مولدات الأرقام العشوائية *A Random Number Generator* اختصارا *RNG* :

عرفنا أن الأعداد العشوائية هي أعداد تكون بصوره عشوائية وغير مرتبه ، حسنا السؤال الذي يطرح نفسه : من أين يمكن الحصول على هذه الأعداد العشوائية ؟؟

هناك مصدرين:
الأول هو لتوليد أعداد عشوائية حقيقية أو كاملة RNG أو True RNG ، وهنا في هذه الحالة سوف نستخدم أجهزه خاصة لتوليد الأعداد (تأخذ مدخل يتغير باستمرار) مثل قياس الظروف الجوية ، حساب سريان التيار الكهربائي وغيرها وهذه الأعداد بالطبع سوف تجتاز الاختبار الإحصائي..

وإذا طلبنا من هذه الاجهزه أعداد عشوائية أخرى ، فلن نحصل على نفس الناتج أبدا ، ولذلك لان المخرج (الأعداد) تعتمد على مدخل غير ثابت (يتغير باستمرار) ، لذلك فإن الأعداد العشوائية الناتجه من هذه الأجهزة لا تتكرر ابدآ ، ولهذه تسمى بالأعداد العشوائية الصحيحة أو الكاملة True Random Number .

قرأت عن أن شركه Intel تقوم باستخدام RNG يوضع داخل النظام ويقوم بحساب الحرارة أو شيء مشابه ، وهو مصدر يتغير باستمرار ، أيضا هذا الجهاز لا يأتي مع أي معالج بنتيوم (إلا مع الطلب) ، لكن يحتمل ذلك في السنوات المقبلة .

شركات أخرى مثل nCipher, Chrysalis : تبيع أجهزه تسمى cryptographic accelerators هذه الاجهزه تأتي بـ RNG ، (سوف نلقي نظره بسيطة على cryptographic accelerators بعد قليل) .

المصدر الآخر لتوليد الأرقام العشوائية هو Pseudo-Random Number Generator (الأعداد العشوائية المزيفة) :

من أين يمكننا الحصول على أعداد عشوائية اذا كنا لا نملك هذه الاجهزه ، الجواب باستخدام مولد الأعداد المزيفة ، وهو عبارة عن خوارزمية لتوليد هذه الأعداد "المزيفة" ، بالتأكيد كلمه "مزيفه" يسبب لك بعضا من الحيرة ، لكنه سيتضح بعد قليل .

هنا في حاله الأعداد العشوائية المزيفة اذا استخدمنا الخوارزمية وولدنا الأعداد (مثلا ألف عدد) ، بعدها ذهبنا إلى صديقنا الإحصائي وقمنا باختبار هذه الأعداد ، الناتج هو أن هذه الأعداد سوف تنجح أيضا في الاختبار (مثلها مثل T-RNG) ، لكنها يحتمل أن تكون عشوائية .

الذي يجعل هذه الإعداد مزيفه هو أنها تتكرر (وألف خط تحتها) اذا شغلت مولد الأعداد المزيفة في جهازين مختلفين سوف يطلع بنفس الناتج ، اذا شغلت البرنامج بعد سنه سوف يطلع بنفس الناتج .

لذلك قبل قليل قلنا أن النتيجة التي يخرج بها الإحصائي هي محتمله أن تكون عشوائية وليس عشوائية 100% .
اذا الإحصائي يعطينا أجابه على أن الأعداد عشوائية فقط ، ولكن هو لا يعرف هل هي تتكرر أم لا ، يعطينا فقط نصف الاجابه.