على العموم DES 3 لها مشكله وهي أنها بطئيه جدا ، الـ DES العادية هي بطيئة ، فما بالك بـ DES ثلاث مرات ، واغلب التطبيقات تتطلب السرعة في العمل ، وهذه الخوارزمية لا تنفع لأنها بطيئة جدا ، اذا العالم مره أخرى بحاجه إلى خوارزمية!!

البدائل:

بعد مشكله البطء في خوارزمية الـ DES 3 ، اتجه العديد من الأفراد والشركات لتطوير خوارزمياتهم الخاصة وكانت النتيجة أن هناك العديد من الخوارزميات الجيدة والتي تأخذ مفاتيح متغير الطول (وليس ثابتة الطول كما في DES) ، من هذه الخوارزميات
RC2, RC5, IDEA, CAST, SAFER, Blowfish .
هذه الخوارزميات بالرغم من قوتها لم تصبح واسعة الانتشار كما في DES و Triple DES .
اذا العالم بحاجه هذه المرة إلى مقياس أو خوارزمية واسعة الانتشار كـ DES

Advanced Encryption Standard

نتيجة لهذا الأمر قام المعهد الوطني للمعايير National Institute of Standards and Technology اختصارا NIST ، باستدعاء جميع المهتمين بهذا الأمر وكلفت بكل منهم بعمل خوارزميته الخاصة وفي النهاية أقوى خوارزمية سوف تكون هي المقياس الجديد AES ، وقد قدمت 15 خوارزمية (منها القوي ومنها الضعيف) .

وفي 1999 قامت NIST باختيار أفضل 5 خوارزميات بعد إجراء العديد من الاختبارات ، وقد جعلت الأمر بالتصويت لأفضل خوارزمية ، وفي 2000 تم اختيار خوارزمية **Rijndael** كالمقياس الجديد AES .

اداره المفتاح المتناظر *Symmetric-Key Management* :

توصلنا سابقا إلى أن التشفير بالمفتاح المتناظر يقوم بتشفير الرسالة بمفتاح ما ، ثم يقوم بفك التشفير بنفس المفتاح ، لذلك عمليه الحفاظ على المفتاح أمر في غاية الاهميه ، فإذا انكشف المفتاح انكشفت جميع الأسرار ، لذلك يجب حفظ المفتاح في مكان امن جدا ، عمليه الحفاظ على المفتاح تسمى بـ **اداره المفتاح Symmetric-Key Management** .

ربما الآن تتساءل"اذا كان هناك مكان أستطيع أن احفظ في المفتاح ، فلماذا لا احفظ الرسالة في ذلك المكان ولا احتاج إلى التشفير" ؟

في الحقيقة حفظ مفتاح التشفير (56 بت مثلا) يكون أسهل كثيرا من حفظ الرسالة (بعض الأحيان حجمها يكون مئات من الميغا بايت MB) ، بالاضافه إلى هناك حلول لحفظ المفتاح عن طريق حفظها داخل أجهزه صغيره مصممة لهذا الغرض.

Password-Based Encryption

إن المفتاح الذي كنا نستخدمه للتشفير وفك التشفير يسمى في الحقيقة "**بمفتاح الجلسة session key**" ، وأحد الطرق لحماية هذا المفتاح هي عن طريق تشفيره أيضا ، أي أن المفتاح (مفتاح الجلسة) يحتاج إلى مفتاح آخر لكي يتم تشفيره.