|  |  |
| --- | --- |
| Prof. Dr. Abdul Hamid M. Ragab, Co-researchers: Nabil A. Ismail, Osama S. Farag Allah | Researcher/s |
| تحسين وتنفيذ تشفير RC6 لكتل البيانات وذلك من أجل التحقق من أمن البيانات | Research Title (Arabic) |
| Enhancements and Implementation of RC6 Block Cipher for Data Security | Research Title (English) |
| أمن البيانات | Research Topic (Arabic) |
| Data Security | Research Topic (English) |
| جمعية مهندسي الكهرباء والإلكترونيات | Publisher (Arabic) |
| IEEE | Publisher (English) |
| 2001 | Publishing Year (Arabic) |
| 2001 | Publishing Year (English) |
| ISBN: 0-7803-7101-1  ieeexplore.ieee.org/iel5/7544/20542/00949566.pdf  http://ieeexplore.ieee.org/xpl/freeabs\_all.jsp?arnumber=949566 | ISBN |
| أمن البيانات ، تشفير كتل البيانات | Key Words (Arabic) |
| Data Security, Block Cipher | Key Words (English ) |
| Ieeexplore, 2001 | Journal Name, or (Conference + place and date being held) |
| vol.1 | Volume No. or Issue No. and the Number of Pages in case it has been published in a scientific journal |
| تعرض هذه الورقة العلمية أسلوب تشفير يطلق عليه تشفير كتل البيانات ويتميز بالسرعة والتطوير وهو عبارة عن خوارزمية تشفير متناسقة ومصممة لتلبية طلبات معايير التشفير المتقدم AES. التشفير عبارة عن امتداد مطور لتشفير كتل البيانات باستخدام شفرة RC6 مع امكانية زيادة الأمان وتحسين الأداء. يستخدم اسلوب كتلة التشفير التحويرات المعتمدة على البيانات بشكل كبير. ومن أهم صفاتها البارزة هو استخدام ثمانية سجلات للعمل بدلاً من أربعة وأيضا احتوائها على عمليات ضرب الأعداد الصحيحة كعمليات إضافية أولية. إن إجراء عملية الضرب باستخدام ثمان سجلات يزيد من الإسهاب في كل دورة بحيث تزيد نسبة الأمان وتقل عدد الدورات ومن ثم يؤدي ذلك إلى زيادة في الإنتاجية. باستطاعة هذا الأسلوب التعامل مع نصوص ذات 256 – بت وتشفير كتل النصوص ما يجعله قابلاً للتنفيذ باستخدام البرمجيات والعتاد الإعتيادي. يتوقع من هذه التحسينات أن توافي بمتطلبات السوق ومطوري أنظمة الأمان باستخدام المعالجات المتطورة المتوفرة. لقد تم تنفيذ توصيف متكامل لأسلوب تشفير كتل البيانات المطور، وتم اجراء عدة اختبارات باستخدام المتجهات للتحقق من صحة خوارزمية التشفير وفك التشفير. وتم مناقشة أيضاً تقييم ومقارنة الأداء لأسلوب تشفير كتل البيانات ، و أسلوب RC5 ، وأسلوب RC6 وأيضاً اسلوب نظام تشفير البيانات المسمى DES. تظهر نتائج المحاكاة بأن اسلوب تشفير كتل البيانات هذا قد حقق انتاجية قصوى ووقت قصير في للقيام بعملية التشفير. | Research Abstract (Arabic) |
| This paper presents an Enhanced fast Block Cipher, which is a symmetric encryption algorithm designed to meet the requirements of the Advanced Encryption Standard (AES). It is an enhancement extension of RC6 block cipher with the potential of increasing security and improving performance. The proposed block cipher makes essential heavy use of data-dependent rotations. Its salient features include the use of eight working registers instead of four, and the inclusion of integer multiplication as an additional primitive operation. The use of multiplication with eight working registers greatly increases the diffusion achieved per round, allowing for greater security, fewer rounds, and increased throughput. It is also capable to handle 256-bits plaintext and ciphertext block sizes and suitable to be implemented simply using hardware or software. These enhancements are expected to satisfy market demands and system security developers using advanced processors available. A complete specification and implementation for the enhanced block cipher are given. Several test vectors are used for inspecting the validity of the encryption and decryption algorithm. Comparative performance evaluation of the proposed block cipher, RC6, RC5, and DES are addressed. Simulation results show that the enhanced block cipher achieves maximum throughput and minimum encryption time. | Research Abstract (English) |