cryptanalysts قد اقروا بعدم وجود ثغرات بخوارزمية معينه ، بعدها بفترة قمت أنت بكشف ثغره فيها ، نعم ممكن ولكن احتمال ضعيف جدا جدا .

في حال اقر الجميع بان الخوارزمية آمنه ولا توجد ثغرات بها ، فان فرصه إيجاد ثغره ضئيلة للغاية .

توليد المفتاح *Key Generation* :

في التشفير المتناظر ، المفتاح عبارة عن رقم وطوله على حسب نوع الخوارزمية (64 بت مثلا)، ويمكن توليده بصوره عشوائية ، السؤال هنا كيف يتم توليد الأرقام العشوائية ؟

حسنا ، الأرقام العشوائية هي بكل بساطه أرقام مثل (3،1،5،100) يتم اختيارها بشكل عشوائي، اغلب المبرمجين يعرفون قيمه هذه الأعداد فهي تستخدم بكثرة في عده نواحي مثل الألعاب Game، نمذجه ومحاكاة الحاسب Simulation And Modeling والتشفير Cryptography وغيرها من المجالات .

في التشفير ، أهم ما يجب أن يتوفر في هذه الأعداد هو أن لا تتكرر أبدا ، أيضا أن تتجاوز الاختبارات الاحصائيه ، الاختبارات الاحصائيه هي مجموعه اختبارات يتم تطبيقها على الأعداد (أو العدد) لكي تعرف هل هي عشوائية أم لا..

لنفترض لدينا مجموعه من الأعداد (ألف عدد مثلا) ، وقمنا بسؤال احد الذين يقومون بهذه الاختبارات "هل هذه الأعداد عشوائية أم لا "، كل ما يقومه هذا الشخص (الإحصائي) بالقيام بتحويل الأعداد أولا إلى الترميز الثنائي Binary Format أي يقوم بتحويل الأعداد إلى 0 و1 ، بعدها يقوم بإجراء عده اختبارات على هذه الأعداد ، الاختبارات تكون عبارة عن عده اسئله:
هل العدد 1 يظهر بنفس تكرار 0 ؟ أم أكثر أم اقل ؟
هل العددين 1و 0 يظهران بشكل محدد كل مره ؟ (مثلا تأتي 1 أولا بعدها 0) ؟
وغيرها من الاسئله....

المهم ، بعدها في حال نجح الاختبار ، تكون الأعداد العشوائية التي أعطيتها للإحصائي محتمله أن تكون عشوائية !! لا نستطيع أن نقول هي عشوائية بصوره مؤكده 100% ، لماذا ، سنعرف لاحقا .