|  |  |
| --- | --- |
| Prof. Abdul Hamid M. Ragab, Co-researchers: Ismail, N.A. Allah, O.S.F. | Researcher/s |
| خوارزمية فعالة "لهضم الرسالة" وذلك من أجل تأمين البيانات | Research Title (Arabic) |
| An efficient message digest algorithm (MD) for data security | Research Title (English) |
| خوارزميات أمن البيانات | Research Topic (Arabic) |
| Data Security Algorithms | Research Topic (English) |
| جمعية مهندسي الكهرباء والإلكترونيات | Publisher (Arabic) |
| IEEE | Publisher (English) |
| August 2002 | Publishing Year (Arabic) |
| أغسطس 2002 | Publishing Year (English) |
| 0-7803-7101-1 | ISBN |
| أمن البيانات ، خوارزميات الهضم | Key Words (Arabic) |
| Data security, Digest algorithms | Key Words (English ) |
| IEEE Xplore , August 2002 | Journal Name, or (Conference + place and date being held) |
| **Volume:** 1 | Volume No. or Issue No. and the Number of Pages in case it has been published in a scientific journal |
| تقدم هذه الورقة العلمية خوارزمية مقترحة لهضم الرسائل. تعتبر مميزات هذه الخوارزمية متشابهة مع فصيلة خوارزميات هضم الرسائل (4) MD4 لدوال التجزئة من حيث مجال التطبيق والأداء وبنية التنفيذ. الخوارزمية المقترحة تقوم بإدخال رسالة عشوائية الطول وتخرج رسالة تم هضمها وتحويلها إلى ترميز ذو 128/160بت. من ضمن الخصائص الجديدة للخوارزمية المقترحة الأستخدام المكثف للتحويرات المعتمدة على البيانات و احتواء عملية الضرب للأعداد الصحيحة كعمليات إضافية أولية. من المتوقع ان ترفع هذه المميزات الفريدة من مستوى أمان البيانات مع تعزيز الإنتاجية. الخوارزمية المقترحة أعدت لغرض تطبيقات التواقيع الإلكترونية، حيث لا بد من ضغط الملفات الكبيرة بطريقة مؤمنة قبل توقيعها (تشفيرها) بمفتاح سري خاص ضمن نظام تشفير المفتاح العام. لقد تم تصميم الخوارزمية المقترحة لتكون أسرع على أنظمة 32 بت. بالإضافة إلى أنها لا تتطلب أي جداول تعويض كبيرة الحجم ، لذلك يمكن ترميز الخوارزمية بشكل مضغوط. لقد قمنا بوصف الخصائص العامة والهيكلية وكذلك التنفيذ لهذه الخوارزمية وأعطينا مواصفات مكتملة لنظام هضم الرسائل ذو 120/160بت. لقد تم استخدام عدة متجهات اختبار للتتحقق من دقة الخوارزمية المقترحة. بالإضافة إلى القيام بمقارنة الأداء البرمجي لعدة خوارزميات معتمدة على نظام هضم الرسائل (4) MD4 والتي تعتبر ذات أهمية مستقلة. تبين نتائج المحاكاة بأن انتاجية الخوارزمية المتقرحة ذات نظام 128 لهضم الرسائل تصل غلى 76.4 ميجا بت بينما خوارزمية RIPEMD-128 ( تصل إلى 69.8 ميجا بت فقط. | Research Abstract (Arabic) |
| This paper presents a new proposed message digest (MD) algorithm. Many of its characteristics (application domain, performance and implementation structure) are similar to those of the MD4 family of hash functions. The proposed algorithm takes as input a message of arbitrary length and produces as output a 128/160-bit fingerprint or message digest. New features of the proposed algorithm include the heavy use of data-dependent rotations and the inclusion of integer multiplication as an additional primitive operation. These proposed features are expected to provide a high security level with enhancement in throughput. The proposed algorithm is intended for digital signature applications, where a large file must be compressed in a secure manner before being signed(encrypted) with a private secret key under a public-key crypto system. The proposed algorithm is designed to be quite fast on 32-bit machines. In addition, it does not require any large substitution tables, so that the algorithm can be coded quite compactly. We describe its general characteristics, architecture and implementation, and give a complete specification for MD-160/128. Several test vectors are used to inspect the validity of the proposed algorithm. Also, we compare the software performance of several MD4-based algorithms, which is of independent interest. Simulation results show that the throughput of the proposedMD-128 algorithm is about 76.4 Mbit/s while that of RIPEMD-128 (Race Integrity Primitives Evaluation MD, 128-bit) is about 69.8 Mbit/s. | Research Abstract (English) |