DES:

الگوریتم DES در دههٔ ۷۰ میلادی در آمریکا به‌عنوان یک استاندارد کدگذاری مطرح شد. این الگوریتم این‌گونه عمل می‌کند که رشته‌ای از متن اصلی با طول ثابت را به عنوان ورودی می‌گیرد و پس از انجام یک سری اعمال پیچیده روی آن خروجی را که طولی برابر طول ورودی دارد تولید می‌کند DES .هم چنین از یک کلید برای ایجاد رمز استفاده می‌کند و تنها کسانی قادر به رمزگشایی خواهند بود که مقدار کلید را می‌دانند. اگرچه تحلیل‌هایی که دربارهٔ DES انجام شده‌است از هر روش رمز قطعه‌ای دیگری بیشتر است ولی عملی‌ترین حمله علیه این الگوریتم جستجوی جامع فضای کلید است. سه حمله تئوریکی برای این الگوریتم وجود دارند که زمان کمتری نسبت به جستجوی جامع فضای کلید نیاز دارند ولی این روشها در عمل امکان‌پذیر نیستند.

با شکسته شدن الگوریتم DESاین استاندارد در سال ۱۹۹۸ تمدید نشد و در سال ۲۰۰۱، الگوریتم AES به عنوان استاندارد جایگزین آن تصویب شد. این الگوریتم مانند DES یک الگوریتم رمزقطعه‌ای است ولی بر خلاف DES از ساختار فیستل استفاده نمی‌کند. تا سال ۲۰۰۶ تنها حمله مؤثر علیه الگوریتم AESحمله side channel بوده‌است. در ژوئن سال ۲۰۰۳ دولت آمریکا اعلام کرد که از AES می‌توان برای حفاظت از اطلاعات رده‌بندی شده و سری نیز استفاده کرد. برای اطلاعات فوق سری و محرمانه باید از کلیدهایی با طول ۱۹۲ یا ۲۵۶ بیت استفاده کرد.

در سال ۱۹۷۲ مؤسسه بین‌المللی استاندارد و فناوری آمریکا اعلام کرد که به یک الگوریتم برای حفاظت از اطلاعات غیر رده‌بندی شده خود نیاز دارد. این الگوریتم می‌بایست ارزان، قابل دسترس و بسیار مطمئن می‌بود. در سال ۱۹۷۳، NIST فراخوانی برای چنین الگوریتمی اعلام نمود ولی هیچ‌یک از الگوریتم‌هایی که در پاسخ به این فراخوان ارائه شدند شرایط لازم را نداشتند. دومین فراخوان در سال ۱۹۷۴ مطرح شد در این زمان IBM الگوریتم خود را مطرح نمود که به نظر می‌رسید می‌تواند نیازهای NIST را بر طرف کند. این الگوریتم به عنوان یک استاندارد فدرال در سال ۱۹۷۶ تصویب شد و در سال ۱۹۷۷ منتشر شد. با امکان‌پذیر شدن حمله جستجوی جامع فضای کلید برای این الگوریتم، سازمان ملی استاندارد و فناوری آمریکا در آغاز سال ۱۹۹۷اعلام کرد که برای تدوین استاندارد پیشرفته رمزنگاری تلاشی را آغاز کرده‌است. در سپتامبر همان سال این سازمان به طور رسمی فراخوانی را برای ارائه الگوریتم‌های رمزنگاری اعلام نمود.

در کنفرانس اول، AES-1، ۱۵ الگوریتم کاندیدا انتخاب شدند، NISTاز تمام دانشمندان و مؤسسه‌های علمی خواست که نظرات خود را در مورد این الگوریتم‌ها ارائه دهند. هم چنین NIST با کمک جامعه بین‌المللی رمزنگاری و تشکیل کمیته‌هایی، اقدام به بررسی قابلیتها و توانایی‌های الگوریتم‌های ارائه شده نمود. در آگوست سال بعد، در سمینار دوم،

AES-2، پنج الگوریتم انتخاب و برای رقابت نهایی معرفی شدند. این الگوریتم‌ها عبارت بودند از : Rijndael - RC6 - MARS - Twofish - Serpent

آخرین نظرات و انتقادات تا تاریخ ۱۵ مه ۱۹۹۹ جمع‌آوری شد و بالاخره در سمینار AES-3، پس از بررسی گزارش کمیته‌های بررسی کننده، الگوریتم Rijndael به عنوان الگوریتم استاندارد پذیرفته شد.

الگوریتمDES

در DES طول قطعات ۶۴ بیت است. کلید نیز شامل ۶۴ بیت است ولی در عمل تنها از ۵۶ بیت آن استفاده می‌شود و از ۸ بیت دیگر فقط برای چک کردن parity استفاده می‌شود. الگوریتم شامل ۱۶ مرحله مشابه‌است که هر مرحله یک دور ۴نامیده می‌شود. متنی که قرار است رمزگذاری شود ابتدا در معرض یک جایگشت اولیه(IP) قرار می‌گیرد. سپس یک سری اعمال پیچیده وابسته به کلید روی آن انجام می‌شود و در نهایت در معرض یک جایگشت نهایی (FP) قرار می‌گیرد IP,FP .معکوس هم هستند FP عملی که توسط IP انجام شده‌است را خنثی می‌کند؛ بنابراین از جنبه رمزنگاری اهمیت چندانی ندارند و برای تسهیل نمودن بار کردن قطعات داده در سخت‌افزارهای دهه ۱۹۷۰ استفاده شدند ولی اجرای DES در نرم‌افزار را کند کردند. قبل از دور اصلی، داده به دو بخش ۳۲ بیتی تقسیم می‌شودکه این دو نیمه به طور متناوب مورد پردازش قرار می‌گیرند این تقاطع به عنوان شکل فیستل شناخته می‌شود. ساختار فیستل تضمین می‌کند که رمزگذاری و رمزگشایی دو رویه کاملاً مشابه هم هستند و تنها تفاوت آنها این است که زیر کلیدها در زمان رمزگشایی در جهت معکوس رمزگذاری به کار برده می‌شوند؛ و بقیه الگوریتم درهر دو یکسان است که این امر پیاده‌سازی رابه خصوص در سخت‌افزاربسیار آسان می‌کند و دیگر نیازی به الگوریتم‌های متفاوت برای رمزگذاری و رمزگشایی نیست. تابعی که خروجی IP را می‌گیرد وپس از شانزده مرحله ورودی FP را فراهم می‌کند تابع F نامیده می‌شود. این تابع یک ورودی ۳۲ بیتی و یک ورودی ۴۸ بیتی دارد و یک خروجی ۳۲ بیتی تولید می‌کند. بلاک ورودی شامل ۳۲ بیت که نیمه سمت چپ را تشکیل می‌دهد و با L نشان داده می‌شود و به دنبال آن ۳۲ بیت دیگر که نیمه راست را تشکیل می‌دهد و با R نمایش داده می‌شود است. پس کل بلاک را می‌توان به صورت LR نمایش داد.

اگر K یک بلاک ۴۸ بیتی باشد که از کلید اصلی ۶۴ بیتی مشتق شده‌است و خروجی یک دور با ورودی LR و خروجی L1R1به صورت زیر تعریف می‌شود L1=R R1=L XOR F(R,K) .اگر KS تابعی باشد که کلید ۶۴ بیتی KEY و یک عدد صحیح در محدوده ۱ تا ۱۶ را به عنوان ورود ی می‌گیرد و کلید ۴۸ بیتی Kn را به عنوان خروجی تولید می‌کند به طوری که بیتهای Kn از تغییر محل بیتهای KEY حاصل شده‌اند داریم(n.KEY) =Kn KS :

KSرا تابع key schedule می‌نامند؛ بنابراین در حالت کلی داریم Ln=Rn-1 Rn=Ln-1 XOR f(Rn-1,Kn) :برای رمزگشایی نیز داریم R=L1 L=R1 XOR f(L1,K) :

در نتیجه رمزگشایی با همان الگوریتمی که برای رمزگذاری استفاده شد انجام می‌شودو در هر مرحله همان K بیتی که به عنوان کلید برای رمزگذاری استفاده شده بود مورد استفاده قرار می‌گیرد بنابراین می‌توان نوشت Rn-1=Ln Ln-1=Rn : XOR f(Ln,Kn)

برای محاسبات رمزگشایی R16L16 ورودی IP و R0L0 ورودی FP است. کلید شانزدهم در مرحله اول، کلید پانزدهم در مرحله دوم و به همین ترتیب کلید اول در مرحله شانزدهم مورد استفاده قرار می‌گیرد.

تابع F

بسط: در این مرحله با استفاده از یک جایگشت انبساطی ۳۲ بیت به ۴۸ بیت گسترش داده می‌شود.

ترکیب کلید: در این مرحله حاصل مرحله قبل با یک زیر کلید XOR می‌شود. شش کلید ۴۸ بیتی با استفاده از الگوریتم key scheduleاز کلید اصلی تولید می‌شود.

جایگزینی: بعد از ترکیب کلید هر قطعه داده به هشت بخش ۶ بیتی تقسیم می‌شود) قبل از پردازش توسط جعبه‌های جایگزینی (هر کدام ازs-box ها ورودی ۶ بیتی خود را با استفاده از یک تبدیل غیر خطی که به شکل یک جدول look upاست به یک خروجی ۴ بیتی تبدیل می‌کندS-box ها قلب DES هستند و بدون آنها رمز خطی خواهد بود و در نتیجه قابل شکستن خواهد شد.

جایگشت: در نهایت ۳۲ بیت خروجی S-boxها با استفاده از یک جایگشت ثابت مجدداً سازماندهی می‌شود (P-box).

الگوریتمKey Schedule

تولید کلید مراحل مختلف

از این الگوریتم برای تولید زیر کلیدها استفاده می‌شود. درابتدا ۵۶ بیت از ۶۴ بیت کلید توسط انتخاب جایگشت۱ (PC1)انتخاب می‌شوند و ۸ بیت باقی‌مانده یا دور ریخته می‌شوند و یا به عنوان parityبرای چک کردن مورد استفاده قرار می‌گیرند سپس این ۵۶ بیت به دو نیمه ۲۸ تایی تقسیم می‌شوند و پس از آن با هرنیمه به طور مستقل رفتار

می‌شود. در دور بعدی هر دو نیمه یک یا دو بیت به سمت چپ انتقال می‌یابند.. سپس ۴۸ بیت زیرکلید توسط PC2 انتخاب می‌شوند. ۲۴ بیت، نیمه راست و ۲۴ بیت دیگر نیمه چپ را تشکیل می‌دهند. با استفاده از انتقال در هر زیر کلید مجموعه متفاوتی از بیتها مورد استفاده قرار می‌گیرد. هر بیت تقریباً در ۱۴ تا ۱۶ زیر کلید مورد استفاده واقع می‌شود. الگوریتم key schedule در رمزگشایی مانند رمزگذاری است ولی زیر کلیدها در مقایسه با رمزگذاری در جهت معکوس هستند به غیر از این تغییر، بقیه الگوریتم مانند رمزگذاری انجام می‌شود.

پیاده سازی در cryptool:

ابتدا در قسمت templates>>Cryptography>>Modern>>DES Cipher را باز می کنیم.

در قسمت Plaintext متن اصلی Faeze Karami را وارد می کنیم. در قسمت Key کلید را 11 11 11 11 A1 B1 C1 11 در نظر میگیریم. قطعات را به صورت EBC میخواهیم رمز کنیم با padding صفرها. با زدن کلید start و تنظیم خروجی به صورت هگزادسیمال متن رمز شده DE 66 44 AC D7 8C 1A 67 9D B0 AB DB 44 E4 A5 9F خواهد بود.