تحسين مستوى أمان الاتصال الضوئي للبيانات باستخدام التشفير

إعداد

وسن سامي هيجل الدليمي

المشرف

د. عدنان حنيف

جامعة الزيتونة الأردنية، 2020

الملخص

تعتمد خوارزميات التشفير المتماثل على استخدام نفس المفتاح في التشفير وفك التشفير. من مميزات التشفير المتماثل أنه سهل الاستخدام وسريع. الخوارزمية المعتمدة في هذه الأطروحة هي معيار التشفير المتقدم (AES). تعتبر هذه الطريقة رسمية وآمنة للتشفير بسبب طول مفتاح التشفير DES.

بسبب احتمال حدوث أي اختراق في الخوارزمية، وإثبات أن أحد الباحثين يدرس وجود تأخير بسبب خطوة معينة في الخوارزمية ويجب التخلي عنه لتجاوز التأخير.

تم اقتراح هذه الرسالة لتحسين أمان الخوارزمية ولإجراء تعديل على القوانين السابقة، كما اعتمدنا على الرقم 1 في إحدى مراحل الترميز في الخوارزمية، بالإضافة إلى المقترح في وظيفة المفتاح. أظهرت عوامل الدراسة التي تأثرت إيجابياً بتحسين النتائج ومقارنتها من خلال تجارب تحسناً في المعدل معايير Hamming 65٪، Avalanche 0.44٪ و Balance 60٪.

أخيرًا، تم اقتراح إرسال هذه البيانات المشفرة بواسطة تقنية اتصال خفيفة تسمى light Fidelity (LIFI). تعتبر هذه التقنية آمنة للغاية وسريعة أكثر بكثير من الإنترنت المستخدم في حياتنا اليومية. لذا، ستقترح هذه الرسالة تشفير البيانات وأمنًا كبيرًا من حيث تحسين الخوارزمية ووجود تقنية الاتصال الضوئي.