Diffusion and Confusion

Diffusion means that changing a character in the plaintext, changes several characters in the cipher text and vice versa.

An example of this is the hill cipher. The plain text (V) is a 1 x n matrix and the key (M) is an n x n matrix. The product of V and M is the cipher text w.

Let V = [$0 \quad 1 \quad 2$] and M = $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{bmatrix}$

Then the cipher text will be V.M = [$0 \quad 23 \quad 22$] (mod 26)

Let us change the plain text V to [$0 \quad 2 \quad 2$]

Now the cipher text will be [$4 \quad 2 \quad 2$] (mod 26)

Confusion means that to change even 1 character in the cipher text, several characters must be changed in the key.

Hill cipher can be cited as an example for this too.

Some ciphers that do not have these properties are Vigenere and substitution ciphers. This is why they are more susceptible to frequency analysis.