السؤال السابق نطرحه مره أخرى ،" **في حال شفرت الرسالة بخوارزمية لا يعرفها احد ، وإذا استخدمت مفتاح فلن ابلغ احد بطول المفتاح** " هل تكون الرسالة أمنه ؟

و هناك ثلاثة أجوبه :

الجواب الأول : هم دائما يعرفون الخوارزمية:

المخترقين سوف يعرفوا الخوارزمية مهما فعلت ، ولا أي واحد في تاريخ التشفير تمكن من إبقاء خوارزميته سريه ، لطالما تمكن الجواسيس في الحرب كشف الخوارزميات سواء باستخدام عمليات رياضيه أو أجهزه لكسر الشفرات ، أو حتى يوظفوا جواسيس لدى العدو ، أو يسرقوا الخوارزمية ، أو يسرقوا الجهاز المستخدم للتشفير .

في الحرب العالمية الثانية ، تمكن الجنود البولنديين من سرقه الجهاز الألماني الذي كان الألمان يستخدموه للتشفير (اسمه **Engima**) وتم بيعه للبريطانيين (الحلفاء) وبعدها تمكن هؤلاء الحلفاء من كسر اغلب الرسائل الالمانيه !!

وبدون أي سرقه ، فان الـ cryptanalysts يستطيعوا ببساطه كسر الشفرات ، ففي الحرب العالمية الثانية تمكن كاسري الشفرات الأمريكيين (اسمهم **Code breaker**) من معرفه طريقه عمل الجهاز المستخدم في التشفير لدى اليابانيين(بدون الحاجة إلى سرقه الجهاز) .

مثال آخر ، هناك خوارزمية اسمها RC4 اخترعت من قبل شركه RSA في عام 1987 لكن لم تنشر ، كل الـ cryptanalysts والمشفرين اجمعوا في ذلك الوقت أن هذه الخوارزمية آمنه جدا وتجعل البيانات سريه للغاية ، ولم تنشر تلك الخوارزمية لأغراض بيع برامج للتشفير (وليس لأغراض عسكريه) ، المهم في 1994 قام احد الهكرز بوضع الخوارزمية مشروحة بالتفصيل في الانترنت ! كيف عرف هذا الهكرز الخوارزمية ؟؟ بالتأكيد من خلال برامج Disassembly And Debugger، وهي برامج تستخدم لفتح الملفات التنفيذية وتتبعها سطر بسطر وتغيير الأكواد والكثير من الأمور التي يعرفها الكراكرز . حاليا خوارزمية RC4 تستخدم كجزء من بروتوكول الـ SSL وهي من احد الخوارزميات التي تستخدم المفتاح المتناظر للتشفير.

بعض الأحيان ممكن أن تبقى الخوارزمية سريه لبعض الوقت ولكنها تنكشف في النهاية ، مثلا في الحرب العالمية الثانية استخدم الأمريكان لغة Navajo وطبعا اليابانيين لم يكونوا على علم بهذه اللغة ، لذلك الرسائل الامريكيه كانت مشفره . لكن حاليا اغلب الجيوش تحتوي على فريق كامل من العلماء باستطاعتهم تعلم أي لغة مهما كانت وبأسرع وقت .

الجواب الثاني : لا تستطيع جني المال من الخوارزمية السرية:

لأنك في حال عملت برنامج وقمت ببيعه فبالتأكيد سوف يقوم احد الهاكر باستخدام طرق الهندسة العكسية والوصول إلى خوارزميتك (كما حصل في RC4) . لذلك الخوارزمية التي طورتها سوف تستخدمها لنفسك أنت وحبيبتك فقط ☺ .

الجواب الثالث : الخوارزميات المعروفة هى أكثر آمانا:

لأنها تكون مثبته أنها آمنه من قبل جميع الـ cryptanalysts والمشفرين ، من الممكن أن هؤلاء