1. DES is comprised of rounds, having a round key and also a substitution layer. The substitution is non-linear and is combined with the key mixing by XOR.

Thus, if 'f' is the substitution and K_{r-1}, K_r are the successive round keys:

$$f(f(x \oplus K_{r-1}) \oplus K_r) \neq f^2(x) \oplus K'$$

because of the non-linearity of f, wrt $\oplus$.

Thus, the effective key is $\langle K_{r-1}, K_r \rangle$ for two rounds of DES. Likewise, composing DES helps in increasing the key length.

2. DES': DES × DES.

For p_i, $1 \leq i \leq l$, $\quad DES'(P_i) = C_i$

or, $\quad DES_{K_2}(DES_{K_1}(P_i)) = C_i$

or, $\quad DES_{K_1}(P_i) = DES^{-1}_{K_2}(C_i)$. $\forall i$.

QED.

3. Total number of keys, $(K_1, K_2) = 2^{2n}$.

We need to find out the probability with which a key : (K_1, K_2) will satisfy, $DES_{K_1}(P_i) = DES^{-1}_{K_2}(C_i)$, $\forall i$., $1 \leq i \leq l$. This probability for a given i is 2^{-n}, and for all the i's it is 2^{-ln}.

∴ Expected value of number keys satisfying the equation is $2^{2n} \times 2^{-ln} = 2^{2n-ln}$.

4. If $l \geq 2^n/m$, Exp. No of keys satisfying the equation,

$$DES_{K_1}(P_i) = DES^{-1}_{K_2}(C_i) \quad \forall i,\ 1 \leq i \leq l \text{ is}$$

$$2^{2n-lm} \leq 1.$$

Thus we will say to the attacker that if for a key (K_1, K_2) $DES_{K_1}(P_i) = DES^{-1}_{K_2}(C_i)\ \forall i, 1 \leq i \leq l$ then there is a very high probability that $K = (K_1, K_2)$ is the correct key.

5. L_1:

$DES_{K_1^1}(P_1), DES_{K_1^1}(P_2), \ldots, DES_{K_1^1}(P_l)$	K_1^1
⋮	⋮
$DES_{K_1^{2^n}}(P_1), \ldots, DES_{K_1^{2^n}}(P_l)$	$K_1^{2^n}$

L_2:

$DES^{-1}_{K_2^1}(C_1), \ldots DES^{-1}_{K_2^1}(C_l)$	K_2^1
⋮	⋮
$DES^{-1}_{K_2^{2^n}}(C_1), \ldots DES^{-1}_{K_2^{2^n}}(C_l)$	$K_2^{2^n}$.

That is, the attacker makes list L_1 with each row having the outputs after one DES with a possible key value for K_1. Each row has the output of l encryptions. There being 2^n values of K_1, there are same no. of rows.

Likewise, attacker has in list L_2, 2^n rows for possible values of K_2. Thus each row has the output of l decryptions with one DES, with the corresponding key value for K_2.

The attacker now searches L_1 and L_2, and looks for a match. There is a high chance that if the rows are i and j (resp for L_1 and L_2), the key $= (K_1^i, K_2^j)$.

Memory $= 2 \times 2^n (lm+n) = 2^{n+1}(lm+n)$ bits.

Encryptions / Decryptions $= 2 \times l \cdot 2^n = l \times 2^{n+1}$.

6. Known PlainText Attack (because the plaintext is known but not chosen).