1 a) assume F_k' is not a permutation $\therefore \exists$

x_1, x_1' & x_2, x_2' s.t -

$$F_k'(x_1 \| x_1') = F_k'(x_2 \| x_2') \quad x_1 \neq x_2, \; x_1' \neq x_2'$$

$$\Rightarrow F_k(x_1) \| F_k(x_1 \oplus x_1') = F_k(x_2) \| F_k(x_2 \oplus x_2')$$

As it is just a concatenation of two strings $\Rightarrow F_k(x_1) = F_k(x_2) \Rightarrow x_1 = x_2$.

Now $F_k(x_1 \oplus x_1') = F_k(x_2 \oplus x_2')$

$$\Rightarrow x_1 \oplus x_1' = x_2 \oplus x_2'$$

$$\Rightarrow x_1' = x_2'$$

which is a contradiction $\Rightarrow F_k'$ is a permutation.

b) let $x \in \{0,1\}^n$ & $x' = 0^n$ & the distinguisher D queries the oracle on $x \| x'$ In this case the output will be →

$$F_k'(x \| x') = F_k(x) \| F_k(x \oplus 0^n)$$

$$= F_k(x) \| F_k(x)$$

i.e. a $2n$ bit string with 2 stings of n bit which are same concatenated together

If the oracle was a completely random function then the output will be comming uniformly from $\{0,1\}^{2n}$.

$$\therefore \Pr[D^{F_k'}(1^{2n}) = 1] = 1$$

& $$\Pr[D^f(1^{2n}) = 1] = \frac{2^n}{2^{2n}}$$

$$\Rightarrow \left| \left(\Pr[D^{F_k'}(1^{2n}) = 1] - \Pr[D^f(1^{2n}) = 1] \right) \right| = 1 - \frac{1}{2^n}$$

$>>$ negl(n)

PAGE No.
DATE / /

2) Let the adversary A choose m_0, m_1 of dn bytes each.

m_0 is choosen such that

$$ctr + i + m_0^i = ctr$$

$$\Rightarrow m_0^i = 2^n - i$$

m_1 is choosen such that all m_1^i are random n bit strings

∴ The adversary will output '0' if he observes in the ciphertext that n bits are repeated 'd' times. with & '1' if this does not happen.

The Probability that A loses is $= \frac{1}{2^{dn}} * \frac{1}{2}$

$$\therefore \Pr\left[\text{PrivK}^{cpa}_{\Pi,A}(ctr, 1^n) = 1\right] = 1 - \frac{1}{2^{dn+1}}$$

$$\geq \frac{1}{2} + \text{negl}(n)$$

∴ this scheme does not have a indistinguisable encryption.