نظره حول Netscape's Seed :

أن التشفير بالمفتاح المتناظر هو احد مكونات SSL الذي اخترع من قبل العلماء في شركه نت سكيب (احد العلماء بل رئيس العلماء في فتره التسعينات هو العالم العربي المصري **طاهر الجمل** ، والذي اخترع الخوارزمية التي تعرف بـ ELGAMAL نسبه إلى اسمه ، سأتكلم عنه في النسخة النهائية) ، وفي وقت توليد الاتصال في SSL يجب أن يولد رقم عشوائي ، وقد استخدمت الشركة PRNG يجمع المعلومات (الوقت + رقم العملية process ID) واستخدم كبذره Seed للمولد PRNG .

بالنسبة إلى process ID فيمكن الحصول عليه من خلال الدخول إلى نفس الجهاز الذي ولده ، أو يمكن تطبيق هجوم brute-force attack حيث طوله فقط 15 بت ، أما بالنسبة إلى الوقت ، استخدمت الشركة الثواني (وليس جزء من الألف من الثواني) ولذلك هناك 60 ثانيه فقط .

على العموم في 1995 قام Goldberg و Wagner بإيجاد ال Seed وبالتالي إيجاد المفتاح في اقل من دقيقه ، سواء كان المفتاح 40 بت أو 128 بت ، سوف يأخذ اقل من دقيقه !!

وقد قامت نت سكيب بعدها باضافه Seed جديد يعتمد على عده عوامل:
. mouse position, memory status, last key pressed, audio volume, and many others
و هكذا يصعب إيجاد ال Seed .

كسر الخوارزمية Breaking the Algorithm :

الطريقه الأخرى للهجوم على البيانات المشفرة هي كسر الخوارزمية ، وهنا يعتمد على قوه ملاحظه وذكاء المخترق ، مثلا لاحظ أن رقم معين يظهر في مكان معين ، هنا يستطيع تخمين هذا العدد بعد تجربه العديد من المحاولات حتى يحصل على النص الأصلي .

مثل تلك الخوارزميات الضعيفة يمكن أن تخترق وحتى لو كان حجم المفتاح كبير .