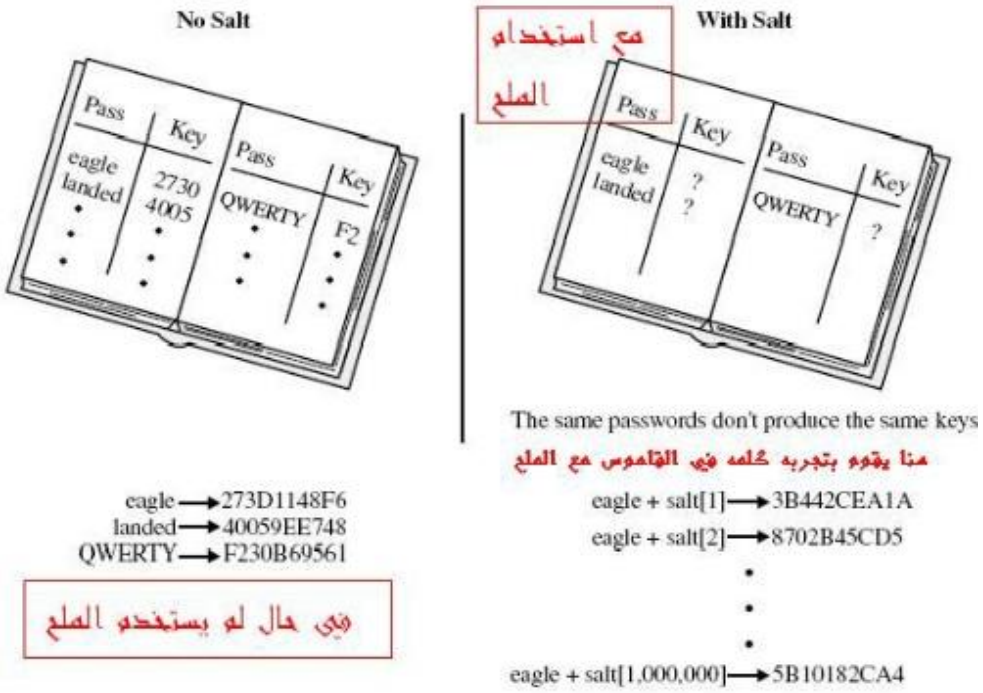
ما أهميه هذا الملح The Necessity of Salt ؟

هذا الملح ببساطه يستخدم لمنع محاولات تخمين الباسورد ، لأنه في حاله استخدمنا الباسورد فقط ك KEK فان المخترق بمكانه أن ينشئ قاموس به كل اغلب الباسوردات والمفاتيح وبعدها يبدأ في البحث عن الباسورد الخاص بك لكي يعرف الـ KEK (هذا الهجوم يعرف بـ dictionary attack) .

لكن اذا استخدمنا الملح ، فان المخترق لكي يعرف الـ KEK يجب في البداية أن يعرف هذا الملح للباسورد الفلاني هل هو صحيح أم لا ، اذا كان غير صحيح يقوم بتجربة ملح أخر في نفس الباسورد السابق ، اذا كان غير صحيح يقوم بتجربة ملح آخر في نفس الباسورد ، بعدها يغير الباسورد ويجرب الأملاح (☺) مره أخرى ، وهكذا يكون الأمر طويل جدا جدا جدا..



الآن وبعد تشفير مفتاح الجلسة باستخدام مفتاح KEK ، هل تعتبر في أمان كامل من جميع الهجمات ؟

بالطبع لا ، لان المخترق بإمكانه عمل هجوم على المفتاح KEK (هجوم القوه العنيفة Brute Force attack)ويقوم بتجربة مفتاح مفتاح إلى أن يصل إلى المطلوب .

أو بإمكانه عمل هجوم على الباسورد (Brute Force Attack) ، ويقوم بإدخال الباسورد والملح في الخلاط ، بعدها يأخذ الناتج KEK ويفك تشفير مفتاح الجلسة وبعدها يفك تشفير البيانات ، وإذا لم يصلح الباسورد يقوم بتغييره واختيار واحد أخر .

قد تبدو العملية طويلة ، لكن في الحقيقة أساليب هجوم Brute Force قد تأخذ أساليب متطورة ، مثلا عمل البرنامج **بالتوازي in parallel** وهنا سوف يستفيد من عمل المعالج بشكل كبير ، أيضا من الممكن أن يعمل أكثر من جهاز في عمليه الكسر .