وزارة التعليم العالي والبحث العلمي
جامعة الموصل
كلية علوم الحاسوب والرياضيات
قسم علوم الحاسوب

تنفيذ خوارزمية تشفير كتلي مقترحة للنص

رسالة مقدمة

الى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل

كجزء من متطلبات نيل شهادة ماجستير علوم في

علوم الحاسوب

من قبل

آمنة خالد خليل الرجبو

بإشراف

أ.م.د. ياسين حكمت أسماعيل الحمو

14445 2023م

الخلاصة

بعد أن اتسع استخدام الانترنت وتداول الملفات بين المستخدمين أصبح أمن المعلومات من الاولويات المهمة التي يجب تحقيقها بوسائل أنظمة مختلفة، ويأتي تشفير المعلومات في مقدمة التقنيات المستخدمة في أمن المعلومات، فالتشفير معروف منذ قديم الزمان، وتطور على مر العصور؛ فظهرت أنظمة التشفير التقليدية التي ما لبثت وأن تطورت تطوراً كبيراً، ولا تزال أساليب التشفير التقليدية تستخدم في الكثير من الدراسات العلمية والبحوث التطويرية بهدف استحداث أنظمة جديدة لتشفير الابدال والتعويض وزيادة قدرته على مواجهة الهجمات المختلفة.

تعرضت أساليب التشفير التقليدية إلى هجمات عدة، دفعت الباحثين إلى تطويرها وتجاوز نقاط ضعفها أمام تلك الهجمات، واستعمل بعض الباحثون تراكيب من تلك الأساليب في تصميم أنظمة جديدة للتشفير بناءً على أفكار متداخلة للتشفير التقليدي، كانت لبعضها قدرة أكبر على مواجهة الهجمات، وواصل الباحثون تطوير تلك الأساليب واستعمالها إلى جانب أنظمة التشفير الحديثة لزيادة قوة التشفير.

تتطرق هذه الرسالة إلى استعمال مجموعة من أساليب التشفير التقليدية في تصميم نظام جديد للتشفير الكتلي تمتزج فيه تلك الأساليب بأفكار حديثة، تساعد على زيادة قوة التشفير وقدرته على مواجهة بعض الهجمات مثل تحليل التكرار Frequency Analysis، لتقديم نظام تشفير كتلي يضم في تصميمه عدداً من الأنظمة التقليدية في التشفير، مثل (Ceaser، Vigener، Rail Fence)، والتشفير الابدالي والتعويضي، مع بعض المفاهيم الأساسية في أنظمة التشفير الكتلي. اعتمد النظام المقترح على الدالة الفوضوية Tent map لخواصها العشوائية في توليد سلسلة مفتاح عشوائي، وأستخدم أسلوب جديد في التعامل مع أحرف النص الواضح بصيغتها القياسية (A–Z) دون تحويلها الى الصيغة الثنائية لتقليل التعقيد البرمجي، وأستخدمت هذه الصيغة في بناء صناديق التعويض والأبدال.

قدمت الرسالة ربط مفتاح التشفير بناتج دورات التشفير للحصول على نسبة انهيار جيدة بعد زيادة عدد المقاطع، بلغت نسبة التغيير في النص المشفر (95.8%) عند تغيير حرف واحد من النص الأصلي في ملف حجمه 15 KB ضمن سرعة أداء وانتاجية جيديتين في علميتي التشفير وفك التشفير.

Ministry of Higher Education and

Scientific Research University of Mosul

College of Computer Science and Mathematics

Department of Computer Science

Implementing aproposed Block cipher algorithm for text

A Thesis Submitted to the Council of the College of Computer Science and Mathematics University of Mosul as a Partial Fulfillment of Requirements for the Degree of Master of Science in Computer Science

By

Amina Khaled Khalel Alregabo

Supervised by

Assist. Prof. Dr. yassen hekmet ismail

2023 A.D. **1444 A.H.**

Abstract

After the wide spreard of the Internet use and the circulation of files between users expanded, information security became one of the important priorities that must be achieved by means of different systems. Information encryption comes at the forefront of the techniques used in information security. Thus, traditional cipher systems appeared, which soon developed greatly. The traditional cipher methods are still used in many scientific studies and developmental research with the aim of developing new substitution and compensation cipher systems and increasing its ability to confront various attacks.

The traditional encryption methods were subjected to several attacks, that prompts researchers to develop them and overcome their weaknesses in front of these attacks. Some researchers used combinations of these methods to design new encryption systems based on overlapping ideas of traditional encryption methods. Their use in addition to modern encryption systems aim to increase the strength of encryption.

This thesis deals with the use of a set of traditional encryption methods to design a new block cipher system. In which, these methods are mixed with modern ideas that help to increase the strength of encryption and its ability to confront some attacks such as frequency analysis, to present a block cipher system that includes in its design a number of traditional systems in cryptography, such as (Ceaser, Vigener, Rail Fence), permutation and substitution ciphers, with some basic concepts in block cipher systems. The proposed system relied on the chaotic function Tent map for its random properties to generate a random key string. It used a new method in dealing with plain text characters in its standard format (A-Z) without converting it into binary format to reduce programming complexity. This format was used in building compensation and substitution boxes.

The thesis presented linking the encryption key to the output of the encryption rounds to obtain a good avalanche effect rate after increasing the number of the replaced syllables. The percentage of change in the ciphertext is about (95.8%) when changing one letter of the original text within the speed of good performance and productivity in the encryption and decryption processes.