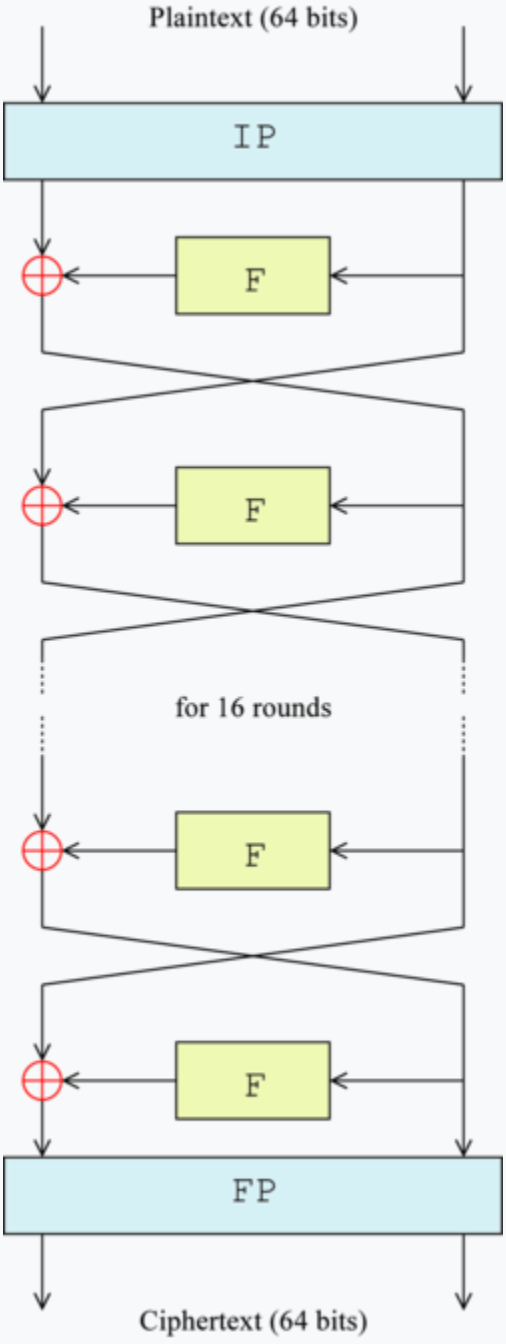
DES cryptography algorithm document

الگوریتمDES



نمای کلی الگوریتم

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.

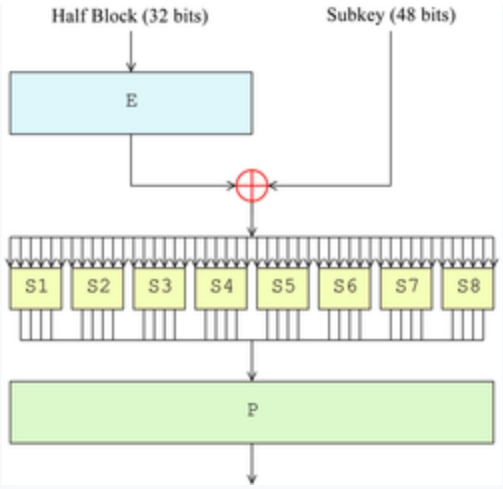
اگر K یک بلاک ۴۸ بیتی باشد که از کلید اصلی ۶۴ بیتی مشتق شده‌است و خروجی یک دور با ورودی LR و خروجی L1R1 به صورت زیر تعریف می‌شود L1=R R1=L XOR .
F(R,K)اگر KS تابعی باشد که کلید ۶۴ بیتی KEY و یک عدد صحیح در محدوده ۱ تا ۱۶ را به عنوان ورود ی می‌گیرد و کلید ۴۸ بیتی Kn را به عنوان خروجی تولید می‌کند به طوری که بیتهای Kn از تغییر محل بیتهای KEY حاصل شده‌اند داریم(n.KEY) KS =Kn :

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(L1,K)f XOR R=L1 L=R :

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



F تابع

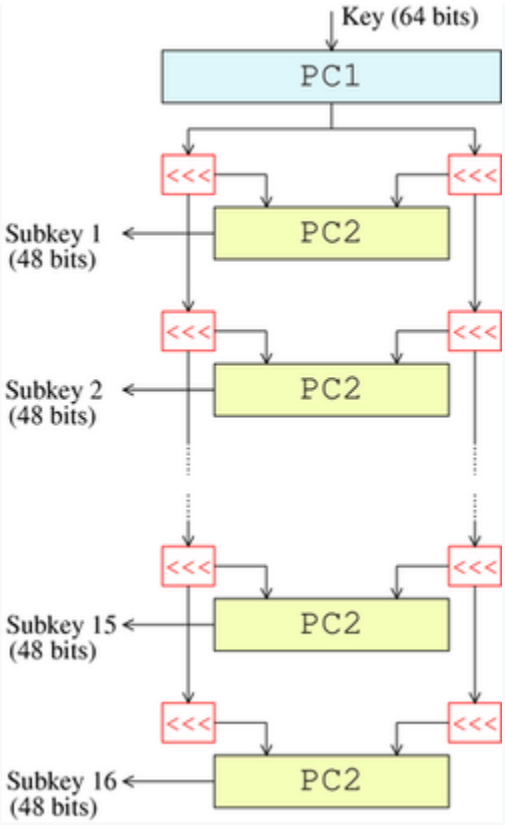
بسط :در این مرحله با استفاده از یک جایگشت انبساطی ۳۲ بیت به ۴۸ بیت گسترش داده می‌شود.

ترکیب کلید :در این مرحله حاصل مرحله قبل با یک زیر کلید XOR می‌شود. شش کلید ۴۸ بیتی با استفاده از الگوریتم key schedule از 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 up است به یک خروجی ۴ بیتی تبدیل می‌کند S-boxها قلب DES هستند و بدون آنها رمز خطی خواهد بود و در نتیجه قابل شکستن خواهد شد.

جایگشت :در نهایت ۳۲ بیت خروجیS-box ها 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 جایگشت1(PC1) انتخاب می‌شوند و ۸ بیت باقی‌مانده یا دور ریخته می‌شوند و یا به عنوانparity برای 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.

امنیتDES

اساسی‌ترین حمله برای هر رمزی، امتحان کردن کلیه مقادیر ممکن، برای کلید است. طول کلید، تعداد مقادیر ممکن برای کلید و هم چنین عملی بودن این روش را مشخص می‌کند. تردیدی که از ابتدا و حتی قبل از اینکه DES به عنوان استاندارد شناخته شود در مورد DES وجود داشت کافی بودن طول کلید بود NSA ،. IBMرا به کاهش طول کلید از ۱۲۸ بیت به ۶۴ بیت و سپس به ۵۶ بیت متعاقد نمود و این نشان می‌دهد که NSA حتی در آن زمان نیز، قادر به شکستن کلیدهایی با طول ۵۶ بیت بوده‌است. طرحهای متنوعی برای یک ماشین که قادر به شکستن کلیدهای DES باشد مطرح گردیده‌است. در سال ۱۹۷۷، Hellmanو Diffie ماشینی طراحی کردند که بیست میلیون دلار قیمت داشت و می‌توانست کلید DES را در یک روز پیدا کند. در سال Wiener ،1993 یک ماشین جستجوی کلید را پیشنهاد داد که یک میلیون دلار قیمت داشت و قادر بود کلید را در مدت هفت ساعت پیدا کند؛ ولی هیچ‌یک ازاین طرحهای ابتدایی پیاده‌سازی نشد و هیچ پیاده‌سازی ای مورد تأیید قرار نگرفت. در سال ۱۹۹۷ مؤسسه RSA securityاعلام کرد که به اولین تیمی که بتواند یک پیغام، که با استفاده از DES رمزگذاری شده‌است را بشکند یک جایزه ده هزار دلاری اعطا خواهد نمود. پروژه DESCHALL برنده این رقابت شد که این کار را با استفاده از زمان بیکاری (idle cycle) هزاران کامپیوتر در اینترنت، انجام داد. عملی بودن شکست DES با اختراع یک DES-cracker توسط EFF در سال ۱۹۹۸ بر همگان روشن شد. این ماشین قیمتی حدود دویست و پنجاه هزار دلار داشت و انگیزه این تیم برای اختراع این ماشین، این بود که نشان دهند که DES همچنان که از لحاظ تئوری قابل شکست است، از لحاظ عملی نیز می‌توان آن را شکست. این ماشین، کلید را با استفاده از روش جستجوی جامع فضای کلید در طی مدت زمان کمی بیش از دو روز پیدا می‌کند. تنها DES-crackerتأیید شده پس از ماشینEFF ، ماشین COPOCOBANA که در آلمان ساخته شد و بر خلاف EFF از مدارات مجتمع در دسترس و قابل پیکربندی دوباره ساخته شده‌است در این ماشین صد و بیست عدد FPGA از نوع XILINX Spartan- 1000 موازی با هم کار می‌کنند. آنها در ماژولهای DIMM 20 گروه بندی شده‌اند. هر کدام از این ماژولها

شامل شش FPGA می‌باشند. استفاده از سخت‌افزارهای قابل پیکربندی دوباره، سبب می‌شود که این ماشین برای شکستن کدهای دیگر نیز، قابل استفاده باشد. یکی از جنبه‌های جالب این ماشین، فاکتور هزینه آن است این ماشین با ده هزار دلار می‌تواند ساخته شود. کاهش هزینه با ضریب ۲۵ نسبت به EFF نشان دهنده پیشرفتهای متوالی در زمینه سخت‌افزارهای دیجیتالی است.

الگوریتم‌های جایگزینDES

نگرانی‌هایی که در مورد امنیت و طول کم کلید در DES وجود داشت محققان را به طراحی های جایگزین برای رمز قطعه‌ای، تشویق کرد که این تلاشها از سال ۱۹۸۰ شروع شد و تا اوایل ۱۹۹۰ ادامه داشت این تلاش ها منجر به ایجاد طراحی هایی از قبیل Blowfish ،RC5 ،IDEA، NEWDES، SAFER، CAST5و FEAL گردید. بیشتر این الگوریتم‌ها مانند DES روی قطعه‌های داده با طول ۶۴ بیت کار می‌کردند و می‌توانستند جایگزین DES شوند. اگرچه عموماً از کلیدهایی با طول ۶۴ یا ۱۲۸ بیت استفاده می‌کردند DES .می‌تواند دچار تغییراتی شود تا امن تر عمل نماید Triple DES .توسط یکی از مخترعان DES مطرح شد. در این روش DESبا استفاده از دو کلید (2TDES) و یا سه کلید متفاوت (3TDES) سه بار به کار برده می‌شود.

مشخصات عمومی الگوریتم رایندال

رایندال، یک الگوریتم رمز قطعه‌ای متفارن، با طول قالب داده ۱۲۸، ۱۹۲ و ۲۵۶ بیت است. طول کلید نیز مستقل از طول قالب، ۱۲۸،۱۹۲یا ۲۵۶ بیت باشد. الگوریتم بسته به طول قالب داده و طول کلید، مشتمل بر ۱۰، ۱۲ یا ۱۴ دور خواهد بود. رایندال دارای ساختاری برای بسط کلید است که از روی کلید اصلی بسته به تعداد دورها، تعدادی زیر کلید تولید می‌کند که در هر دور به قالب داده اضافه می‌شوند. الگوریتم، شامل سه تبدیل مهم MixColumn() و ShiftRow()و SubByte()است که اولی یک تابع جایگزینی غیر خطی و تأمین کننده امنیت سیستم و دومی و سومی توابعی خطی برای افزایش گسترش و اختلاط الگوریتم اند. در این رمز قطعه‌ای، ساختار سیستم رمزگشا، دقیقاً مشابه سیستم رمزگذار **نیست** .هم چنین چون با افزایش طول کلید تعداد دورهای الگوریتم افزایش می‌یابد، زمان اجرا و سرعت الگوریتم به طول کلید وابسته است.

تعاریف

- Nbتعداد چهاربایتی‌های موجود در قالب داده‌است به عنوان مثال برای قالب داده ۱۲۸ بیتی Nb=4است.

- Nkنیز تعداد آرایه‌های ۴ بایتی موجود در کلید است برای کلیدهای ۱۲۸، ۱۹۲ و ۲۵۶ بیتی Nkبه ترتیب ۴، ۶ و ۸ خواهد بود.

آرایه حالت یک آرایه دو بعدی با ابعاد ۴*Nbاز بایتها است بنابراین تعداد بایتهای آرایه حالت برابر تعداد بایتهای قالب داده خواهد بود در ابتدای الگوریتم متن اصلی بایت به بایت ازبالا به پایین و از چپ به راست در جدول حالت چیده می‌شود.

آرایه کلید بسط یافته - آرایه‌ای از کلمات ۴ بایتی است که کلید بسط یافته‌ای راکه تابع بسط کلید تولید کرده در خود ذخیره می‌کند این آرایه از (Nb*(Nr+1 کلمه ۴ بایتی تشکیل شده که (1 (Nr+کلید دورهای مختلف را در خود ذخیره می‌کند.

تعداد دورهای الگوریتم رایندال را با Nr نشان می‌دهیم که به طول قالب داده و کلید بستگی دارد بدین ترتیب که اگر هر کدام از Nb یاNk ، برابر ۶ باشد، خواهیم داشت، =Nr۱۲ و اگر هر کدام برابر ۸ باشد، خواهیم داشت، =Nr۱۴ .در غیر این صورت تعداد دورها برابر ۱۰ خواهد بود.

تبدیلها و توابع مورد استفاده

هر کدام از توابع و تبدیلهای زیر، روی آرایه حالت عمل کرده و آن را به نحوی تغییر می‌دهند.

تابعSubByte

این تابع یک تابع غیرخطی است که به طور مستقل روی بایتهای آرایه حالت عمل کرده و به جای هر بایت به کمک جدول S-box یک بایت جدید قرار می‌دهد این تبدیل معکوس پذیر است و از دو تبدیل زیر تشکیل شده‌است:

۱ -ابتدا معکوس ضربی بایت مورد نظر محاسبه می‌شود. معکوس «۰۰را» ۰۰ " در نظر می‌گیریم.
۲- تبدیل صحیح (affine)روی بایت مورد نظر اعمال می‌شود.

تبدیل ShiftRow

این تبدیل سه سطر آخر آرایه حالت را به تعداد معینی انتقال دورانی می‌دهد. برای اولین سطر، r=۰، انتقالی انجام نمی‌شود تعداد انتقال دورانی در سه سطر آخر بستگی به Nb دارد به این ترتیب که برای Nb=۸ انتقالهای سه سطر آخر به ترتیب برابر ۱،۳ و ۴ و برای Nb<8 برار ۱،۲ و ۳ خواهد بود.

تبدیل MixColumn

این تابع روی آرایه حالت، ستون به ستون عمل می‌کند. هر ستون به عنوان یک چندجمله‌ای در میدان دو به توان هشت در نظر گرفته می‌شود و در چند جمله‌ای ثابت a(x) ضرب می‌شود و به پیمانه+ x4 ۱ محاسبه می‌گردد.

تابع AddRoundKey

این تابع Nb کلمه اول آرایه را، همراه با Nb ستون آرایه حالت، XORمی‌کند و حاصل را، در آرایه حالت، قرار می‌دهد.

تابع بسط کلید

الگوریتم رایندال K(کلید اصلی) را گرفته و تعداد (1+Nr) کلید دور (Round key) تولید می‌کند. از آنجا که هر کدام از کلیدهای دوری از Nb کلمه ۴ بایتی تشکیل شده‌اند، جمعاً Nb*(Nr+1)کلمه ۴ بایتی به عنوان کلید بسط یافته از روی کلید اصلی تولید می‌شود. کلیدهای تولید شده، یک آرایه خطی تشکیل می‌دهند که هرکلید با W[i] نشان داده می‌شود. قبل از توصیف نحوه بسط کلید، ابتدا توابع زیر را تعریف می‌کنیم:

1-()SubWordاین تابع ر وی یک بردار ۴ بایتی عمل می‌کند به این صورت که S-box رایندال را روی تک تک بایتهای بردار اعمال کرده و بردار چهار بایتی جدیدی می‌سازد.

2-()RotWordاین تابع روی یک بردار چهار بایتی مانند (a0,a1,a2,a3) عمل کرده آن را می‌چرخاند و بردار (a3,a2,a1,a0) را به عنوان خروجی به دست می‌دهد.

3-Rcon[i]یا ثابت دور: این تابع یک بردار چهار بایتی به صورت زیر تولید می‌کند .

Rcon[i]=(xi#1,00,00,00) که xi ## 1 توانهای x هستند.

الگوریتم به این صورت است که ابتدا کلید اصلی، داخل آرایه کلمات قرار می‌گیرد و سپس هر کلمه جدید،w[i]، از XOR کلمه قبل، w[i-1]، و کلمه Nk مرتبه قبل، w[i-Nk]، به دست می‌آید.

توجه به این نکته ضروری است که الگوریتم تولید کلید، برای کلیدهایی با طول ۲۵۶ بیت، با الگوریتم مربوط به تولید کلید برای کلیدهای ۱۲۸ و ۱۹۲ بیتی، اندکی متفاوت است. اگر Nk=8و i-4 ضریبی از Nk باشد SubWord() روی w[i-1] ، پیش ازxor ، اعمال می‌شود.

استاندارد پیشرفته رمزنگاریAES

تا سال ۲۰۰۶ تنها حمله مؤثر علیه الگوریتم AES حمله side channel بوده‌است. آژانس ملی امنیت آمریکا (NSA) هر پنج الگوریتمی را که به مرحله نهایی راه یافتند را بررسی کرد و پس از بررسی، اعلام نمود که همه این الگوریتم‌ها برای حفاظت اطلاعات غیر سری آمریکا، به اندازه کافی، امنیت را فراهم می‌کنند. 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. این اولین بار بود که NSA یک روش رمزنگاری را برای رمزگذاری اطلاعات فوق محرمانه در اختیار عموم قرار می‌داد.
رایج‌ترین راه برای حمله به رمز قطعه‌ای امتحان کردن حملات متنوع، روی نسخه‌های رمز با تعداد کاهش یافته‌ای "دور" است AES .برای کلیدهای ۱۲۸ بیتی ۱۰ دور، برای کلیدهای ۱۹۲ بیتی ۱۲ دور و برای کلیدهای ۲۵۶ بیتی ۱۴ دور دارد. تا سال ۲۰۰۶ بهترین حمله با استفاده از ۷ دور برای کلیدهای ۱۲۸ بیتی، ۸ دور برای کلیدهای ۱۹۲ بیتی و ۹ دور برای کلیدهای ۲۵۶ بیتی بوده‌است. برخی از رمزنگاران در مورد امنیت AES اظهار نگرانی می‌کنند آنها معتقدند که حاشیه امنیت (فاصله بین دورهای الگوریتم و دورهای لازم برای شکستن رمز کم است. هم چنین این خطر وجود دارد که با پیشرفت الگوریتم‌های ذکر شده این الگوریتم‌ها بتوانند رمز را با زمانی کمتر از زمان لازم برای جستجوی جامع در فضای کلید بشکنند. شکستن یک کلید ۱۲۸ بیتی به ۲۱۲۰ عمل نیاز دارد که در مقایسه با ۲۱۲۸ بسیار کم است که امروزه کاملاً غیرممکن و غیر

عملی است. بزرگترین حمله که با استفاده از جستجوی جامع روی فضای کلید صورت گرفته‌است منجر به شکستن کلید RC5 شصت و چهار بیتی شده‌است. پس در این مورد، جای نگرانی وجود ندارد. بقیه تردیدهایی که در مورد این الگوریتم وجود دارد راجع به ساختار ریاضی AES است. بر خلاف اکثر الگوریتم‌های رمزقطعه‌ای، AESیک تعریف جبری مرتب دارد. این ساختار، تاکنون منجر به هیچ حمله‌ای نشده‌است. ولی برخی از محققان می‌گویند که ایجاد یک رمز بر مبنای فرضیات سخت جدید، به دور از ریسک نیست. در سال ۲۰۰۲ یک حمله تئوریکی به نام حمله XSLتوسط Nicolas Courtois و Josef Pieprzyk مطرح شد. این دو نفر اعلام کردند که در این الگوریتم ضعفهایی وجود دارد. چندین متخصص رمزشناسی مشکلاتی را درساختار ریاضی حمله پیشنهاد شده، کشف کردند و اعلام کردند که مخترعان این حمله احتمالاً در تخمین‌های خود دچار اشتباه شده‌اند. اینکه آیا حمله XSL می‌تواند علیه AES عمل کند یا نه، سؤالی است که هنوز به آن پاسخی داده نشده‌است؛ ولی احتمال اینکه این حمله بتواند در عمل انجام شود بسیار کم است

حمله کانال جانبی

حمله کانال جانبی به رمز صدمه‌ای نمی‌رساند ولی به پیاده‌سازی رمز روی سیستم، حمله می‌کند و باعث فاش شدن داده‌ها می‌شود. چندین حمله برای برخی از پیاده‌سازیهای خاص AES شناخته شده‌است که در اینجا، مورد اشاره قرار می‌گیرند. در آوریل سال ۲۰۰۵، D.J.Bernsteinاعلام کرد که حمله cache timing می‌تواند یک سرور متعارف را که برای دادن اطلاعات تنظیم وقت به اندازه ممکن طراحی شده‌است واز روش رمزنگاری openSSL AESاستفاده می‌کند را مورد حمله قرار دهد. یک حمله به بیش از دویست میلیون chosen plaintextنیاز دارد. برخی معتقدند که این حمله با فاصله یک و بیش از یک hop در اینترنت امکان‌پذیر نیست. در اکتبر سال ۲۰۰۵، Dag Arne Oskiv، Adi Shamir، Eran Tromerیک مقاله منتشر کردند و در آن چندین حمله cache timing را که می‌توانست علیه AES مؤثر واقع شود، توضیح دادند. یکی از این حمله‌ها قادر بود که کلید را پس از ۸۰۰ عمل و در مدت ۵۶ میلی ثانیه به دست آورد ولی برای انجام این حمله، حمله کننده باید برنامه را روی همان سیستمی که از AES استفاده می‌کند به اجرا در بیاورد.