جامعة الموصل
كلية علوم الحاسوب والرياضيات

تحسين خوارزمية التشفير الكتلية الخفيفة لتأمين جواز السفر الألكتروني

رسالة تقدمت بها

ورقاء سالم نجم عبدالله البكر

بإشراف

د. سفيان سالم محمود الدباغ

مدرس

رسالة دبلوم عالي

علوم الحاسوب

١٤٤١هـ ٢٠١٩ م

الخلاصة

يعد أمن المعلومات مسألة هامة جداً في نقل المعلومات وإن أي خسارة أو تهديد في نقلها سيكون بالتالي خسارة كبيرة في عملية إرسال المعلومات وبما أنه لدينا معلومات مهمة (معلومات جواز السفر) فسوف تقوم تقنية التشفير الدور الرئيس في أنظمة أمن المعلومات.

في بحثنا هذا قدمنا طريقة مقترحة لتحسين خوارزمية التشفير الكتلية خفيفة الوزن (Highest (HISEC Security Lightweight Block Cipher Algorithm لتشفير بيانات جواز السفر الألكتروني؛ لكوننا نحتاج إلى أمنية عالية للحفاظ على هذه المعلومات كونها معلومات شخصية. ان خوارزميات التشفير الكتلية خفيفة الوزن لاقت قبولا؛ لكونها لها القابلية على العمل في بيئة مقيدة مثل(جواز السفر الألكتروني والبطاقة الذكية وغيرها).

تم في هذا البحث تقديم خوارزمية مقترحة لتعزيز وتحسين خوارزمية HISEC من خلال إدخال مفهوم key dependent S-box إذا خططنا في هذا المقترح توليد كتلة شفرات أكثر أماناً وتحل مشكلة البنية الثابتة لـ S-box المستخدم , وتم أيضاً التقصي عن العوامل الثلاثة الأساسية لكل خوارزمية بصورة عامة ألا وهي عامل الكلفة ,السرعة والأمان وفي النهاية سيتم عمل مقارنات بين استخدام خوارزمية HISEC قبل التحسين والمحسنة والخروج باستنتاجات تفيد مجتمع الباحثين والمصممين في الحصول على الأمان بالدرجة الأولى و السرعة ثانياً والكلفة ثالثاً في خوارزميات التشفير الكتلية خفيفة الوزن . ويمكن تلخيص أهم ما توصلنا إليه من نتائج :من ناحية عامل الكلفة فان خوارزمية HISEC المحسنة تتطلب GE (1704.76) بينما خوارزمية HISEC قبل التحسين تتطلب (GE (1694.08 ,ومن ناحية عامل السرعة فان خوارزمية HISEC المحسنة تستغرق (٣,٠٩٢٥) Mili seconds وقتاً أكثر مقارنة بخوارزمية HISEC قبل التحسين التي تستغرق (٢,٩٤٢٤) Mili seconds عند تشفير البيانات نفسها والمفتاح نفسه, ومن ناحية عامل الأمان فان خوارزمية HISEC المحسنة قد حققت عشوائية أكثر من خوارزمية HISEC قبل التحسين ؛ وذلك لكونها تعتمد على مفهوم الاعتماد

على المفتاح في إختيار الـ S-box والذي بدوره لا يتأثر بهجمات تحليل الشفرات الخطية (linear cryptanalysis) و كذلك تحليل الشفرات التفاضلية (Differential Cryptanalysis) إذ حققت العشوائية في Avlanche Test منذ الدورة الأولى فقد بلغت قيمة الفحص(٠,٥٣١٢٥) بينما خوارزمية HISEC قبل التحسين حققت العشوائية في الدورة الثالثة إذ بلغت قيمة الفحص (٠,٠٦٢٥).

University of Mosul

College of Computer Sciences and Mathematics

ENHANSMENT OF LIGHTWEIGHT BLOCK CIPHER ALGORITHM FOR SECURING E-PASSPORT

A these is Submitted By

Warkaa Salim Najm Al-Bakr

Supervised By

Dr. SUFYAN SALIM MAHMOOD AL-DABBAGH

Lecturer

Higher Diploma / these is

Computer Science

2019

Abstract

Information security is a very important issue in the transmission of Information and any loss or threat in the transfer of information will be a great loss in the process of sending information since we have important data (passport Information) will be encryption technology plays a major role in information security systems.

In this paper we present a suggested method to improve Highest Security Lightweight Block Cipher Algorithm (HISEC) to encrypt electronic passport data because we need high security to maintain this information as personal information. Lightweight Block Cipher Algorithm have been accepted to operate in a restricted environment (e-passport, smart card, etc.).

In this paper, we propose to introduce a proposed algorithm to enhance and improve the HISEC algorithm by introducing the concept of key dependent S-box. In this proposal, we plan to generate a more secure code block and solve the problem of the fixed structure of the used S-box. The algorithm is generally the cost factor, speed and security and ultimately the examples will be compared through the use of the HISEC algorithm before and after improvement and come to conclusions that benefit the research community and designers in obtaining safety in the first place and cost second and speed third in lightweight block cipher algorithms.. The main findings can be summarized as follows: In terms of cost factor, the improved HISEC algorithm requires (1704.76) GE, while the HISEC algorithm before optimization requires (1694.08) GE, and on the one hand the speed factor, the improved HISEC algorithm takes (3,0925) Mili seconds More compared to the HISEC pre-optimization algorithm that takes (2,9424) Mili seconds when encrypting the same data and the same key, in terms of safety factor, the improved HISEC algorithm has achieved more randomness than the HISEC algorithm prior to optimization because it depends on the concept of key

dependence in the selection S-box , which in turn is not affected by linear cryptanalysis attacks Analysis of Differential cipher (Differential Cryptanalysis) where random achieved in Avalanche Test since the first session, reaching examination value (0.53125), while HISEC algorithm optimization achieved by random at the third session where the total value of the examination (0.0625).