2022암호경진대회 1번 문제

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

nonce N

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

$L = E_K(N)$

$\Sigma = 0$

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

$\Sigma = \Sigma \oplus M_i$

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

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

$\therefore \Sigma = \Sigma \oplus Pad \oplus C_m \| 0^* = \Sigma \oplus Pad \oplus C_m \ (\because len(C_m) = n)$

$= \Sigma \oplus Pad \oplus (M_m \oplus Pad)$

$= \Sigma \oplus Pad \oplus (Pad \oplus M_m)$

$= \Sigma \oplus (Pad \oplus Pad) \oplus M_m$

$= \Sigma \oplus 0 \oplus M_m$

$= \Sigma \oplus M_m$

$= M_1 \oplus M_2 \oplus \cdots \oplus M_m$

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.)

1. 새로운 평문 만들기

$encryption\ mode$:

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

$\Sigma = 0 \oplus M_1 \oplus M_2 \oplus \ldots \oplus M_{m-1} \oplus Pad \oplus (C_m \| 0^*),$

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

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

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

$Let\ M_{inject} = 00 \cdots 00(n\ bits).$

$M_{inject} \oplus (n - bit\ M_{any}) = M_{any}.$

$\because\ 0 \oplus x = x.$

$\therefore\ as\ long\ as\ M_{inject}\ does\ not\ compromise\ the\ integrity\ of\ each\ component\ of\ \Sigma,$

$it\ can\ be\ injected\ to\ M\ an\ arbitrary\ number\ of\ times.$

$\therefore\ A\ new\ plaintext\ M'\ can\ be\ generated\ by\ injecting\ M_{inject}\ into\ M$

$an\ arbitrary\ number\ of\ times\ in\ the\ places\ described\ below;$

$(i)\ before\ M_1;$

$(ii)\ between\ M_i\ and\ M_{i+1},\ 1 \le i < m;$

$(iii)\ after\ M_m.$

2. 새로운 암호문 만들기

$decryption\ mode$:

$Ciphertext\ C = C_1 \parallel C_2 \parallel \cdots \parallel C_m.$

$\Sigma = 0 \oplus M_1 \oplus M_2 \oplus \cdots \oplus M_{m-1} \oplus Pad \oplus (C_m \parallel 0^*),$

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

$Pad\ =\ E_k(len(C_m) \oplus L).$

$T' = E_k(\Sigma \oplus L).$

$Let\ C_{inject}\ =\ encrypt(M_{inject}).$

$\Rightarrow decrypt(C_{inject})\ =\ decrypt\left(encrypt(M_{inject})\right) = M_{inject} = 00 \cdots 00.$

$\therefore\ injecting\ C_{inject}\ in\ C\ in\ a\ way\ that\ does\ not\ change\ each\ component$

$of\ \Sigma\ will\ ensure\ T' = T$

$\because\ if\ each\ C\_i\ (1 \le i < m)\ is\ intact,\ then\ so\ will\ M\_i,$

$and\ Pad_{encrypt} = Pad_{decrypt}\ (\because\ len(C_m) = len(M_m).)$

$\therefore\ A\ new\ ciphertext\ C'\ can\ be\ generated\ by\ injecting\ C_{inject}\ into\ C$

$an\ arbitrary\ number\ of\ times\ in\ the\ places\ described\ below;$

$(i)\ before\ C_1;$

$(ii)\ between\ C_i\ and\ C_{i+1},\ 1 \le i < m;$

$(iii)\ after\ C_m.$