Abstract

Blowfish is a secret-key block cipher designed in 1994. It is a Feistel network, iterating a simple encryption function 16 times. The block size is 8-bytes and the key can be any length up to 256-bytes. Serpent block cipher algorithm was designed in 2000. Serpent is a 32 round iterated block cipher with a 128-bit block size and uses 128, 192, and 256 bits key length. But the fact remains that the best Serpent software implementation will be 3-4 times slower than other candidates.

B-S, a new secret-key block cipher, is proposed. It is a Feistel network, iterating a simple encryption function 16 times. The block size is 128 bits, and the key can be any length up to 256 bytes. It is designed to take advantage of the powerful algorithm, which is supported by Blowfish and Serpent algorithms with overcoming their weaknesses, resulting in a much improved security/performance tradeoff over existing ciphers. As a result the proposed algorithm offers better security than Blowfish and Serpent algorithms.

The proposed algorithm is compact, fast, simple and easy to understand. It also uses large key compared with Blowfish and Serpent algorithms and this makes the algorithm infeasible to Brute force attack. To meet the requirements of the AES, a block cipher must handle 128-bit input/output blocks, while Blowfish acts with 64-bits block size. On the other hand, its large memory requirement makes it infeasible for smart card applications. So the B-S algorithm increases the block size and reduces memory requirements to become suitable to hardware implementation.

PDF created with pdfFactory trial version www.pdffactory.com

الخـــــلاصـــــة

خوارزمية الـــ Blowfishهي خوارزمية كتلية ذات مفتاح سري صممت في عام ١٩٩٤, وهـــي تستخدم ال Feistel network,دورية حيث تقوم بتكرار وظيفة function بسيطة ١٦ مرة .حجم الكتلة التي تقوم بتشفيرها ٨ بايت اما طول المفتاح فهو متغير يتراوح من ٦٤-٤٤٨ بت .

خوارزمـــية الـــ Serpent فهي خوارزمية كتلية صممت في عام ٢٠٠٠ تتكون من ٣٢ دورة , دورية , طـــول المفتاح امـــا يكون (١٢٨،١٩٢, ٢٥٦)بت .لكن هنالك حقيقة باقية وهي ان افضل تنفيذ لل Serpent كبرنامج ٣-٤ مرات اضعاف مثيلاتها من خوارزميات التشفير الموثوقة.

B -S الخوارزمية المقدمة فهي خوارزمية كتلية ذات مفتاح سري وهي تستخدم الـــ Feistel network , دورية تستخدم وظيفة Function بسيطة ١٦ مرة ,حجم الكتلة المستخدمة ١٢٨ بت ,المفتاح متغير الطول يصل الى ٢٥٦ بايت .هذه الخوارزمية صممت لأخذ المحاســـن ونقاط القوة الموجدة في خوارزمية Serpent , Blowfish مع تجاوز نقاط الضعف الموجدة فيهما للوصول الى افضل امنية , انجاز , تناوب مع الخوارزميات الموجودةوالنتيجة هو الوصول امنية افضل من خوارزمية Serpent, Blowfish .

الخوارزمية المقترحة هي قوية ,سريعة , بسيطة وسهلة الفهم . اضافة الى ذلك تستخـــدم مفتاح كبير مقارنة مع Serpent, Blowfish وهذا يجعل الخوارزمية صعبة الكسر باستخدام هجوم القوة الوحشية ولتحقيق متطلبات الـــ AES يجب ان يكـــون التشفير الكتـــلي يعـــالج ١٢٨ بت كمدخل ومخرج بينما خوارزمية ال Blowfish تعالج ٦٤ بت ومن جهة اخـــرى احتياجـــها الى ذاكرة كبيرة يجعل تطبيق الخوارزمية ككارت ذكي غير ممكن . لذلك خوارزميـــة الـــ B-Sزادت من حجم الكتلة للتغلب على هجوم الـــ matching attack وتقليل حجم الذاكرة يكون ملائـــم لتطبيقـــها كـــ hardware.

PDF created with pdfFactory trial version www.pdffactory.com