الخلاصة

تقنيات التشفير لها دور أساسي في أمنية الشبكات و إن خوارزميات التشفير التسلسلي هي واحدة من هذه التقنيات المهمة في صيانة الأمنية و حماية المعلومات من إي جهة التي تحاول إساءة استعمال هذه المعلومات .

في هذا البحث تم تقديم مفاهيم حديثة إلى التشفير التسلسلي وهي : جعل حجم المحتويات في LFSR يساوي إلى 32 bits بدلا من 1 bit وجعل خوارزمية التشفير الكتلي يولد قيم ابتدائية لتهيئة محتويات إل LFSR و كذلك جعل تعقيد الخطي ل LFSR يزداد بواسطة استخدام Sbox الذي يعتمد على المفتاح و هو مشتق من خوارزمية التشفير الكتلي و مع استخدام FSM .

كذلك في هذا البحث تم تقديم اقتراحين الاول يسمى Snowfish 1 و الثاني يسمى Snowfish 2 لتحسين خوارزمية تشفير التسلسلي Sosemanuk من خلال الاستفادة من محاسن التشفير الكتلي Twofish و الذي يمتلك جدولة المفاتيح و Sbox جيدين في زيادة الأمنية و العشوائية و محاولة التغلب على هجوم guess and determine الموجود على Sosemanuk .

إن هذين الاقتراحين يستخدمون خوارزمية Twofish بدلا من خوارزمية التشفير الكتلي Serpent الذي هو المستخدم في Sosemanuk . و كذلك يستخدمون Sbox الذي يعتمد على المفتاح بدلا من Sbox الذي يعتمد على قيم الثابتة أو جدول ثابت. هم متشابهين في استخدام نفس الطول للمفتاح (128 bits إلى 256) و ل IV (128 bits) و LFSR و FSM و output transformation .

و لقد نفذ المشروع بلغة فيجوال بيسك 0.6 لما توفيره من إمكانيات و تسهيلات برمجيه يتناسب مع متطلبات البحث و طبقت البرمجيات على حاسبة شخصية من نوع P4 و 2.00 HZ RAM و 504 MB و معالج من نوع Intel لتطبيق هذين النظامين المقترحين كذلك مع تطبيق نظام إل Sosemanuk لعمل مقارنة بينهم باستخدام اختبارات العشوائية و الهيكلية و تعقيد الخوارزمية فنتائج الاختبارات تبين إن النظامين المقترحين لهما نتائج جيدة في تحقيق الأمنية و العشوائية مقارنة مع نظام إل Sosemanuk .

PDF created with pdfFactory trial version www.pdffactory.com

Abstract

Cryptographic techniques play an important role in network security and stream ciphers are one of the main cryptographic techniques that play a very important part in maintaining security and protecting valuable information from potential misuse.

This thesis will introduce updated concepts to stream cipher which are: let the size of states in LFSR equal to 32 bits rather than 1 bit, let the block cipher algorithm generate initial values of states in LFSR, let the linear complexity of LFSR increased by using key-dependent Sboxes which are derived from block cipher algorithm with using FSM. Also this thesis will introduce two proposal algorithms (Snowfish 1) and the (Snowfish 2) to improve the Sosemanuk stream cipher algorithm by benefiting from the efficient properties of the Twofish block cipher and also use its key schedule, key-dependent Sbox to increase the security, randomness and try to avoid the guess and determine attack of Sosemanuk. These two proposals use Twofish algorithm rather than Serpent algorithm which was used in the Sosemanuk and also they use key-dependent Sbox rather than static Sbox. They are similar in the same key length (128 to 256 bit), IV length (128 bit), LFSR, FSM and output transformation.

This thesis is implemented using Visual Basic 6.0 language on PC computer type P4 with RAM 504 MB and 2.00 GHz with Intel processor to perform these two proposed systems and also to perform the Sosemanuk system to make a comparison between them by using the tests of randomness, the structural tests and the complexity of the algorithm. These tests give results that shows the two proposed systems have good results in increasing the security and randomness compared

PDF created with pdfFactory trial version www.pdffactory.com