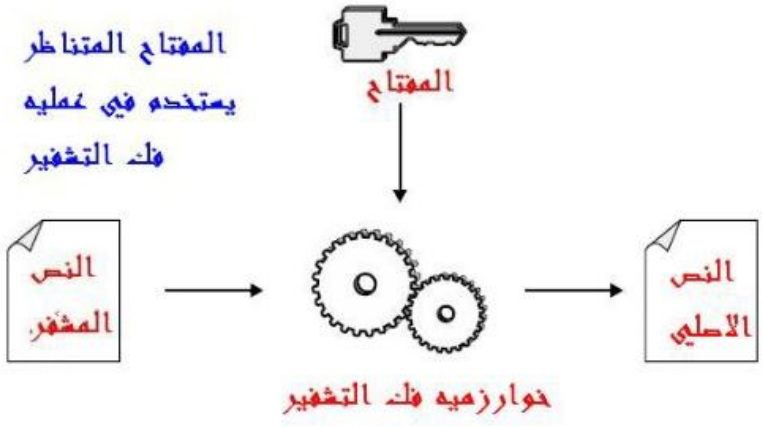

لاحظ انه في حاله شفرت الرسالة بخوارزمية معينه (مثلا DES) ومفتاح معين (مثلا 10) ، الآن في حاله فك التشفير يجب أن استخدم نفس الخوارزمية ونفس المفتاح والا فلن احصل على النص الأصلي.

نعود للسؤال ، ما هي أهميه المفتاح ؟؟؟

لقد رأينا في المثال السابق (محمد وعلي ، عندما لم يستخدموا مفتاح سري) انه في حاله حصول المخترق على البرنامج (أو معرفه الخوارزمية المستخدمة في التشفير) فانه بكل بساطه يستطيع إرجاع النص المشفر إلى النص الأصلي .

قد يسأل أحدكم سؤال "**حسنا ، لماذا لا اخترع خوارزمية وأبقيها سريه عن الجميع وبهذا لا يعرفها المخترق وبالتالي لا احتاج إلى مفتاح**" ؟؟

سؤال جيد ، ولكن له عده مشاكل ، أولا لان المخترقين دائما يكسروا ويخترقوا الخوارزمية (سنشاهد بعد قليل بعضا من الامثله الواقعية) ، ثانيا ، في حال انك لم تكن خبير في التشفير ولا تستطيع تطوير خوارزمية خاصة بك (مثل أخونا محمد) يجب في تلك الحالة أن تثق بالشركة المنتجة للبرنامج (الخوارزمية) الذي تستخدمه (في هذه الحالة يجب أن تثق ب Romansy) ؟ هل يستطيع أحدكم أن يمنح شركه ما كل هذه الثقة ، بالطبع لا .
وهنا يأتي السؤال الحقيقي ، من تثق بحفظ أسرارك ، **خوارزميه يجب أن تكون سريه من الجميع**، أم **الخوارزمية التي تؤدي عملها بشكل جيد وحتى لو عرفها الجميع** ، وهنا يأتي دور المفتاح في حال اخترت الخيار الثاني .

المفتاح يجعلك تشعر بالارتياح التام ، لأنك اذا شفرت الخوارزمية باستخدام المفتاح ، سوف تكون مهمتك الحفاظ على المفتاح فقط ، بالتأكيد هو أسهل بكثير من الحفاظ على الخوارزمية التي اخترعتها.

أيضا في حال استخدمت مفتاح تشفير لكل رسالة ، في حال تم كسر احد المفاتيح ، فان باقي الرسائل تكون سريه وغير مكشوفة ، على العكس اذا استخدمت خوارزمية من تطويرك وتم كشفها فان كل الرسائل سوف تنكشف أيضا.