Data Standard Encryption

KING SABRI : الكاتب

أحبتي في الله .. السلام عليكم ورحمة الله وبركاته

موضوعنا اليوم لن أقول أنه جديد لكني سأقول أني أكاد أجزم أنه لأول مرة يتم عرضه بهذا الطريقة بين الصفحات العربية .. لن أعرّف هنا معنى كلمة تشفير لأن المقدمة الواجب أن أضعها قد وضعها إخواني في المنتديات و جزاهم الله عنا خير الجزاء. لكني سأضع أمامك مادة علمية قويه جدا تشرح واحد من أقدم خوارزميات التشفير و أقواها – قد يعترض أكثركم على كلمه أقواها لكن عندما تم عمل هذا الخوارزم و إعتماده كان من أقوى أنواع التشفير في و قته و قد تم تحديثه أكثر من مرة و أصبح هناك الـ Double DES و Treble DES و Advanced DES (AES) - وللعلم لو تم فهم موضوعنا هذا فستعرف بحق معنى كلمه تشفير و كيف يتطور علم التشفير بالنسبه للتشفير المتماثل أو ال Symmetric Encryption و ما سيأتي في المسقبل لن يكون غريبا عنك أبدا بعد ذلك سأضع الرسومات (الخوارزميات) ثم أشرحها .. لندخل في الموضوع

Data Encryption Standard (DES)

تم إختياره في عام ١٩٧٧م قِبل المعهد الدولي للمعايير التكنولوجية أو National Institute Standard Technology (NIST) على أنه معيارا للتشفير دوليا و يتم التطوير على أساسه في أنواع التشفير اللتي هي من فئته أي Symmetric Encryption و قد كان لـ IBM باعا في وضع بذرة هذا التشفير لا نستطيع تجاهله.

أعتقد تكفي هذه المقدمة ..... نبدأء الشغل

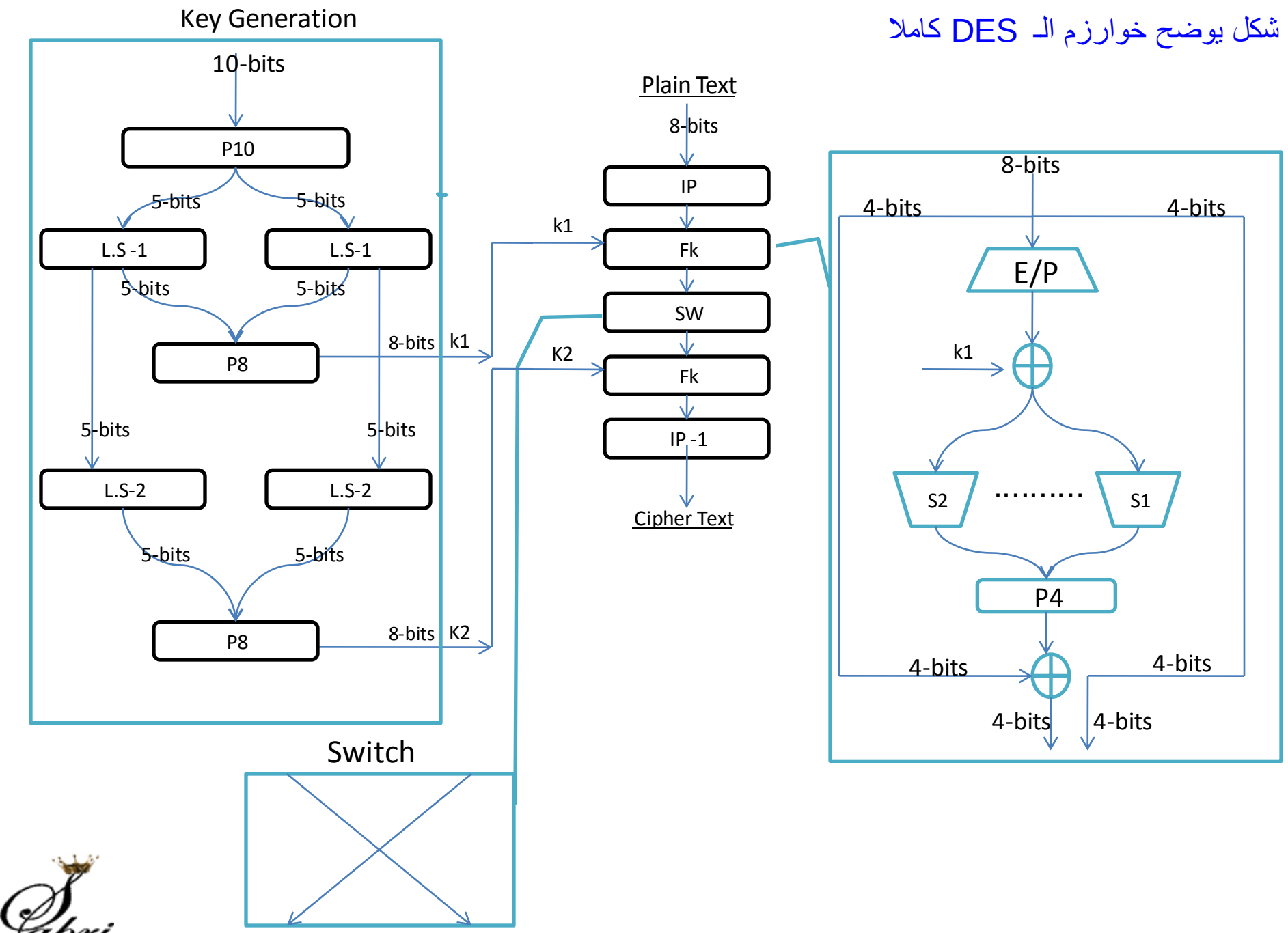
بسم الله

ملاحظة : هذا العلم درسته في آخر سنة في هندسة حاسب آلي و طرحه يجبرني على الإعتماد أن قارئ الموضوع يعرف أساسيات التعامل مع ال B!n@ry و مع العمليات المنطقية وقد نوهنا أن أساسيات التشفير و المقدمه المطلوبة قد كتبها إخواني من قبل و Google خير برهان

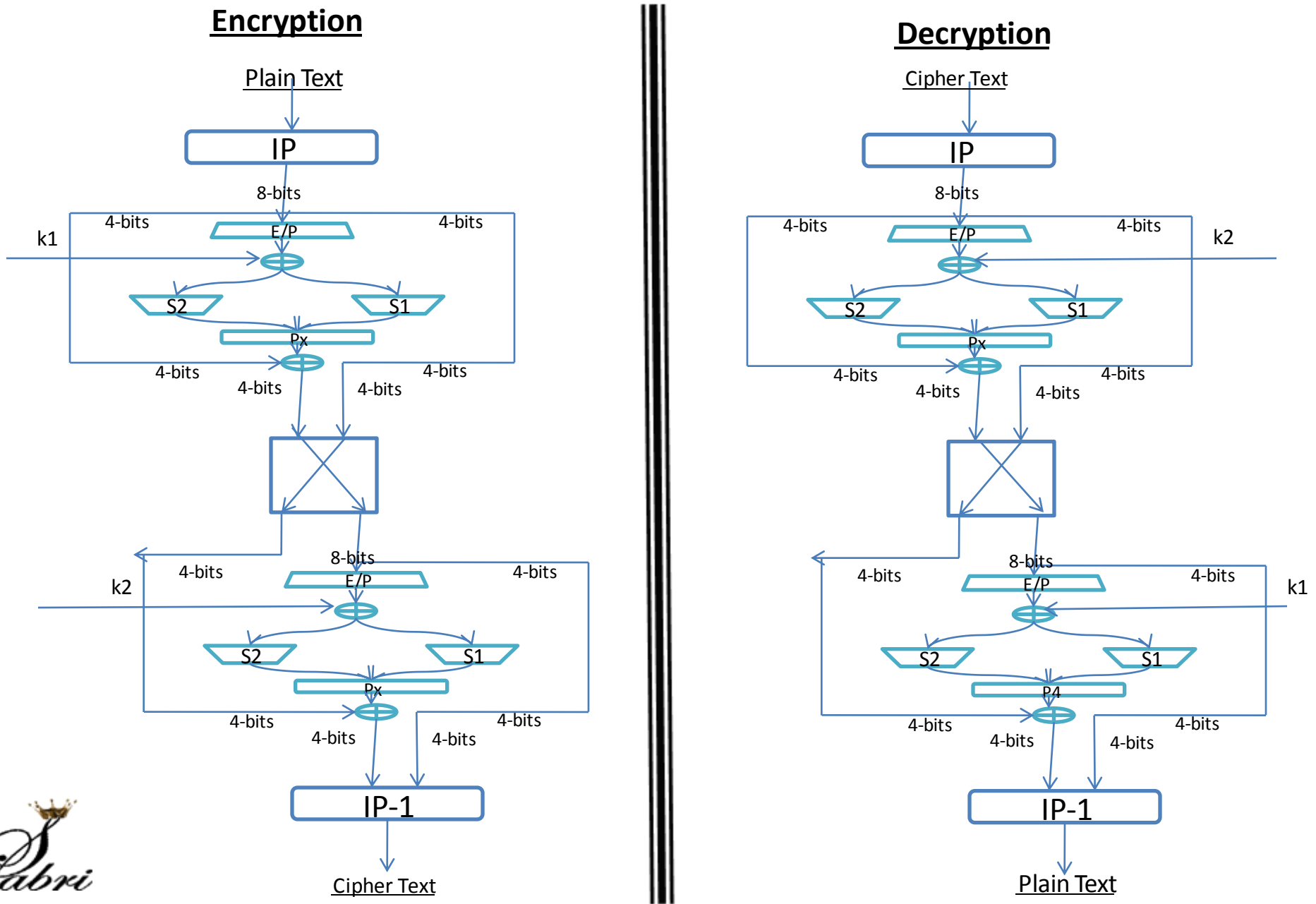
لندخل في الموضوع

Sabri

شكل يوضح خوارزم الـ DES كاملا



Final DES Algorithm

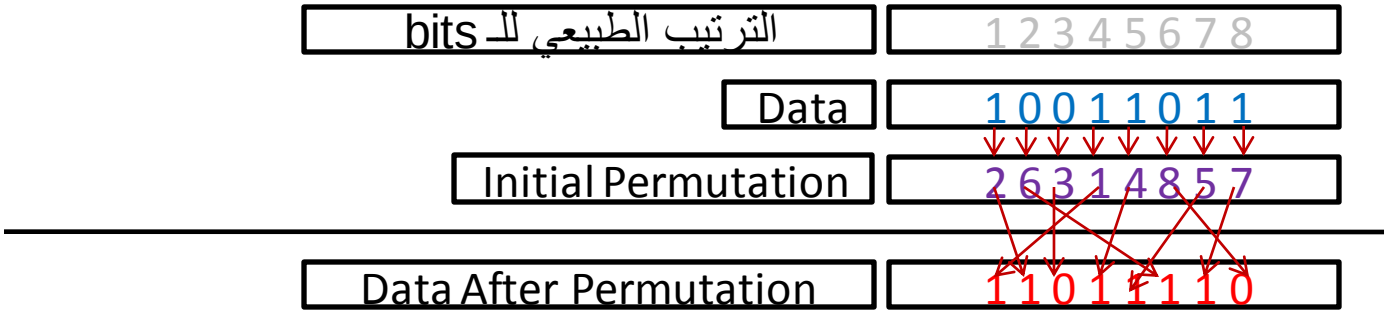


طبعا يا إخواني الأحباء لم يفهم أحد ما هذه الرسومات أو معاناها بشكل دقيق ... ولا أنا D: لكن بإذن الله سنعلم ماذا هناك...
و سنعرف الأشياء غالبا بمعناها العلمي العملي أي نعرفها بوظيفتها لنبعد عن الكلام النظري البحت و يجب أن نظع دوما في الحسبان أنا تعاملنا مع ال data سيكون على شكل Binary و في بعض الأجزاء سنستخدم ال Decimal ....لنبدأ على بركه الله بالتفاصيل .

تعاريف :/

Initial Permutation (IP) : بالبلدي معناها اللخبطة و حرفيا التبديل المبدئي و وظيفتها أن ندخل لها 8 بت فنقوم بتغيير أماكنهم بشكل غير منظم بناءً على أرقام تم تحديدها بطلبنا و تكون من رقم 1 إلى رقم 8 ولكن تلك الأرقام غير مرتبه (لم تفهموا شئ هههههه) سأريكم مثالا عمليا ...
عندي 8 bits و هم من اليسار إلى اليمين كالتالي : 10011101 فإن ترتيب أول bit الذي هو 0 سيكون 1 و الثاني الذي هو 1 سيكون 2 إلخ...
جميل ؟؟ ... إذن لو كان عندي ال IP =[26314857] و تقرأ أيضا من اليسار إلى اليمين فهو يقصد أن يلخبط أول Bit عندي اللذي هو 1 يجعله الثاني و أنا ترتيب ثاني Bit عندي اللذي هو 0 سيكون السادس و هكذا
أي أن ال Stream السابق (10011101) سيصبح شكله بعد إدخاله في عملية ال Initial Permutation هكذا (01011110)

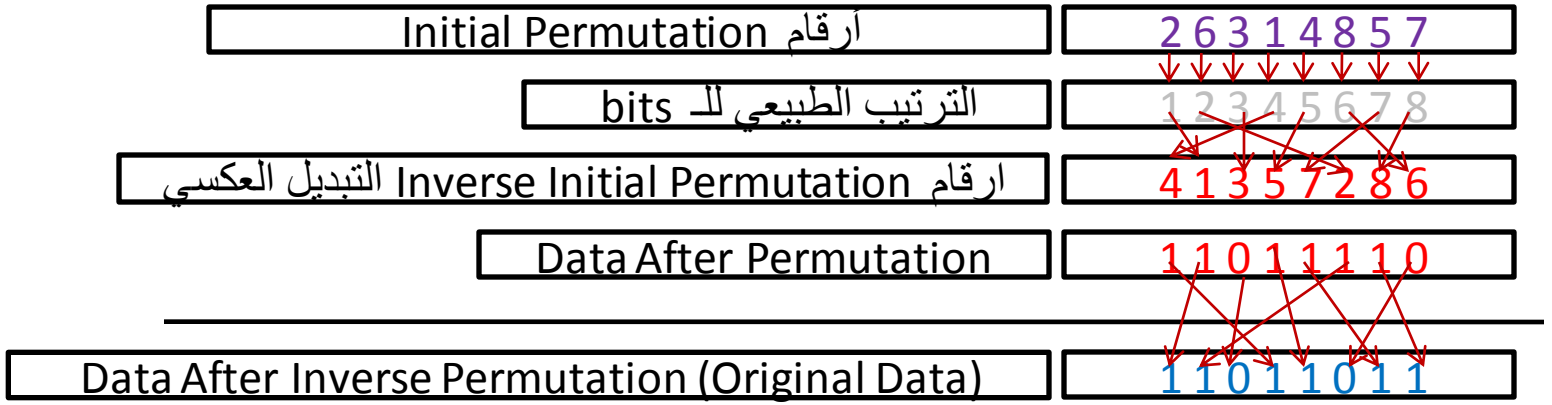
مثال آخر :
Data = 10011101 , IP=[26314857]
11010110=Data (ip)



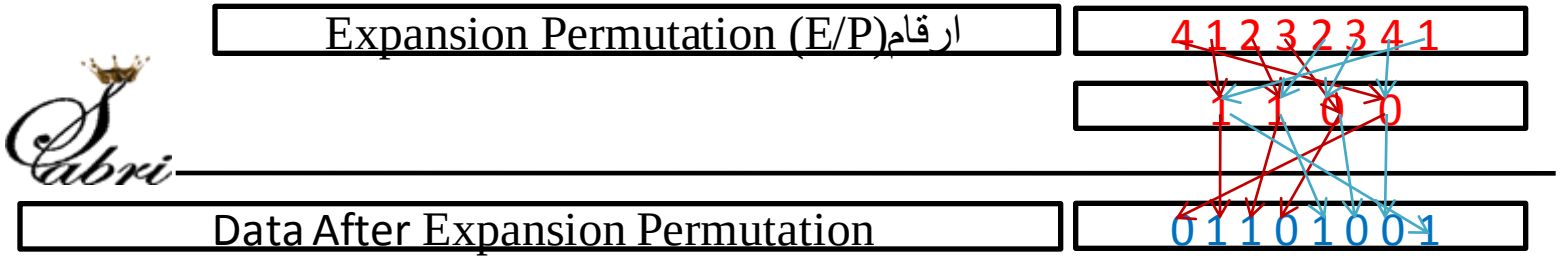
Inverse Initial Permutation (IP-1) :

- نرقم الـ Inverse Initial بالترتيب من اليسار إلى اليمين
- ننظر إلى أرقام الترتيب الطبيعي للـ bits ثم نجعل ترتيبها في المكان الذي يساوي الرقم المقابل له في الـ Inverse Initial

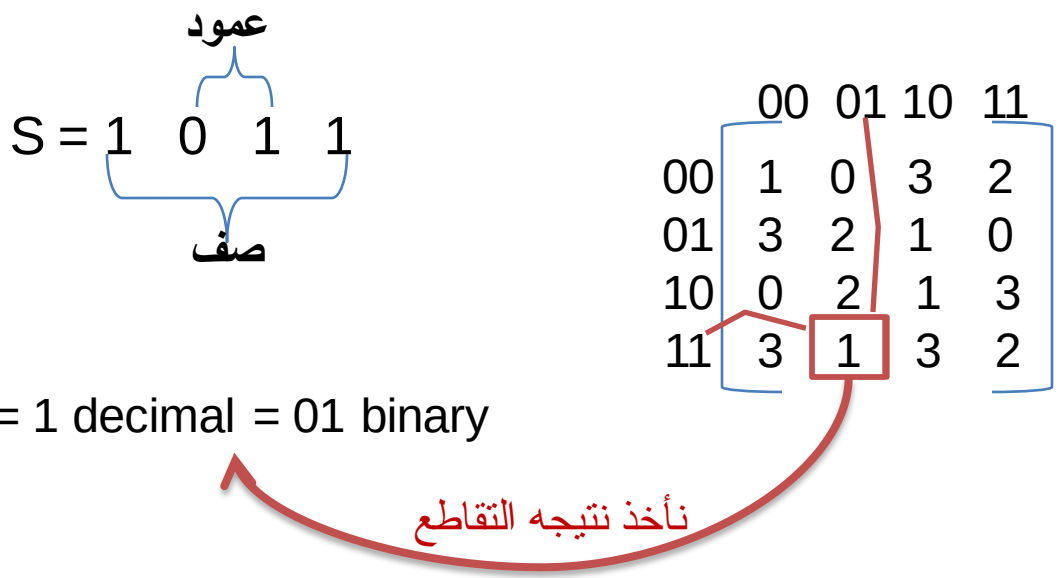
بهذا نكون أخرجنا أرقام التبديل العكسي



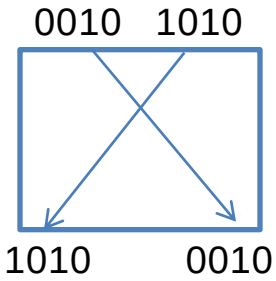
Expansion Permutation (E/P) : وهي عملية اللخبطه أيضا كما عهدناها لكن ستتسبب في زياده عدد ال bits لذلك سمية Expansion . و هطريقته هو أن نكرر ال bit على حسب تكرار مكانه في ال E/P مثال عملي



S-Box: هي عملية Permutation لكنها مختلفة تماما عن سابقاتها و ستتسبب في تقليص عدد ال bits إلى 2bits وتستخدم اللتبديل بالمصوفات أو الـ Matrices لإيجاد قيمتها و في المسائل العلميه فإنك تعطى المصفوفة و قيمة الـ S تسخرجها من تقاطع الصف مع العمو من ثم تحول القيمه إلى binary
هكذا .....



Switch (SW) : من الإسم العمليه واضحه هنا أي أنه سيقوم بتغيير مسار ال bits التي في ناحية إلى الناحيه الأخر و أظنها واااااضحه من الرسمة ...



Key Generation : وهو مولد المفاتيع اللتي ستضاف على ال Data لتزداد عملية اللخبطة أو تعقيد التمويه و التبديل و نستطيع أن نولد أكثر من **Sub key** في ال DES التفاصيل قادمة ....

Left Shift (LS-x) : يعني **ترحيل أو إزاحه** عدد محدد يتم تحديده في الأول نزيع بمقدار واحد و الثاني بمقدار ٢ و هكذا يكب أن تراقب الرسمه الأساسيه أيضا لتكتمل مخيلتك العلميه ويقوم بإزاحه ال bits من اليسار إلى اليمين بغرض اللخبطه و يستقبل في ال DES عدد **5-bits** و عندما تحدد عدد الإزاحات فإنه يبدأ بالإزاحه من اليسار إلى اليمين و يرمز أيضا لها بهذه العلامه ">>>" سنفهم بمثال خفيف ...

k1 k2 k3 k4 k5 نريد أن نعمل لهم إزاحه بمقدار 3 من اليسار إلي اليمين فالناتج سيكون k4 k5 k1 k2 k3
طبعا ال k تعبر عن ال bit الواحد

XOR : هي عمليه منطقيه يكون ناتج ال bits المتشابهة بـ 0 و المختلفة بـ 1 ، مثال ....

$$\begin{array}{r} 0\,0\,0\,1\,1\,0\,1\,1 \\ 0\,1\,0\,0\,1\,1\,1\,1 \oplus \\ \hline 0\,1\,0\,1\,0\,1\,0\,0 \end{array}$$

Data Encryption Standard DES

حسنا .. الأن سنتكلم مره أخرى عن الأجزاء التي عرفناها في التعاريف لكن سنتكلم عنها من ناحية عملها و مهمتها في هذا النظام من التشفير فهذه الأجزاء ليست حصرية لهذا التشفير و لكن يختلف تشفير عن آخر في شكل و خطه الخوارزميات و في Block size of data و في عدد تكرار الشئ وطريقه ترابط جزاء ال data المقسمة ... كل هذا الكلام عام ... لنبدأ و ستعرف معنى كلاماتي هذه عندما نشرح أكشر من نوع تشفير إن شاء الله .

١/ حجم البيانات المراد تشفيرها Plaintext block size :

وجد أنه أنسب حجب للبيانات المراد تشفيرها بالنسبه لـ DES هو 64-bit و إن زادت حجم البيانات عن ضلك فإنها تقسم كما يحصلي في الهارد ديسك ، لكن !.... لو كان حجم البيانات المراد تقسيمها لا يقبل القسمه على 64 لكي نقسمها ... سأبحث عن آخر bit ثم نقوم بعملية ال Padding http://www.di-mgt.com.au/cryptopad.html ، ☹

حسنا بدون نظريسنوضح الأمر بشكل ودي

لنفرض أن حجم ال data المراد تشفيرها هي 660-bit <<< الرسالة الأصلية

660/64=10.3 و نحن نعلم أنه لا يمكن حجز جزء من اللل Block of data ونترك الباقي فارغا فيجب إما ملئه أصفارا وهذا لا يصح مع التشفير لأنه سيأثر على شكل الداتا أصلا أو أنه هناك حل أخر لإصل و بدون تفصيل هو ....

أن نقرب الرقم 10 حتى يصبح ناتج القسمة عدد صحيح بدون كسور هذا كلام عام بالنسبه لل padding لكنه ليس موضوعنا أساسا .

٢/ المفتاح السري Secrete Key Size : تمااااما مثل مفتاح المنزل به تشفر البيانات و به تفك تشفيرها و تجده على كل باسوورد في البرامج ☺ و حجمه في ال DES يصل إلى 65-bit=8 characters

٣/ عدد اللفات Number of rounds : عدد اللفات في ال DES = 16-rounds=16-sub keys وكل subkey حجمه 64-bit

٤/ Key Generation توليد المفاتيح : فإن مولد المفاتيح هو اللذي يخرج ال Subkey فنحن نختار ال Secret key و أما الـ Subkey أجعله عبارة عن 16× 48 حيث ٤٨ هو الحجم الاقصي لل الواحده ، وال ١٦ أقصى عدد Subkey يتحمله ال DES

حسنا ... أعتقد أن الموضوع محتاج تركيز و يحتاج أن تقرأه أكثر من مرة و أن تسأل فيه قبل أن أفكر أن أضح مسأله أني أريد أن أكسر تشفير بال DES رياضيا بطريقة الإحتمالات أو ال Brute Force وعامة سأضل ملخص لأهم خصائص الـ DES لك تتضح الأمور أما عينيك ...

Characteristics	DES
Plaintext Block Size	64-bit
Key Size	56-bit
No. of Sub key	16-bit
Sub key Size	48-bit
No. of S-box	8-bit
S-box Size	4 ×16 -bit
No. of rounds	16-bit

المراجع :

• حبيب قلبي William Stallings و كتابه الأشهر بين نظرائه Cryptography and Network Security الإصدار الرابع
• www.king-sabri.net

للمراسلة : king-sabrii@hotmail.com

أسألكم الدعاء لي ولوالدي ...