بِسْمِ اللهِ الرَّحْمنِ الرَّحِيمِ

قَالَ اللهُ تَعَالَى:

۞﴿"نَرْفَعُ دَرَجَاتٍ مَنْ نَشَاءُ ۗ وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ "﴾۞

الآية ۞(٧٦)۞ سورة يوسف

صدق الله العظيم

Dedication

To my parents for their love and support throughout my life…..

To my beloved brothers and sisters….

To my Teachers, Students, Friends and everyone who have been a part of my life…..

ACKNOWLEDGEMENT

First, I would like to thank Allah for giving me the power and health to do this work.

Second, I would like to express my special thanks to my supervisor ***Dr: Faisal Mohammed Abdallah*** *for the guidance, encouragement and advice.*

I am indebted to the Sudan University of Science &Technology for providing the facilities to conduct this work.

Finally, grateful acknowledgement is made to all those who participated with their time, effort, advise and knowledge to make this a successful study.

ABSTRACT

The increase use of the electronic communication demands more security on the exchange of the critical information. cryptography now a day's get more and more important to address this issue. encryption algorithms available for textual data are highly efficient. but sometime the information is available in form of image. in such cases we need a specialized algorithm that is highly optimized to protect pictorial information. in this research two state tables are used to solve correlation problem between the public known output of internal state by using permutation between state1 and state2 that is improve the RC4 algorithm. the enhanced RC4 Algorithm is used for images encryption and decryption the results obtained show that, the enhanced RC4 achieved high security compared with standard RC4, so it can be used in WEP protocol instead of RC4 to overcome weak keys problem. diehard statistical test tool is used to test the randomness of the enhanced RC4 algorithm, also we measure the efficiency of the method using Peak Signal -to-Noise Ratio (PSNR)and mean squared error (MSE) and results obtained give optimum values of robustness.

المستخلص

إن التطور السريع في المجالات التقنية أدى إلى زيادة الإتصال الإلكتروني مما يتطلب تحسين التأمين لتبادل المعلومات الحساسة . يعتبر علم التشفير من العلوم المهتمة بتلك القضايا . خوارزميات التشفير المستخدمة للبيانات النصية ذات كفاءة عالية ، ولكن في بعض الأحيان المعلومات تكون في شكل صور وبالتالي نحتاج إلى خوارزميات متخصصة لحماية معلومات الصورة . في هذا البحث قمنا بإستخدام (two state table) لحل مشكلة الارتباط بين الناتج المعروف مسبقاً داخل ال(state) بإستخدام تبديل بين ال (state1) و (state2) لتحسين خوارزمية(RC4). الخوارزمية المحسنة تم إستخدامها في تشفير وفك تشفير الصور .وكانت النتيجة الحصول على خوارزمية محسنة حققت درجة عالية من الأمن مقارنة ب(RC4) ولذلك يمكن إستخدامها في بروتوكول ال(WEP) بدلاًمن ال(RC4) لتفادي مشكلة ضعف المفاتيح .لقد قمنا بإستخدام أداة (Diehard) الإحصائية لإختبار العشوائية في خوارزمية (RC4) المحسنة ومن ثم قمنا بقياس كفاءة الخوارزمية بإستخدام (PSNR) و(MSE) والقيم الناتجة من الخوارزمية أعطت نتائج جيدة.

List of Tables

List of Figures

List of Abbreviations

Abbreviations	Stand For
RC4	Rivest Cipher
WWW	World Wide Web
WPA	Wi-Fi Protected Access
WEP	Wired Equivalent Privacy
DES	Data Encryption Standard
AES	Advance encryption Standard
LFSRs	Linear Feedback Shift Registers
KSA	Key Scheduling Algorithm
PRGA	Pseudo Random Generator algorithm
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
ERC4	Enhanced Rivest Cipher

Contents