Sunandan Adhikary

21CS91R14

(2) $m \longrightarrow$ 

(i) ... $c_1 \oplus c_2 = v_1 \oplus v_2 = S[u_1] \oplus S[u_2]$

$= S[m_1 \oplus k_0] \oplus S[m_2 \oplus k_0]$

$= 1 \oplus 8 = 9$

(ii) ... $m_1 \oplus m_2 = u_1 \oplus u_2 = S^{-1}[v_1] \oplus S^{-1}[v_2]$

$= S^{-1}[c_1 \oplus k_1] \oplus S^{-1}[c_2 \oplus k_1]$

$= S^{-1}[1 \oplus k_1] \oplus S^{-1}[8 \oplus k_1]$

steps:

→ we can guess k_0 and derive eqn (i) and

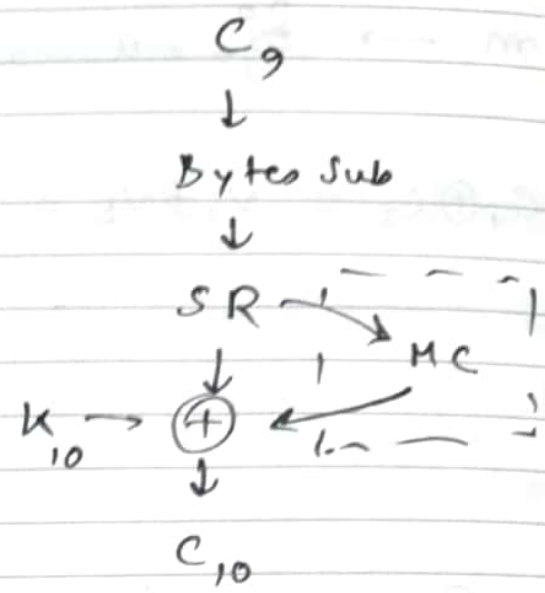
→ we can guess k_1 and derive eqn (ii) because

→ if we k_0 then we can get a relation between k_1 and k_0 i.e. guess m_1 and m_2 with further guesses and derive end value of (ii) [i.e. $m_1 \oplus m_2$]

(Proved)

③ Last round of AES :

$$C_{10} = SR[BSB[C_9]] \oplus K_{10}$$



with MC

(i) $C'_{10} = MC[SR[BSB[C_9]]] \oplus K_{10}$

(ii) $MC^{-1}[C'_{10}] = SR[BSB[C_9]] \oplus MC^{-1}[K_{10}]$

$\tilde{C}_{10} = SR[BSB[C_9]] \oplus \tilde{K}_{10}$ i.e. a new cypher with a new key without MC like eq (i)

∴ it adds no extra security and hence skipped at the last round to make the decryption algo steps symmetric to encryption.

④ Steps :

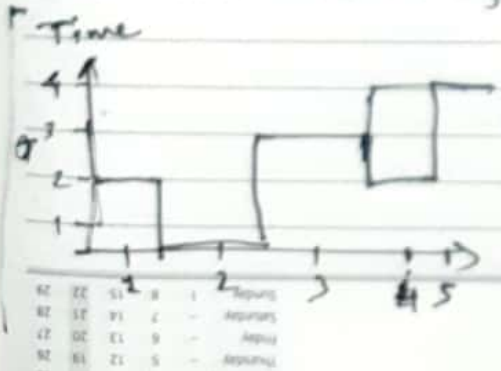
(i) We can log the time at start and of the execution and measure time for every A[i], A[j] pairs i.e. N×N iterations

(ii) the lowest time consumption will signify no swap i.e. $A[i] < A[j] \quad \forall j \leq N$

$\Rightarrow B[i] = 1$

(iii) As the time signature increase we can be sure there are more swaps i.e. if $T(A[i_1], A[j_1]) > T(A[i_2], A[j])$ $\forall j \leq N$

$\Rightarrow A[i_1] > A[i_2]$ and sorting these $T(i,j)$ values [Time sig] we can figure out $B[i_1] > B[i_2]$



← is the expected time consumption for given A $\Rightarrow T = [2, 0, 3, 1, 4, 3]$

$\Rightarrow B = [3, 1, 2, 5, 4]$ (Proved)

(1) $P(x) = x^m + x^n + 1 \Rightarrow x^m = x^n + 1$

$x^{m+1} = x^{n+1} + x$

$\vdots$

$x^{2m-2} = x^{n-2} + x^{m-2} + 1$

$A(x) = \sum_{i=0}^{m} a_i x^i$

$(A(x))^2 = \sum_{i=0}^{m} a_i^2 x^{2i}$

$\therefore$

~~$\therefore$ there will be only even coefficients even after~~

$\therefore C(x) = \sum_{i=0}^{m-1} c_i x^i$

$\therefore$ if i is even and $i < n$ or $i \geq 2n \Rightarrow c_i = a_i^2$

if i is $n < i < 2n \Rightarrow c_i = a_i^2 \oplus a_j^2$

$2n < j < 2m-2$

~~where $j \in [2n-2,$~~

if i is odd $i < n \Rightarrow c_i = a_j$.

$m < j < 2m-2$

if i is odd $i \geq n \Rightarrow c_i = a_i^2 \oplus a_j$

$m < j \leq 2m-2$