Q2:

We have two approaches:
A: uses a password as a key to encrypt a fixed plain text. And then compare the resulting cipher text with a cipher texts stored in a file.
B: uses a password as plain text, and encrypt it using a fixed key. And then compare the resulting cipher text with a cipher texts stored in a file.

Approach A is considered to be more secure because each user has its own key (password). So there is only one pair of plain text and cipher text for this key.
So if some body knows the password of a certain user (the key), he can log onto that user computer only, but not to the other users computers, because he don’t know their keys (passwords).

While in approach B: The key is fixed for all users, and it is used to encrypt the passwords of all users, i.e. we have the same key for all users. So there are many pairs of plain texts and ciphers for this key and by applying one of the attaches, we can know the key. users. So if this key is known to some body, then he will be able to log into all the users computers, by encrypting the password and getting the cipher texts.

Q4:

We need to show that if we have $K : P \rightarrow C$ then using $K'$ we have $K' : P' \rightarrow C'$.

We know that $S = S' \oplus 11..1$

And from XOR properties we know: $S' \oplus 11..1 = S$.

Note: (’) means complement.

$Li = Ri-1$ ………………….1
$Ri = Li-1 \oplus f(ki, Ri-1)$ ……….2

But $Ri-1 = R’i-1 \oplus 11..1$, Substitute in eq 1:
$Li = R’i-1 \oplus 11..1$ , from XOR properties showed above:
$Li \oplus 11..1 = R’i-1$. But the LHS = $Li$;
$L’i = R’i-i$……………………………………..1’ .
Also we know that \( f(k_i, R_{i-1}) \) contains XOR operation: \( k_i \oplus R_{i-1} \)

But \( k_i = k'_i \oplus 11..1 \), substitute above we get:
\[ k'_i \oplus 11..1 \oplus R_{i-1} = k_i \oplus R'_i - 1 \]

So we will have \( f(k'_i, R'_i - 1) \)

As we know: \( L_{i-1} = L'_i - 1 \oplus 11..1 \)

Substitute these two results in eq2:
\[ \begin{align*}
R_i &= L'_i - 1 \oplus 11..1 \oplus f(k'_i, R'_i - 1) \\
R_i \oplus 11..1 &= L'_i - 1 \oplus f(k'_i, R'_i - 1) \\
R'_i &= L'_i - 1 \oplus f(k'_i, R'_i - 1) \\
\end{align*} \]

So from equations 1’ and 2’ we conclude that \( k' \) used to encrypt \( P' \) to get \( C' \)

Q5:
(a): Let \( k=11..1 \) be the DES key consisting of all ones. Show that if \( E_k(P) = C \), then \( E_k(C) = P \), so encryption twice with this key returns the plain text.

We need to show \( E_k[E_k(P)] = P \) ……………..1

Since we \( k = \) all 1’s, this means the any permutation process will result in a key of 1’s, so all the keys in the 16 rounds will be the same.
But we know that the decryption process is the same as encryption process, except we apply the keys in reverse order. But since all the keys are the same (\( k_{16}=k_1=..... \)), then the encryption and decryption will be the same, i.e. \( E_k(P)=D_k(P) \).

So if we substitute in eq1 we will get:
\[ D_k[E_k(P)] = P \]
And this is the proof.

(b): another key with the same property is all 0’s. \( k=0000….000 \).
also there are another two keys: which is half of the key is 1’s and other half is 0’s
\( k=11...100..0 \). or the reverse \( k= 00…011..1 \).