Block VS Stream من الأفضل

شفره التدفق هي أسرع بكثير من شفرات الكتل وعمليه كتابه برامج سهله وأكودها اقل بكثير من الكتل ، واحد اشهر أنواع شفرات التدفق RC4 وهي أسرع بكثير من أي نوع من أنواع شفرات الكتل ، وتتطلب حوالي 30 سطر فقط في الكود . معظم شفرات الكتل تأخذ على الأقل 200-400 سطر.
شفرات الكتل من جهة أخرى تسمح باعاده استخدام المفتاح ، بعكس شفرات التدفق التي تستخدم المفتاح مره واحده فقط ، في الكثير من الأحيان يجب أن نشفر العديد من الأشياء بمفتاح واحد.

مثال ، شركه لديها قاعدة بيانات ضخمه للعملاء تحتوي معلوماتهم من أرقام هواتف وبطاقات ائتمانية وغيرها ، في حال استخدمت شفرات التدفق سوف تتطلب لكل مدخل (عميل) مفتاح خاص وهذا يتطلب مئات من المفاتيح وهو أمر غير عملي ، أما في حاله استخدمت شفرات الكتل فإنها تشفر جميع البيانات باستخدام مفتاح واحد ، ولفك تشفير بيانات أي عميل نستخدم نفس المفتاح . عمليه اداره المفتاح أسهل بكثير في هذه الحالة.

لذلك في معظم قواعد البيانات يتم استخدام شفرات الكتل Block Cipher وأيضا في برامج البريد الالكتروني ، وأيضا في برامج تشفير الملفات.

Digital Encryption Standard

في بدايه السبعينات تم معرفه انه اغلب الشفرات القديمة لم تعد مجديه وغير نافعة للتشفير ، ولهذا قرر علماء في شركه IBM بعمل خوارزمية جديدة للتشفير تبنى على بنية قديمة تسمى Lucifer (نسبه إلى مخترعها Horst Feistel) ، ومن خلال مساعده وكاله الأمن القومي NSA تم عمل خوارزمية DES .

DES هي احد شفرات الكتل Block Cipher ، وتأخذ مفتاح بطول 56 بت ، وتعمل على كتله طولها 64 بت .

وفي الثمانينات لم يتم اكتشاف أي ثغره في DES لذلك كانت اقوي الخوارزميات في ذلك الوقت، ولكسر أي رسالة مشفره بها لم يكن هناك إلا استخدام هجوم الـ brute-force ، ولأن طول المفتاح 56 بت (مداه من 0 إلى 72 كوارلديون) و الاجهزه بطيئة للغاية ، فكانت عمليه الكسر تتطلب سنه كاملة.

وفي 1999 وفي احد المؤتمرات تم كسر هذه الخوارزمية في 24 ساعة من قبل the Electronic Frontier Foundation اذا العالم يجب أن ينتقل إلى خوارزمية أخرى .

Triple DES

احد البدائل كانت خوارزمية Triple DES أو البعض يسموها 3DES ، هي بكل بساطه DES ولكن ثلاثة مرات ، يعني سوف تدخل الكتلة الأولى (16 بايت) إلى الخوارزمية بالمفتاح الأول ، والناتج سوف يدخل إلى الخوارزمية مع المفتاح الثاني ، والناتج سوف يدخل مع المفتاح الثالث .