الخلاصة

تحتوي بعض خوارزميات التشفير الانسيابي على مجموعة من مسجلات الازاحة ذوات التغذية الخلفية الخطية (LFSR) التي تولد كل منها متتابعة ذات دورة عظمى وذات خواص احصائية جيدة، وتحتوي ايضا على دالة توافقية لا خطية مدخلاتها هي المتتابعات المتولدة من مسجلات الازاحة ومخرجاتها تمثل المفاتيح الانسيابية ، للحصول على درجة تعقيد عالية .

ان اية علاقة احصائية بين المدخلات والمخرجات لهذه الدالة اللاخطية وباحتمالية ترابط ($p \neq 0.5$) يعرض هذا النظام للتحليل بوساطة الارتباط (Correlation Attack) الذي يعتمد مبداء فرق تسد (Divide And Conqer Attack) والذي يمتاز بكونه يتعامل مع كل مسجل ازاحة بصورة مستقلة عن باقي المسجلات وبالتالي يقلل بشكل كبير عدد الاحتمالات لمعرفة المفتاح (الحالة الابتدائية ودالة التغذية الخلفية).

تم بناء مجموعة برامج لتطبيق هذا النوع من التحليل الذي استخدم في تحليل نظام (Pless) كنموذج لنظام تشفير انسيابي تتوفر فيه خاصية الارتباط بين المدخلات والمخرجات .

لقد تم تنفيذ جميع البرامج المتعلقة بهذا النوع من التحليل للحصول على المفتاح من خلال النص المشفر فقط . كما نفذت في البحث طريقة جديدة في حساب الاستهلال (Threshold) لتقليل عدد الاحتمالات .

تم تنفيذ البحث على الحاسبة (IBM/PS2) وبلغة برمجة باسكال (Turbo Pascal Version 5.5) كما اعتمد معجم الرياضيات (المجمع العلمي العراقي) ومعجم الحاسبات (المعجم العربي الموحد) في تعريب المصطلحات ذات العلاقة.

PDF created with pdfFactory trial version www.pdffactory.com