معرفی و بررسی امنیت الگوریتم های رمزنگاری RSA و DES (نسخه PDF)

در این مقاله قصد دارم مختصری در خصوص امنیت الگوریتم رمزنگاری DES ِ RSA توضیح بدم .

مقدمه‌ای بر رمزنگاری

رمزنگاری(Cryptography) علم کـدها و رمزهاست. علم رمزنگاری در جسـتجوی روش‌هایی برای کد کردن یا رمز کردن پیغام‌ها، و روش‌های متناظری برای از کـد درآوردن یا رمز خوانـدن است.رمز کردن به‌طور شاخص از یک کلیـد عددی مشـخص (که ممکن است رقم‌های زیادی داشـته باشـد) اسـتفاده می‌کنـد و همان عـدد برای رمزخوانی به کار می‌رود. بـدون این کلیـد خواندن پیغام‌های رمز شده ممکن نیست؛ بنابراین ایمنی دستگاه به‌سختی یافتن این کلید بستگی دارد.

دو سیستم رمزنگاری مهم وجود دارد:

- ۱- سیستم رمزنگاری متقارن
- ۲- سیستم رمزنگاری نامتقارن یا کلید عمومی

سیستم رمزنگاری متقارن – الگوریتم DES

در این رمزنگاری از یک کلید برای رمزگذاری و رمزگشایی داده‌ها اسـتفاده می‌شود. سـرعت عملیات رمزگذاری در این حالت بیشتر می‌شود ولی درجه اطمینـان آن نیز کمـتر هست. الگوریتم DES در دهـۀ ۷۰ میلادی در آمریکا به‌عنوان یک اسـتاندارد کدگـذاری مطرح شـد. این الگوریتم این‌گونه عمل می‌کند که رشـته‌ای از متن اصـلی با طول ثابت را به‌عنوان ورودی می‌گیرد و پس از انجام یک سـری اعمال پیچیده روی آن خروجی را که طولی برابر طول ورودی دارد تولید می‌کند.

DES هم‌چنین از یک کلیـد برای ایجاد رمز اسـتفاده می‌کند و تنها کسانی قادر به رمزگشایی خواهند بود که مقدار کلید را می‌دانند. اگرچه تحلیل‌هایی که دربارۀ DES انجام‌شده است 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 نسـبت به جستجوی جامع فضای کلید نیاز دارند ولی این روش‌ها در عمل امکان‌پذیر نیستند.

با شکسـته شدن الگوریتم DES این اسـتاندارد در سال ۱۹۹۸ تمدیـد نشد و در سال ۲۰۰۱، الگوریتم AES به‌عنوان اسـتاندارد جایگزین آن تصویب شد. این الگوریتم مانند DES یـک الگوریتم رمز قطعه‌ای است ولی برخلاف DES از ساختار فیسـتل استفاده نمی‌کند. تا سال ۲۰۰۶ تنهـا حمله مؤثر علیه الگوریتم AES حمله side channel بوده است. در ژوئن سـال ۲۰۰۳ دولت آمریکـا اعلام کرد که از AES می‌توان برای حفاظت از اطلاعات رده‌بندی‌شده و سـری نیز اسـتفاده کرد. برای اطلاعات فوق سری و محرمانه باید از کلیدهایی با طول ۱۹۲ یا ۲۵۶ بیت استفاده کرد.

اساسـی‌ترین حمله برای هر رمزی امتحان کردن کلیه مقادیر ممکن برای کلیـد است. طول کلید، تعداد مقادیر ممکن برای کلید و هم‌چنین عملی بودن این روش را مشخص می‌کند. تردیدی که از ابتدا و حتی قبل از اینکه DES به‌عنوان استاندارد شناخته شود در مورد DES وجود داشت کافی بودن طول کلید بود NSA، IBM را به کاهش طول کلید از ۱۲۸ بیت به ۶۴ بیت و سپس به ۵۶ بیت نمود و این نشان می‌دهد که NSA حتی در آن زمـان نیز قـادر به شکسـتن کلیـدهایی با طول ۵۶ بیت بوده است. طرح‌هـای متنوعی برای یـک ماشـین که قادر به شکستن کلیدهای DES باشد مطرح گردیده است.

در سال ۱۹۷۷، Hellman و Diffie ماشینی طراحی کردند که بیست میلیون دلار قیمت داشت و می‌توانست کلید DES را در یک روز پیدا کند. در سال ۱۹۹۳ Wiener یک ماشـین جستجوی کلید را پیشنهاد داد که یک‌میلیون دلار قیمت داشت و قادر بود کلید را در مدت هفت ساعت پیـدا کنـد؛ ولی هیـچ‌یک از این طرح‌های ابتـدایی پیاده‌سازی نشد و هیچ پیاده‌سازی مورد تأیید قرار نگرفت. در سال ۱۹۹۷ مؤسسه RSA security اعلام کرد که به اولین تیمی که بتواند یک پیغام را که با استفاده از DES رمزگذاری شده است 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 پنجاه‌هزار دلار داشت و انگیزه این گروه بر ای اختراع این ماشین، این بود که نشان دهند که DES هم چنان‌که ازلحاظ تئوری قابل شکست است ازلحاظ عملی نیز می‌توان آن را شکست. این ماشین کلید را با استفاده از روش جستجوی جامع فضای کلید درطی مدت‌زمان کمی بیش از دو روز پیدا می‌کند. تنها DES-cracker تأییدشده پس از ماشین EFF، ماشین COPOCOBANA که در آلمان ساخته شد و برخلاف EFF از مدارات مجتمع در دسترس و قابل پیکربندی دوباره ساخته‌شده است .

در این ماشین صد وبیست عدد FPGA از نوع ۱۰۰۰ -XILINX Spartan موازی باهم کار می‌کنند آن‌ها در ماژول‌های ۲۰ DIMM گروه‌بندی‌شده‌اند هرکدام از این ماژول‌ها شامل شش FPGA می‌باشند. استفاده از سخت‌افزارهای قابل پیکربندی دوباره سبب می‌شود که این ماشین برای شکستن کدهای دیگر نیز قابل‌استفاده 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 نشان‌دهنده پیشرفته‌ای متوالی درزمینهٔ سخت‌افزارهای دیجیتالی است.سه حمله شناخته‌شده وجود دارد که می‌تواند به‌طور کامل ۱۶ دور DES را با پیچیدگی کمتر از حمله brute-force بشکند. این سه حمله از قرار زیر می‌باشند:

differential cryptanalysis (DC), linear cryptanalysis (LC), and Davies' attack

توجه کنید که این حملات صرفاً بحث تئوری می‌باشند و تا حالا به‌صورت عملی انجام‌نشده‌اند.ضعف ساختاری DES مربوط به‌اندازه کوچک کلید و بلوک خود می‌باشد که این مشکل در ورژن ۳DES حل‌شده است.

سیستم رمزنگاری نامتقارن - الگوریتم RSA

رمزگذاری نامتقارن یا کلید عمومی بر اساس دو کلید به نام‌های عمومی و خصوصی صورت می‌گیرد. هر فردی یک کلید عمومی و یک کلید خصوصی خواهد داشت. کلید عمومی شما در دسترس دیگران می‌باشد ولی کلید خصوصی فقط از آن شما و در دسترس شما می‌باشد.فرض کنید فردی برای شما پیغامی را بفرستد. این پیغام در کامپیوتر مبدأ با کلید عمومی شما رمزگذاری شده و برای شما فرستاده می‌شود تنها کسی که قادر به باز کردن رمز می‌باشد شما می‌باشید زیرا کلید خصوصی دارید که با کلید عمومی شما ارتباط دارد.معمولی‌ترین الگوریتمی که برای رمزنگاری نامتقارن استفاده می‌شود، الگوریتم RSA می‌باشد.این روش پس از کارهای اولیه سه ریاضیدان به نام‌های Adi Shamir، Ron Rivest و Leonard Adleman در سال ۱۹۷۸ منتشر شد.الگوریتم RSA در ۳ مرحله کار خود انجام می‌دهد:

- ۱- ساخت کلید
- ۲- رمزگذاری
- ۳- رمزگشایی

انواع حملات به RSA

رمزنگاری سطح پایین، باعث می‌شود که متن رمز شده به‌راحتی شکسته شود.یکی از حملات احتمالی حمله متن رمز شده شناخته‌شده (known ciphertext) می‌باشد. در این حمله مهاجم هم‌متن ساده و رمز شده را می‌داند و سعی در شکستن کلید می‌کند.

حمله Side-channel analysis

حمله side-channel از مکانیزم تجزیه‌وتحلیل BPA و یک فرایند جاسوسی برای کشف کلید خصوصی استفاده می‌کند. زمانی این حمله موفق خواهد بود که بتواند کلید خصوصی را حدس بزند و ازآنجاکه این کلید از بیش از ۱۰۰۰ عدد باینری تشکیل‌شده است، حدس زدن آن کاری خیلی سختی و زمان‌بر و اصطلاحاً غیرممکن می‌باشد.الگوریتم RSA از نوع الگوریتم‌های رمزگذاری نامتقارن (Asymmetric Algorithm) است که از ۲ کلید برای code و decode کردن داده‌ها استفاده می‌کند.

این کلیدها را Public key و Private key می‌گویند. Public برای کد کردن پیام توسط فرستنده و Private key برای رمزگشایی توسط گیرنده استفاده می‌شود. الگوریتم DES از نوع الگوریتم رمزنگاری متقارن (Symmetric) است که از یک کلید برای رمزنگاری و رمزگشایی استفاده می‌کند. درنتیجه، مختصر و مفید، الگوریتم نامتقارن دو کلیدی مثل RSA از الگوریتم متقارن تک کلیدی مثل DES قویی‌تر و امن‌تر است.

میلاد فشی

ممنون از مقـاله خوبتون.همیشه گفتن که RSA نامتقارن و دوکلیـد داره.کلید عمومی با Data ارسال میشه.ولی کلید خصوصـی فقط در اختیار گیرنده پیامه که با اون رمزگشایی میکنه.اما سوال اینجاست که این کلید در واقع چیه ؟ مثال عملی میشه بزنید.این کلید در یک توکن سـخت افزاری ذخیره میشه ؟ مثلاـ چطوری میشه به طور عملی از اون اسـتفاده کرد؟ مثلا برای الگوریتم AES برنامه های زیادی ساخته شده.مثل TrueCrypt و نسخه جدید فورک شده اون VeraCrypt و AESCrypt و ... ولیRSA کاربردی ازش هست ؟

مطلب اصلی