تكلفتها العالية ، وأيضا بسبب أنها غير موثوقه بشكل أكيد ، يعني مثلا اذا أصيب الإصبع بجرح هل يستطيع الجهاز التعرف عليه ، في حال استخدام نبره الصوت وأصيب الشخص بنوبة برد أو التهاب في الحلق ، هل يستطيع الجهاز التعرف على الصوت!

بالتأكيد مع تطور العلوم وخاصة الذكاء الاصطناعي فانه قد يأتي يوما يتم زرع جهاز كمبيوتر شخصي داخل دماغ أي إنسان ويكون التعرف عن طريق قرائه هذا الجهاز (قد قرأت من فتره عن أمر مشابه من شركه مايكروسوفت) .

The Key Distribution Problem and Public-Key Cryptography

تعرفنا قبل قليل على بعضا من أساليب حماية المفتاح (مفتاح الجلسة) ، ويكون إما عن طريق تشفيره مره أخرى (PBE) ، أو عن طريق تخزين المفتاح في احد الأجهزة الخاصة لذلك Token، إلى هنا الأمر تحت السيطرة ، لكن ماذا اذا أردنا أن نرسل المفتاح إلى شخص آخر حتى يقوم بفك تشفير الرسالة التي سوف أرسلها له (تذكر أن التشفير بالمفتاح المتناظر ، المفتاح نفسه يقوم بالتشفير وفك التشفير).

بعبارة مبسطه ، في حال قمت بتشفير رسالة ما بهذا المفتاح المتناظر ، بعدها أرسلت الرسالة إلى الشخص الذي أريد ، في حال وصلت الرسالة للشخص هذا سوف تكون غير مفهومه وذلك لان المفتاح الذي يفك التشفير معي والى الآن لم أرسله للشخص المراد ، أيضا في حال كان هناك مخترق ووصلت الرسالة إليه بطريقه ما (سواء قام باختراق جهاز الشخص الذي أرسلت له الرسالة ، أو قام بالتقاط الرسالة أثناء إرسالها) المهم سوف تكون الرسالة أيضا غير مفهومه لأنه لا يملك المفتاح.

اذا السؤال هنا ، كيف يمكن أن أرسل المفتاح بطريقه آمنه إلى الشخص الذي أريد ، وفي نفس الوقت لا يستطيع المخترق الحصول عليه ؟؟
هذه المشكلة تسمى بمشكله **إرسال المفتاح Key Distribution Problem** ، والتي بسببها تم اختراع الطريقه الأخرى في التشفير وهي التشفير بالمفتاح غير المتناظر Asymmetric key Cryptography .

قبل الخوض في التشفير بالمفتاح غير المتناظر وجدت بعضا من الحلول التي قد تكون مناسبة لحالتك (أي قد تستطيع الاكتفاء بها) ، هذه الحلول هي :
-إرسال المفتاح قبل عمليه الإرسال
-استخدام طرف ثالث موثوق Trusted Third Party ، اختصارا TTP

نبدأ بالحل الأول : إرسال المفتاح قبل عمليه الإرسال :
وهنا في هذه الحالة يجب أن أقوم بإرسال المفتاح إلى الشخص المراد قبل أن ابدأ في إرسال الرسالة ، ولكن بالطبع يجب أن أتأكد أن الاتصال امن حتى أرسل المفتاح وأنا مطمئن انه لا يوجد احد غير الشخص المراد إرسال المفتاح إليه .
حسنا أأمن طريقه لإرسال المفتاح ، هي القيام بإعطاء المفتاح للشخص وجها بوجه ، أي أن اذهب إلى مكتبه أو بيته ، بعدها أقوم بتوليد المفتاح واحفظ نسخه في جهازي ، ونسخه في جهاز