1. Bob's Exp.

a) Input : $f(x)$
Output : X's parity.

if $f(x)]_0 = 0$, Bob returns (0); /* even */ $\rightarrow p = 1$

else Bob returns (1); /* odd */. $\rightarrow p = \frac{2}{3}$.

b) If X is chosen at random.

Prob. that X is chosen even is $\frac{1}{2}$ and so, prob. that X is odd is also $\frac{1}{2}$.

If Alice is honest,

$$\Pr[\text{Bob success}] = \Pr[X \text{ is even} \wedge \text{Bob predicts so}] + \Pr[X \text{ is odd} \wedge \text{Bob predicts so}]$$

$$= \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot 1 = \frac{3}{4}.$$

c) Alice cheats Bob by changing parity of x so that $f(x)$ does not alter.

Case 1 : X is even.

$$f(x)]_0 = \begin{cases} A: 0, & p = \frac{1}{2} \Rightarrow \text{Bob returns } 0 \\ B: 1, & p = \frac{1}{2} \Rightarrow \text{Bob returns } 1. \end{cases}$$

Case 1A Alice cannot cheat.

Case 1B Alice can find X' with a diff parity such that $f(x) = f(x')$

$\therefore$ prob of Alice cheating Bob $= \frac{1}{2} \cdot \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot \frac{1}{2} \cdot 1$

$= \frac{1}{4}$.

Case 2 : X is odd.

$$f(x)\Big|_0 = \begin{cases} 0, & p = 0 \\ 1, & p = 1 \rightarrow \text{Bob returns } 1. \end{cases}$$

$\therefore$ Alice can find X' with a diff parity st $f(x) = f(x')$.

with prob $= \frac{1}{2} \cdot 1 \cdot 1 = \frac{1}{2}$.

$\therefore$ Net Pr $= \frac{1}{4} + \frac{1}{2} = \frac{3}{4}$.

2. Find $a^{n+1} \bmod n = a^{p+q}$.

Apply Pambda method to compute the Discrete Log, $(p+q)$.

Note that $p+q \approx n^{1/2}$.

$\therefore$ No. of steps $= O(\sqrt{n^{1/2}}) = O(n^{1/4})$.

3. $H(P|C) = H(P,C) - H(C)$

$= H(P,K,C) - H(K|P,C) - H(C)$

$[\because H(P,K,C) = \cancel{H(K,C) + H(P|K,C)}$

$= H(P,C) + H(K|P,C)$

$\leq$ (i) $H(P,K,C) - H(C) = H(C|P,K) + H(P,K) - H(C)$

$= H(P,K) - H(C)$ $[\because H(C|P,K) = 0]$

$= H(P) + H(K) - H(C)$ $[\because P$ and K are independent$]$

$= H(K|C)$.

4. Unicity Distance (U.D) $= \dfrac{\log_2 |K|}{R_L \log_2 |P|}$

K is the $m \times m$ matrix with elements in $\mathbb{Z}_{26}$.

$\therefore |K| = 26^{m^2}$. But all the matrices are not invertible $\Rightarrow |K| \leq 26^{m^2}$.

$|P| = 26^m$.

$\therefore$ U.D $\leq \dfrac{m^2 \log_2 26}{R_L \, m \log_2 26} = \dfrac{m}{R_L}$.

(5) $S_1 \times S_2 = ?$ $\quad S_1 : x + K_1 \mod 26$, $S_2 : x + K_2 \mod 26$.

$S_1 \times S_2 = x + K_1 + K_2 \mod 26$

$= x + K \pmod{26}$

$Pr[K = K] = \sum_{K_1} Pr[K_1 = K_1]\, Pr[K_2 = K - K_1]$

$= \sum_{K_1} \frac{1}{26} P_{K_2} = \frac{1}{26} \cdot = Pr[K_1 = K]$.

$\therefore \quad S_1 \times S_2 = S_1$.

(6) Use the fact ~~$f(c(a), K)$~~ for the non-linear part of DES: $f(c(a), c(b)) = f(a, b)$.

$\therefore$ $L^i = R^{i-1}$

$R^i = L^{i-1} \oplus f(R^{i-1}, K^i)$

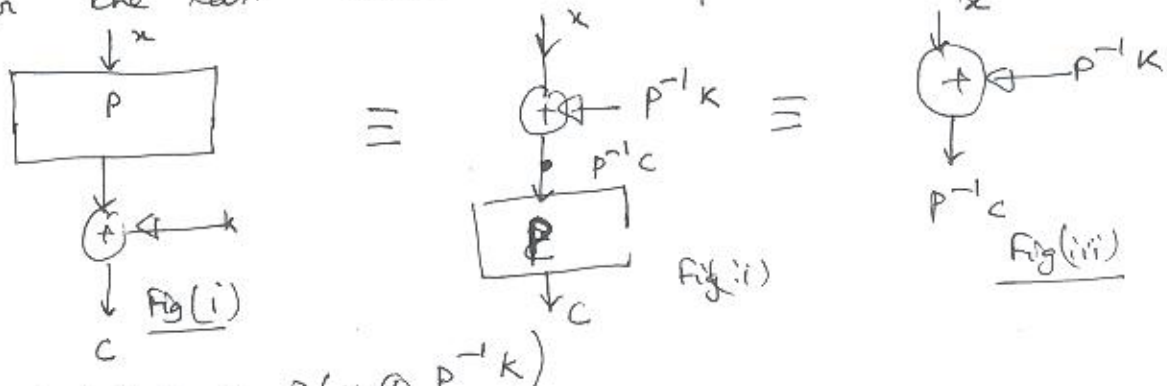
$\therefore \quad c(L^i) = c(R^{i-1})$

$c(R^i) = c(L^{i-1}) \oplus f(c(R^{i-1}), c(K^i))$

$\left[\because f(c(R^{i-1}), c(K^i)) = f(R^{i-1}, K^i)\right]$.

Continuing thus, we get the result.

7. Consider the last round has a permutation module P..



$C = P(x) \oplus K = P(x \oplus P^{-1}K)$

Fig(iii) shows that the last round permutation can always be eliminated.

(b) It is a rearrangement in $\{0, \ldots, 2^m - 1\}$.

So it is a permutation.

(8) If $(X_1 \oplus X_2)$ and $(X_2 \oplus X_3)$ are independent,

Bias of $X_1 \oplus X_2 = 2\epsilon_1\epsilon_2$ and that of $X_2 \oplus X_3 = 2\epsilon_2\epsilon_3$.

bias of $((X_1 \oplus X_2) \oplus (X_2 \oplus X_3)) = X_1 \oplus X_3$ is

$\epsilon_1\epsilon_3$.

i.e $2 \times 2\epsilon_1\epsilon_2^2\epsilon_3 = 2\epsilon_1\epsilon_3$.

or, $\epsilon_1\epsilon_3(4\epsilon_2^2 - 1) = 0 \Rightarrow (\epsilon_1 = \epsilon_3 = 0)$ or. $\epsilon_2 = \frac{1}{2}$.