**الآن لفك التشفير:**

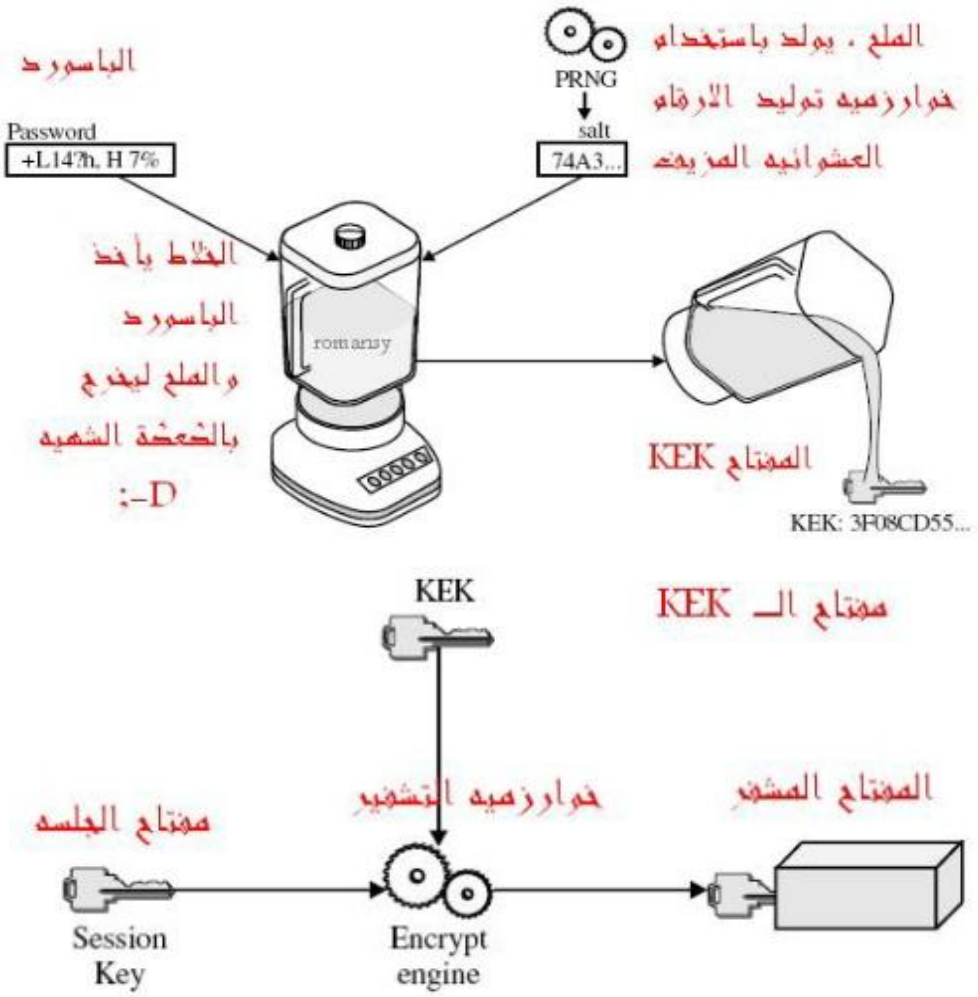
-1- ندخل الباسورد الذي أدخلناه في عمليه التشفير

-2- نأتي بالملح الذي احتفظنا به في مرحله التشفير

-3- ندخل الملح والباسورد في نفس الخلاط الذي استخدمناه في عمليه التشفير ، في حال اختلف احدهم سوف يكون الناتج عبارة عن KEK خاطئ ، وفي حال كانوا صحيحين فالناتج هو الـ KEKالصحيح

-4- نستخدم الـ KEK لفك مفتاح الجلسة ، وبعدها نستخدم مفتاح الجلسة لفك تشفير الرسالة..

وانتهت الخطوات ، والصورة التالية توضح العملية :




**دعنا نوضح بعضا من النقاط و الاسئله التي ربما ستتساءل عنها :**

Mixing Algorithms and KEK لماذا نخلط بين الباسورد والملح ؟ لماذا لا يكون الباسورد هو الـ KEK

الجواب ، لان الباسورد لا يحتوي على الكثير من Entropy ، لذلك هو غير كافي ابداً ، فهنا نستخدم هذه الخوارزمية للخلط بين الملح والباسورد وبذلك النتيجة أكثر عشوائية..