الجمهورية العربية السورية

جامعة البعث

كلية الهندسة المعلوماتية

قسم هندسة النظم والشبكات الحاسوبية

تحسين بروتوكول أمن الشبكات اللاسلكية WEP

دراسة أعدت لنيل درجة الماجستير في هندسة النظم والشبكات الحاسوبية

إعداد:

المهندس نوار فيصل محمد

إشراف:

الدكتور المهندس أكرم المرعي

أستاذ مساعد في قسم هندسة النظم والشبكات الحاسوبية – جامعة البعث

٢٠١٧م

الملخص

هناك نقص في التركيز على سرية شانون للشيفرات كمقياس للأمن في تشفير المفتاح المتناظر، استخدم في هذا البحث نظريات شانون في سرية الشيفرات لحساب متوسط السرية لبعض الشيفرات المتناظرة والتي ستستخدم في هذا البحث. تم القيام بتحليل السرية والأداء من خلال استخدام خوارزمية جديدة. تم التحليل بالاعتماد على مستوى السرية وأداء الخوارزمية. يقدم هذا البحث تحليل لبعض خوارزميات المفتاح المتناظر المستخدمة بشكل شائع والتي تصنف تحت قسمين: الشيفرات الدفقية والشفرات الكتلية مع الخوارزمية المدمجة [RC4 , AES , Hybrid (RC4_AES)]. تم تحقيق كل الخوارزميات بلغة الجافا باستخدام صفوف متوفرة في حزم الجافا Javax.crypto. لحساب سرية الشيفرات و زمن التشفير فإن عدة صفوف منفصلة كتبت باستخدام لغة البرمجة جافا (JAVA) من خلال بيئة برمجية خاصة بلغة البرمجة جافا وهي NEtBeans IDE. وبالتالي فإن محصلة نتيجة البحث الذي تم التركيز عليه هي أن أداء كل الشيفرات الدفقية أعلى من أداء الشيفرات الكتلية ، ومستويات السرية للشيفرات الكتلية أعلى نسبياً من الشيفرات الدفقية، وهو مثبت أكثر في نظريات شانون.

الكلمات المفتاحية:

الشيفرة الكتلية ، الشيفرة الدفقية ، زمن التشفير ، سرية الشيفرة.

Abstract

There is a lack of focus on Shannon's secrecy of ciphers as a security measurement of symmetric key encryption, hence in this research, Shannon's theories on secrecy of ciphers were used to calculate the average secrecy of some symmetric cipher used in this research. All secrecy and performance analysis were done using a newly created algorithm. Analysis is done based on the secrecy level and performance of the algorithm. This paper presents an analysis of some of the widely used symmetric key algorithms which fall under the categories of block and stream ciphers together with one combined algorithm. [AES, RC4, Hybrid (AES+RC4) are used. All the algorithms are implemented in Core Java using classes available in JAVA package javax.crypto. Separate classes are written to calculate the secrecy of ciphers and the encryption time. And also the code is writing using Core Java with the help of Netbeans IDE. As far as the outcome of the research is concerned, the performances of all stream ciphers are higher than that of block ciphers and the combined algorithms have similar performance level to block ciphers. Secrecy levels of block ciphers are comparatively higher than that of stream ciphers as the history says, it is further proved by Shannon's theories in this research. The combined algorithms have more stable secrecy levels.

Keywords :

Block Cipher , Stream Cipher, Encryption time , Secrecy of Cipher .