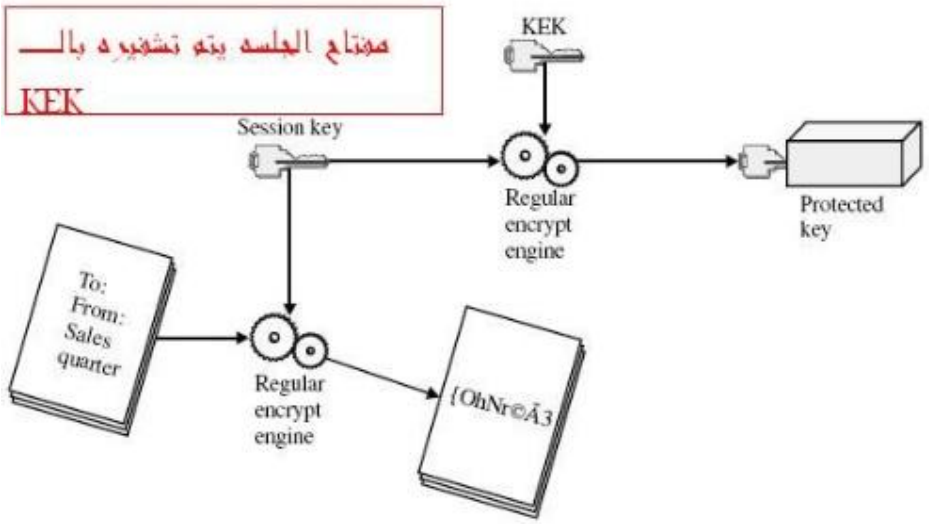
هذه العملية تسمى بالـ **password-based encryption** واختصارا **PBE** .

يعني مفتاح الجلسة session key هو المفتاح الذي نستخدمه في التشفير وفك التشفير
ومفتاح تشفير المفتاح key encryption key هو المفتاح الذي نستخدمه لتشفير مفتاح الجلسة ، واختصارا يسمى KEK .



الآن بما أن المفتاح KEK (من الآن وصاعدا نسميه بهذا الاسم) هو الذي يستخدم لتشفير وفك تشفير مفتاح الجلسة ، السؤال هل أنا بحاجه إلى حماية هذا الـ KEK ؟
الجواب ، هو لا ، عندما نريد أن نشفر المعلومات نقوم بتوليد هذا المفتاح (بأحد طرق توليد الأرقام العشوائية) بعدها نقوم باستخدامه ومن ثم نحذفه ، وفي حاله فك التشفير نقوم بتوليد هذا المفتاح مره أخرى ونستخدمه ومن ثم نحذفه ، وفي مرحله توليد هذا المفتاح يجب أن ندخل باسورد معين سواء في مرحله التشفير أو فك التشفير .

بصوره مبسطه ، **مفتاح الجلسة Session key** هو الذي يشفر المعلومات ونقوم بتوليده عشوائيا .
مفتاح الـ KEK هو الذي يشفر مفتاح الجلسة ونقوم بتوليده عن طريق password-based encryption.

<u>ويتم توليد الـ KEK :</u>
-1- إدخال باسورد
-2- استخدام أي طريقه لتوليد أرقام عشوائية لتوليد الـ salt (الملح) .
-3- ندخل الباسورد والملح مع بعض داخل الخلاط blender والناتج هو خليط من البتات العشوائية ، لقد تطرقنا سابقا عن الـblender وسوف نتحدث عنه بالتفصيل لاحقا .
-4- نأخذ ما يكفي من الخليط السابق ونضعه داخل المفتاح KEK ، وبعدها نستخدم الـ KEK لتشفير مفتاح الجلسة ثم نحذف هذا الـ KEK ، ونحتفظ بالملح .
-5- الآن تم تشفير الرسالة ، ويجب آن تحفظ الملح لأنه سوف يستخدم في فك التشفير .

ما هو هذا الملح ، بالتأكيد هو ليس الذي تستخدمه في الطعام ، وسوف نتطرق له بعد قليل .