|  |  |
| --- | --- |
| Prof Dr Abdul Hamid M. Ragab | Researcher/s |
| تحسين أداء التشفير الخاص بكتل البيانات في أمن نظم المعلومات | Research Title (Arabic) |
|  Enhancing Block Ciphers Performance in Information Systems Security | Research Title (English) |
| أنظمة الأمان | Research Topic (Arabic) |
| Security Systems | Research Topic (English) |
|  جامعة الملك عبد العزيز ، المدينة المنورة | Publisher (Arabic) |
| King Abdulaziz University, The Enlightened City of Al-Madina | Publisher (English) |
|  صفر 1425 ه / أبريل 2004 م | Publishing Year (Arabic) |
| April, 2004 | Publishing Year (English) |
|  | ISBN |
| أمن الأنظمة ، تشفير كتل البيانات | Key Words (Arabic) |
|  Systems Security , Block Ciphers | Key Words (English ) |
| 7th National Conference for Computing and Informatics to Serve The Allah’s Guests (Pilgrims), April 2004 المؤتمر الوطني السابع عشر للحاسب الآلي ، المعلوماتية في خدمة ضيوف الرحمن ، صفر 1425 ه / أبريل 2004 م | Journal Name, or (Conference + place and date being held) |
|  | Volume No. or Issue No. and the Number of Pages in case it has been published in a scientific journal |
| تقدم هذه الورقة العلمية بعض المعايير الجديدة والتي يمكن استخدامها في تعزيز تصميم طرق التشفير الخاصة بكتل البيانات مثل أسلوب معيار تشفير البيانات DES ، واساليب التشفير RC5 و RC6 و ERC6. حيث تقدم لمصممي الأمان تشكيلة واسعة من القيم والمتغيرات التي يمكن عن طريقها انتقاء خوارزمية التشفير التي تتميز بالسرعة ونسبة الأمان العاليتين وذلك من أجل تحسين التطبيقات التي يتم انتاجها، وفي نفس الوقت تقديم اسلوب مبتكر من أجل ضبط المتغيرات حسب الحاجة. ولقد تم تعريف دالة الأمان وعوامل الأمان حيث بإمكان المصمم أن يحدد نقطة العمل القصوى لأسلوب التشفير وذلك من أجل الوصول إلى أعلى نسبة للأمان وكذلك أعلى سرعة ممكنة. تم تحليل النتائج ومقارنتها مع دراسات مشابهة. ولكن الدراسة الحالية تعتبر فريدة من نوعها من حيث تغطيتها لبعض المتطلبات الضرورية المطلوبة لتحسين تصميم الأمان في أنظمة المعلومات. | Research Abstract (Arabic) |
| This paper introduces some new criteria that can be used for enhancing the design of block ciphers such as DES, RC5, RC6, and ERC6. They provide security designers with a range of parameter values so that they can select an encryption algorithm whose security and speed are optimized for enhancing their applications, while providing an evolutionary path for adjusting their parameters as necessary when needed. A security function and a security factor are defined, by which a designer will be able to determine an optimal operating point of the cipher for optimizing both information system security and speed. Results are analyzed and compared with similar studies. However, the work described here is unique and covers some important requirements needed for enhancing the design of information systems security. | Research Abstract (English) |