L$

$\Sigma = \Sigma \oplus M_i$

$Pad = E_K(len(C_m) \oplus L)$

$\Sigma = \Sigma \oplus Pad \oplus C_m \| 0^*$

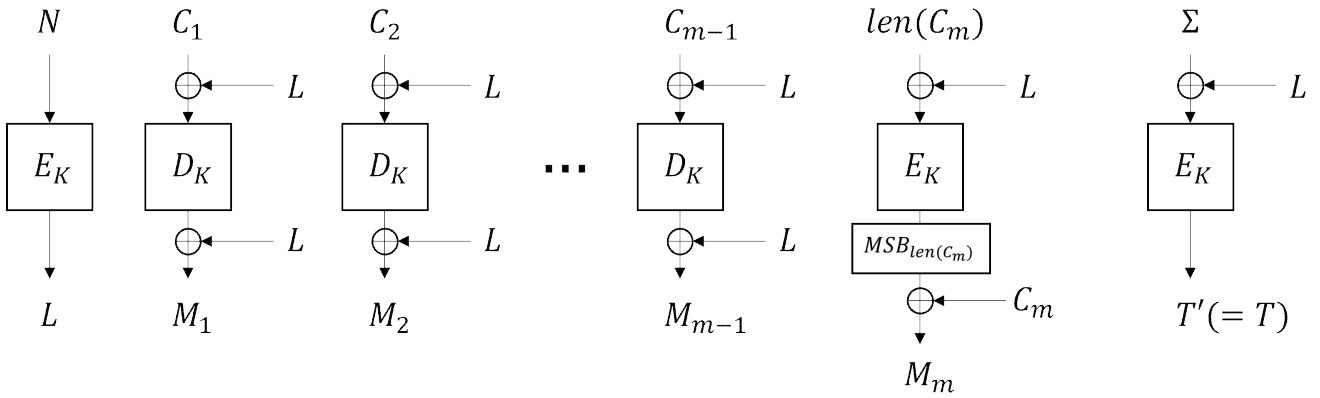
$M_m = C_m \oplus MSB_{len(C_m)}(Pad)$

$T' = E_K(\Sigma \oplus L)$

$M = M_1 \| M_2 \| \cdots \| M_m$

if $T' = T$ return M

else return **False**



<블록암호 기반 인증모드 복호화 과정>

- $len()$ 함수는 입력값을 이진비트열로 나타내었을 때, 그 비트 개수를 n-bit 크기의 자료형으로 출력한다.
  ex) 블록암호의 크기가 64-bit일 경우, $len(0b01011) = 0x0000000000000005$ (단, 0b와 0x는 각각 2진법, 16진법을 나타내는 표시이다.)
- MSB_b 함수는 입력값의 b-bit MSB(Most Significant Bit) 값을 출력한다.
  ex) $MSB_8(0x123456789ABCDEF0) = 0x12$
- $C_m \| 0^*$은 C_m의 크기가 n-bit와 같을 경우 C_m을, n-bit보다 작을 경우 그 차이만큼 LSB(Least Significant Bit)에 0을 연접한 값을 뜻한다.

[문제]

1. 만약 M_m의 크기가 블록암호의 블록 크기와 같다면 Σ는 어떤 형태인가?

2. 중복된 태그값을 갖는 메시지(혹은 암호문)을 찾는 것을 태그 위조공격(forgery attack)이라고 한다. 위에 제시된 인증모드에서 서로 다른 두 메시지(혹은 암호문)이 동일한 태그값을 갖게 만드는 위조공격을 설명하시오 (단, 공격자는 nonce를 재사용 가능함.)